POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proceso gestión de la tecnología y la información

Año 2026

Código SG/MIPG	127-PPPGI-01
Vigencia desde	05/06/2026
Versión	10

ALCALDÍA MAYOR DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

BOGOTÁ

Tabla de Contenido

1. INTRODUCCIÓN

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP reconoce la información como uno de sus activos estratégicos más valiosos para el cumplimiento de su misión institucional, la prestación de servicios a la ciudadanía, la toma de decisiones, la gestión administrativa y el desarrollo de sus procesos misionales, estratégicos, de apoyo, evaluación y control.

En un entorno caracterizado por la transformación digital, el uso intensivo de tecnologías de la información, la adopción de servicios en la nube, la interoperabilidad con entidades públicas y privadas, el intercambio permanente de información y el incremento de las amenazas cibernéticas, resulta indispensable establecer lineamientos que permitan proteger adecuadamente los activos de información y los servicios tecnológicos que soportan la operación institucional.

La Seguridad y Privacidad de la Información constituye un componente fundamental para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, reduciendo la probabilidad e impacto de incidentes que puedan afectar el cumplimiento de los objetivos institucionales, la prestación de servicios, la continuidad de la operación o la confianza de los ciudadanos y demás partes interesadas.

La presente Política General de Seguridad y Privacidad de la Información establece la posición institucional del DADEP frente a la gestión de la Seguridad y Privacidad de la Información y la seguridad digital, definiendo el marco general para la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), en concordancia con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG), los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), las directrices distritales aplicables y las mejores prácticas internacionales en materia de seguridad de la información.

Esta política se fundamenta en los principios establecidos por la norma NTC ISO/IEC 27001:2022 y demás disposiciones legales, regulatorias, técnicas y organizacionales aplicables, constituyéndose en el documento rector que orienta la definición de políticas específicas, procedimientos, estándares, lineamientos y controles destinados a proteger los activos de información del DADEP.

Las disposiciones contenidas en este documento son de obligatorio cumplimiento para servidores públicos, contratistas, proveedores, terceros y demás partes interesadas que, en desarrollo de sus funciones o actividades, tengan acceso a los activos de información, servicios tecnológicos, infraestructura tecnológica, plataformas digitales o recursos de procesamiento de información administrados por el DADEP.

La Alta Dirección del DADEP manifiesta mediante esta política su compromiso con la protección de la información institucional, la gestión adecuada de los riesgos de Seguridad y Privacidad de la Información y la consolidación de una cultura organizacional orientada a la seguridad digital, la protección de los activos de información y el fortalecimiento permanente de la confianza de la ciudadanía.

2. OBJETIVO

Establecer los lineamientos generales que orienten la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital en el Departamento Administrativo de la Defensoría del Espacio Público – DADEP, con el propósito de proteger los activos de información, los recursos tecnológicos, los servicios digitales, la infraestructura tecnológica y la información institucional durante todo su ciclo de vida, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Así mismo, la presente política tiene como finalidad proporcionar el marco de referencia para la implementación, operación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), promoviendo la gestión integral de riesgos de seguridad de la información, el fortalecimiento de las capacidades institucionales, la protección frente a amenazas internas y externas, la continuidad de la operación y el cumplimiento de los requisitos legales, regulatorios, contractuales y organizacionales aplicables.

Mediante la adopción de esta política, el DADEP busca fortalecer la confianza de la ciudadanía, grupos de valor, entidades de control, proveedores y demás partes interesadas, asegurando que la información institucional y los servicios tecnológicos sean gestionados de manera segura, eficiente y alineada con los objetivos estratégicos de la entidad, los lineamientos de Gobierno Digital y las mejores prácticas nacionales e internacionales en materia de Seguridad de la Información.

3. CONTEXTO DE LA ORGANIZACIÓN

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP es una entidad del nivel central del Distrito Capital encargada de contribuir a la defensa, inspección, vigilancia, regulación, administración, sostenibilidad y aprovechamiento del espacio público de Bogotá D.C., mediante la formulación de políticas, la gestión de información estratégica y el desarrollo de procesos institucionales orientados al cumplimiento de su misión.

Para el desarrollo de sus funciones, el DADEP gestiona información de carácter estratégico, administrativo, financiero, contractual, jurídico, tecnológico, geográfico, catastral, documental y de atención a la ciudadanía, apoyándose en activos de información, sistemas de información, servicios digitales, infraestructura tecnológica, servicios en la nube, redes de comunicaciones y recursos tecnológicos que soportan la operación institucional.

La entidad reconoce que la información constituye un activo estratégico para el cumplimiento de sus objetivos institucionales y para la adecuada prestación de servicios a la ciudadanía, razón por la cual requiere implementar mecanismos que permitan protegerla frente a amenazas internas y externas que puedan comprometer su confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad.

En el marco de la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital, el DADEP considera factores internos tales como su estructura organizacional, los procesos institucionales, el talento humano, la infraestructura tecnológica, los activos de información, los servicios tecnológicos, los proyectos de transformación digital, la gestión documental, la cultura organizacional y las capacidades institucionales para la administración de riesgos.

Así mismo, se consideran factores externos relacionados con el marco normativo aplicable, los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), las políticas de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), los requerimientos de los organismos de control, la evolución permanente de las amenazas cibernéticas, las vulnerabilidades tecnológicas, los riesgos asociados a terceros y proveedores, las dependencias con otras entidades públicas y privadas, así como las necesidades y expectativas de los ciudadanos, grupos de valor y demás partes interesadas.

La gestión de la Seguridad y Privacidad de la Información deberá desarrollarse bajo un enfoque basado en riesgos, considerando permanentemente el contexto institucional y el entorno en el que opera la entidad, con el propósito de garantizar la protección de los activos de información, fortalecer la resiliencia institucional, asegurar la continuidad de la operación y contribuir al cumplimiento de los objetivos estratégicos del DADEP.

La presente Política General de Seguridad y Privacidad de la Información se articula con el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los demás instrumentos de gestión institucional, constituyéndose en un elemento fundamental para el fortalecimiento de la seguridad digital y la protección de la información institucional.

4. ALCANCE

La presente Política General de Seguridad y Privacidad de la Información aplica a todos los procesos estratégicos, misionales, de apoyo, evaluación y control del Departamento Administrativo de la Defensoría del Espacio Público – DADEP, así como a los activos de información, recursos tecnológicos, servicios digitales e infraestructura tecnológica que soportan el cumplimiento de la misión institucional.

Su alcance comprende la información institucional en cualquier formato o medio de almacenamiento, procesamiento, transmisión o disposición, incluyendo información física, digital, audiovisual, verbal o cualquier otro mecanismo utilizado para su gestión, independientemente de su nivel de clasificación o ubicación.

La política aplica a los sistemas de información, aplicaciones, bases de datos, plataformas tecnológicas, redes de comunicaciones, estaciones de trabajo, equipos de cómputo, dispositivos móviles, servicios de almacenamiento, herramientas colaborativas, servicios de correo electrónico, mecanismos de respaldo, servicios tecnológicos, infraestructura tecnológica local y servicios en la nube utilizados para el desarrollo de las funciones institucionales.

Igualmente, el alcance comprende los activos de información administrados, procesados, almacenados o transmitidos por terceros, proveedores, contratistas, operadores tecnológicos y demás partes externas que, en cumplimiento de obligaciones contractuales o legales, tengan acceso a información institucional o a recursos tecnológicos del DADEP.

La presente política cubre todas las etapas del ciclo de vida de la información, incluyendo su creación, captura, recepción, clasificación, almacenamiento, procesamiento, consulta, uso, intercambio, transmisión, respaldo, recuperación, conservación, archivo y disposición final.

Las disposiciones establecidas en este documento deberán ser observadas en todas las dependencias, sedes, proyectos, iniciativas tecnológicas, ambientes de desarrollo, pruebas y producción, así como en cualquier modalidad de trabajo autorizada por la entidad, incluyendo esquemas presenciales, remotos o híbridos.

No se identifican exclusiones dentro del alcance definido para la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital del DADEP. Cualquier exclusión futura deberá estar debidamente documentada, justificada, evaluada en términos de riesgo y aprobada por la Alta Dirección de conformidad con los procedimientos institucionales establecidos.

5. APLICABILIDAD

La presente Política General de Seguridad y Privacidad de la Información es de obligatorio cumplimiento para todos los servidores públicos, contratistas, practicantes, pasantes, proveedores, operadores tecnológicos, terceros y demás partes interesadas que, en desarrollo de sus funciones, actividades, obligaciones contractuales o relaciones con la entidad, tengan acceso a los activos de información, recursos tecnológicos, servicios digitales, sistemas de información o infraestructura tecnológica del Departamento Administrativo de la Defensoría del Espacio Público – DADEP.

Las disposiciones contenidas en esta política deberán ser observadas y aplicadas independientemente del tipo de vinculación, nivel jerárquico, ubicación física, modalidad de trabajo o medio utilizado para acceder a la información institucional o a los recursos tecnológicos de la entidad.

La aplicabilidad de esta política se extiende a todas las actividades relacionadas con la creación, acceso, procesamiento, almacenamiento, transmisión, intercambio, conservación y disposición de la información institucional, así como al uso de los activos de información y recursos tecnológicos que soportan la operación del DADEP.

Los terceros que presten servicios a la entidad o que tengan acceso a información institucional deberán cumplir las disposiciones establecidas en la presente política y en los demás instrumentos que conforman el Modelo de Seguridad y Privacidad de la Información (MSPI), sin perjuicio de las obligaciones adicionales que se establezcan mediante acuerdos, contratos, convenios, cláusulas de confidencialidad o demás mecanismos jurídicos aplicables.

El incumplimiento de las disposiciones establecidas en esta política podrá dar lugar a la aplicación de las medidas administrativas, disciplinarias, contractuales, civiles o penales a que haya lugar, de conformidad con la normatividad vigente y las competencias de la entidad.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP reconoce la Seguridad y Privacidad de la Información y la Seguridad Digital como elementos estratégicos para el cumplimiento de su misión institucional, la protección de sus activos de información, la prestación de servicios a la ciudadanía y el fortalecimiento de la confianza de las partes interesadas.

En consecuencia, la entidad se compromete a implementar, mantener y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI), incorporando mecanismos de gestión orientados a la identificación, valoración, tratamiento y monitoreo de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional.

La gestión de la Seguridad y Privacidad de la Información deberá desarrollarse bajo un enfoque basado en riesgos, considerando el contexto organizacional, las necesidades institucionales, los requisitos legales y regulatorios aplicables, las amenazas emergentes, las vulnerabilidades tecnológicas y los impactos potenciales sobre los procesos, servicios y activos de información de la entidad.

El DADEP adoptará controles administrativos, técnicos, físicos y organizacionales orientados a prevenir, detectar, responder y recuperar oportunamente la operación frente a eventos que puedan comprometer la seguridad de la información, la continuidad de los servicios tecnológicos o el cumplimiento de los objetivos institucionales.

La entidad promoverá una cultura institucional de Seguridad y Privacidad de la Información mediante actividades de sensibilización, capacitación y fortalecimiento de competencias dirigidas a servidores públicos, contratistas y demás partes interesadas, fomentando la apropiación de buenas prácticas para la protección de la información y el uso seguro de los recursos tecnológicos.

Así mismo, el DADEP garantizará que la gestión de la Seguridad y Privacidad de la Información forme parte integral de los procesos institucionales, los proyectos tecnológicos, las iniciativas de transformación digital, la adquisición de bienes y servicios tecnológicos, la gestión de proveedores y terceros, y la administración de los recursos tecnológicos que soportan la operación institucional.

La entidad velará por la protección de los activos de información durante todo su ciclo de vida, desde su creación o recepción hasta su disposición final, aplicando criterios de clasificación, manejo, almacenamiento, transmisión, conservación y eliminación acordes con su nivel de criticidad, sensibilidad y valor para la organización.

El DADEP promoverá la implementación de mecanismos que fortalezcan la resiliencia institucional y la continuidad de la operación, mediante la gestión adecuada de incidentes de seguridad de la información, la recuperación ante eventos adversos y la mejora continua de los controles de seguridad implementados.

Todos los servidores públicos, contratistas, proveedores y terceros que tengan acceso a la información institucional o a los recursos tecnológicos de la entidad serán responsables de

cumplir las disposiciones establecidas en la presente política y en los demás documentos que conforman el Modelo de Seguridad y Privacidad de la Información.

La Alta Dirección respaldará permanentemente la implementación de esta política, disponiendo los recursos necesarios para su sostenibilidad y promoviendo el fortalecimiento continuo de las capacidades institucionales en materia de Seguridad y Privacidad de la Información y Seguridad Digital.

7. PRINCIPIOS DE LA POLÍTICA

La gestión de la Seguridad y Privacidad de la Información en el Departamento Administrativo de la Defensoría del Espacio Público – DADEP se fundamenta en los siguientes principios:

a) Protección de la información

La información institucional deberá ser protegida de manera adecuada frente a amenazas internas y externas que puedan afectar su confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad.

b) Gestión basada en riesgos

Las decisiones relacionadas con la Seguridad y Privacidad de la Información deberán sustentarse en la identificación, análisis, evaluación, tratamiento y monitoreo permanente de los riesgos que puedan afectar los activos de información y los servicios tecnológicos de la entidad.

c) Mejora continua

La entidad promoverá el fortalecimiento permanente de su Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la evaluación periódica de controles, la implementación de acciones de mejora y la adaptación a los cambios tecnológicos, normativos y organizacionales.

d) Cumplimiento normativo

La gestión de la Seguridad y Privacidad de la Información deberá realizarse en observancia de las disposiciones legales, regulatorias, contractuales y demás lineamientos aplicables a la entidad.

e) Responsabilidad compartida

La Seguridad y Privacidad de la Información es responsabilidad de todos los servidores públicos, contratistas, proveedores y terceros que tengan acceso a la información institucional o a los recursos tecnológicos del DADEP, de acuerdo con sus funciones y responsabilidades.

f) Protección de los activos de información

Los activos de información deberán ser identificados, clasificados, gestionados y protegidos de acuerdo con su valor, criticidad, sensibilidad y nivel de riesgo para la entidad.

g) Seguridad desde el diseño

Los requisitos de Seguridad y Privacidad de la Información deberán considerarse desde la planificación, adquisición, desarrollo, implementación, operación y mantenimiento de procesos, sistemas de información, proyectos tecnológicos y servicios digitales.

h) Cultura de seguridad

La entidad promoverá el desarrollo de una cultura institucional orientada a la protección de la información, mediante procesos permanentes de sensibilización, capacitación y fortalecimiento de competencias.

i) Continuidad de la operación

La gestión de la Seguridad y Privacidad de la Información deberá contribuir a garantizar la continuidad de los procesos y servicios institucionales frente a eventos que puedan afectar la operación normal de la entidad.

j) Gestión segura de terceros

Los riesgos derivados de proveedores, contratistas, operadores tecnológicos y demás terceros deberán ser gestionados mediante la implementación de controles, acuerdos y mecanismos de seguimiento acordes con el nivel de riesgo identificado.

k) Uso adecuado de los recursos tecnológicos

Los recursos tecnológicos institucionales deberán utilizarse de manera responsable, ética y segura, exclusivamente para los fines autorizados y en cumplimiento de las disposiciones institucionales aplicables.

l) Transparencia y confianza institucional

La gestión de la Seguridad y Privacidad de la Información deberá contribuir al fortalecimiento de la confianza de la ciudadanía, grupos de valor, organismos de control y demás partes interesadas, mediante la protección adecuada de la información institucional y la prestación segura de los servicios digitales.

8. DEFINICIONES / GLOSARIO

Para efectos de la presente Política General de Seguridad y Privacidad de la Información, se adoptan las siguientes definiciones, sin perjuicio de las establecidas en la normatividad vigente, el Modelo de Seguridad y Privacidad de la Información (MSPI), la familia de normas ISO/IEC 27000 y demás lineamientos aplicables:

Activo de Información: Cualquier información o elemento que tenga valor para la entidad y que sea necesario para el cumplimiento de sus objetivos institucionales. Incluye información, datos, documentos, sistemas de información, aplicaciones, servicios tecnológicos, infraestructura tecnológica, recursos humanos y demás elementos relacionados con el tratamiento de la información.

Amenaza: Causa potencial de un incidente no deseado que puede ocasionar daño a un activo de información o afectar la operación de la entidad.

Autenticidad: Propiedad que garantiza que una entidad, usuario, sistema o información es genuina y puede ser verificada como tal.

Confidencialidad: Propiedad de la información que garantiza que esta no sea divulgada ni puesta a disposición de personas, entidades o procesos no autorizados.

Control: Medida de carácter administrativo, técnico, físico u organizacional implementada para gestionar riesgos y fortalecer la protección de los activos de información.

Disponibilidad: Propiedad de la información que garantiza que esta sea accesible y utilizable por los usuarios autorizados cuando sea requerida.

Evento de Seguridad de la Información: Ocurrencia identificada relacionada con el estado de un sistema, servicio o red que indica una posible afectación a la Seguridad y Privacidad de la Información o la existencia de una falla en los controles establecidos.

Incidente de Seguridad de la Información: Evento o conjunto de eventos de seguridad que comprometen o tienen el potencial de comprometer la confidencialidad, integridad, disponibilidad o autenticidad de la información o de los servicios tecnológicos de la entidad.

Información: Conjunto de datos organizados que poseen significado y valor para la entidad, independientemente del medio o formato en que se encuentren almacenados o transmitidos.

Integridad: Propiedad de la información que garantiza su exactitud, completitud y protección frente a modificaciones no autorizadas.

Modelo de Seguridad y Privacidad de la Información (MSPI): Marco de referencia definido por el Ministerio de Tecnologías de la Información y las Comunicaciones para orientar la gestión de la Seguridad y Privacidad de la Información en las entidades públicas.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto sobre los activos de información, los procesos institucionales o los servicios tecnológicos de la entidad.

Seguridad de la Información: Preservación de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Seguridad Digital: Conjunto de políticas, capacidades, procesos, controles y mecanismos orientados a proteger los activos digitales, los servicios tecnológicos, la infraestructura tecnológica y la información frente a amenazas y riesgos del entorno digital.

Trazabilidad: Capacidad de identificar, registrar y reconstruir las acciones realizadas sobre la información, los sistemas de información o los recursos tecnológicos.

Vulnerabilidad: Debilidad de un activo, control o proceso que puede ser explotada por una amenaza para generar una afectación a la seguridad de la información.

9. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección del Departamento Administrativo de la Defensoría del Espacio Público – DADEP reconoce la Seguridad y Privacidad de la Información y la Seguridad Digital como elementos fundamentales para el cumplimiento de la misión institucional, la prestación de servicios a la ciudadanía, la protección de los activos de información y el fortalecimiento de la confianza de las partes interesadas.

En consecuencia, se compromete a liderar, promover, apoyar y respaldar la implementación, mantenimiento, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la

Información (MSPI), asegurando su integración con la gestión institucional, la planeación estratégica, la gestión de riesgos y los demás sistemas y modelos de gestión aplicables a la entidad.

Para el cumplimiento de este compromiso, la Alta Dirección velará por:

a) Promover una cultura institucional orientada a la Seguridad y Privacidad de la Información y la Seguridad Digital, fomentando la participación activa de servidores públicos, contratistas y demás partes interesadas en la protección de los activos de información.

b) Proporcionar los recursos humanos, tecnológicos, financieros y administrativos necesarios para la implementación, operación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información.

c) Garantizar que la gestión de la Seguridad y Privacidad de la Información se encuentre alineada con los objetivos estratégicos, planes institucionales, procesos, proyectos y necesidades de la entidad.

d) Apoyar la identificación, evaluación, tratamiento y monitoreo de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital que puedan afectar el cumplimiento de los objetivos institucionales.

e) Impulsar la adopción de controles administrativos, técnicos, físicos y organizacionales orientados a proteger la información institucional y los servicios tecnológicos que soportan la operación de la entidad.

f) Promover el cumplimiento de los requisitos legales, regulatorios, contractuales y normativos aplicables en materia de Seguridad de la Información, Seguridad Digital y protección de los activos de información.

g) Apoyar el fortalecimiento de las capacidades institucionales para la gestión de incidentes de seguridad, la continuidad de la operación, la recuperación ante eventos adversos y la resiliencia organizacional.

h) Realizar seguimiento periódico al desempeño del Modelo de Seguridad y Privacidad de la Información mediante la revisión de indicadores, resultados de auditorías, evaluaciones de riesgos, planes de mejoramiento y demás mecanismos de control establecidos por la entidad.

i) Promover la mejora continua de los procesos, controles y mecanismos de Seguridad de la Información, garantizando su adaptación a los cambios tecnológicos, normativos, organizacionales y al contexto de amenazas que enfrenta la entidad.

La Alta Dirección ratifica su compromiso de apoyar permanentemente las iniciativas orientadas a fortalecer la Seguridad y Privacidad de la Información y la Seguridad Digital,

reconociendo que la protección de la información constituye un factor esencial para la sostenibilidad institucional, la continuidad de la operación y la generación de valor público para la ciudadanía.

10. ROLES Y RESPONSABILIDADES

La gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital requiere la participación coordinada de todas las dependencias, servidores públicos, contratistas, proveedores y demás partes interesadas que interactúan con los activos de información y los recursos tecnológicos del Departamento Administrativo de la Defensoría del Espacio Público – DADEP.

Las responsabilidades generales se establecen de la siguiente manera:

10.1 Alta Dirección

Corresponde a la Alta Dirección:

a) Liderar y respaldar la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI).

b) Aprobar las políticas, lineamientos y estrategias institucionales relacionadas con la Seguridad y Privacidad de la Información y la Seguridad Digital.

c) Promover la integración de la Seguridad y Privacidad de la Información dentro de la gestión institucional y la planeación estratégica.

d) Asignar los recursos necesarios para la implementación y sostenibilidad de los controles de seguridad de la información.

e) Realizar seguimiento periódico al desempeño del MSPI y apoyar la implementación de acciones de mejora.

10.2 Comité Institucional de Gestión y Desempeño (CIGD)

Corresponde al Comité Institucional de Gestión y Desempeño:

a) Aprobar las políticas, planes, estrategias y lineamientos relacionados con la Seguridad y Privacidad de la Información y la Seguridad Digital cuando corresponda.

b) Realizar seguimiento a la implementación del MSPI y a las acciones de fortalecimiento institucional en materia de seguridad de la información.

c) Revisar los resultados de evaluaciones, auditorías, indicadores y planes de mejoramiento relacionados con la Seguridad de la Información.

d) Promover la articulación de la Seguridad y Privacidad de la Información con los demás componentes del Modelo Integrado de Planeación y Gestión (MIPG).

10.3 Oficina de Tecnologías de la Información y las Comunicaciones (OTIC)

Corresponde a la Oficina de Tecnologías de la Información y las Comunicaciones:

a) Implementar y administrar los controles tecnológicos necesarios para la protección de los activos de información y los recursos tecnológicos institucionales.

b) Administrar la infraestructura tecnológica, los servicios tecnológicos, las plataformas institucionales y los mecanismos de seguridad implementados por la entidad.

c) Apoyar la gestión de incidentes de Seguridad y Privacidad de la Información y Seguridad Digital.

d) Apoyar la implementación de los planes, programas y proyectos relacionados con la Seguridad de la Información.

e) Realizar seguimiento técnico a la efectividad de los controles de seguridad implementados.

10.4 Oficial de Seguridad y Privacidad de la Información

Corresponde al Oficial de Seguridad y Privacidad de la Información:

a) Liderar la implementación, mantenimiento, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información.

b) Coordinar la formulación, actualización y divulgación de las políticas, procedimientos, lineamientos y demás documentos relacionados con la Seguridad de la Información.

c) Coordinar la gestión de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.

d) Realizar seguimiento al cumplimiento de los controles y lineamientos establecidos por la entidad.

e) Promover actividades de sensibilización, capacitación y fortalecimiento de la cultura de seguridad.

f) Presentar informes periódicos sobre el estado de la Seguridad y Privacidad de la Información a las instancias de gobierno correspondientes.

10.5 Líderes de Proceso

Corresponde a los líderes de proceso:

a) Identificar y gestionar los riesgos asociados a la información bajo su responsabilidad.

b) Garantizar la aplicación de los lineamientos y controles de Seguridad y Privacidad de la Información dentro de sus procesos.

c) Apoyar la identificación, clasificación y protección de los activos de información de sus dependencias.

d) Participar en la implementación de acciones de mejora relacionadas con la Seguridad de la Información.

10.6 Propietarios de Activos de Información

Corresponde a los propietarios de activos de información:

a) Identificar y clasificar los activos de información bajo su responsabilidad.

b) Determinar los niveles de protección requeridos para los activos de información.

c) Velar por el adecuado uso, acceso, conservación y protección de los activos de información asignados.

d) Reportar oportunamente situaciones que puedan afectar la seguridad de los activos bajo su responsabilidad.

10.7 Servidores Públicos y Contratistas

Corresponde a todos los servidores públicos y contratistas:

a) Cumplir las disposiciones establecidas en la presente política y en los demás documentos que conforman el MSPI.

b) Proteger la información y los recursos tecnológicos a los que tengan acceso.

c) Utilizar adecuadamente los recursos tecnológicos institucionales.

d) Reportar oportunamente eventos o incidentes de Seguridad de la Información.

e) Participar en las actividades de sensibilización y capacitación definidas por la entidad.

10.8 Proveedores, Contratistas Externos y Terceros

Los proveedores, contratistas externos y terceros que tengan acceso a información institucional o recursos tecnológicos deberán:

a) Cumplir los requisitos de Seguridad y Privacidad de la Información establecidos por la entidad.

b) Proteger la confidencialidad, integridad y disponibilidad de la información a la que tengan acceso.

c) Cumplir las obligaciones contractuales relacionadas con la Seguridad de la Información.

d) Reportar oportunamente cualquier evento o incidente de seguridad que pueda afectar los activos de información o los servicios institucionales.

11. SEPARACIÓN DE FUNCIONES

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP implementará mecanismos de separación de funciones, responsabilidades y niveles de autoridad con el fin de reducir los riesgos asociados a errores, fraude, uso indebido de privilegios, conflictos de interés, accesos no autorizados y demás situaciones que puedan afectar la Seguridad y Privacidad de la Información y la Seguridad Digital.

La asignación de funciones y responsabilidades deberá realizarse de manera que ninguna persona tenga control total sobre actividades críticas que puedan comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información institucional.

Para tal efecto, la entidad adoptará los siguientes lineamientos:

a) Las funciones de administración tecnológica, operación, supervisión, control y auditoría deberán mantenerse segregadas cuando la naturaleza del proceso, el nivel de riesgo o las condiciones operativas así lo requieran.

b) Los usuarios responsables de procesos institucionales no deberán administrar los controles tecnológicos que soportan directamente las actividades bajo su responsabilidad, salvo en aquellos casos debidamente autorizados y gestionados mediante controles compensatorios.

c) El personal encargado de la administración de infraestructura tecnológica, sistemas de información, bases de datos, servicios tecnológicos, redes de comunicaciones o servicios en la nube deberá ejercer sus funciones dentro de los niveles de autorización formalmente definidos por la entidad.

d) La asignación de privilegios especiales o elevados deberá realizarse de acuerdo con las funciones y responsabilidades de cada rol, aplicando criterios de necesidad de negocio, mínimo privilegio y segregación de funciones.

e) Los accesos privilegiados deberán ser gestionados mediante procedimientos institucionales que permitan su control, seguimiento, monitoreo y revisión periódica.

f) Las actividades relacionadas con la identificación, valoración y tratamiento de riesgos, así como las actividades de seguimiento, evaluación o auditoría, deberán desarrollarse con independencia funcional respecto de las actividades operativas objeto de evaluación.

g) Los procesos de desarrollo, pruebas, implementación y operación de sistemas de información deberán contar con mecanismos que minimicen los riesgos derivados de accesos no autorizados, modificaciones no controladas o conflictos de funciones.

h) Cuando las condiciones operativas, técnicas o presupuestales no permitan una segregación completa de funciones, la entidad deberá establecer controles compensatorios, mecanismos de supervisión, revisiones periódicas o actividades de monitoreo que permitan gestionar adecuadamente los riesgos identificados.

i) Los líderes de proceso, administradores de plataformas tecnológicas, propietarios de activos de información y demás responsables deberán velar por el cumplimiento de los principios de segregación de funciones definidos por la entidad.

La separación de funciones deberá ser considerada en el diseño de procesos, la administración de accesos, la gestión de usuarios privilegiados, la contratación de servicios tecnológicos, la gestión de cambios, la administración de infraestructura tecnológica y demás actividades que puedan representar riesgos para la Seguridad de la Información.

12. CUMPLIMIENTO NORMATIVO

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP desarrollará la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital en cumplimiento de las disposiciones legales, regulatorias, normativas, contractuales e institucionales aplicables, así como de los lineamientos emitidos por las autoridades competentes en la materia.

La entidad velará por la identificación, análisis, implementación y seguimiento de los requisitos relacionados con la Seguridad de la Información, garantizando su incorporación dentro de los procesos institucionales, los servicios tecnológicos, los proyectos de transformación digital y las actividades que involucren el tratamiento y protección de los activos de información.

Para tal efecto, el DADEP promoverá el cumplimiento de:

a) La Constitución Política de Colombia y demás disposiciones legales relacionadas con la protección de la información, el acceso a la información pública, la seguridad digital, la administración pública y las tecnologías de la información.

b) Las políticas, lineamientos, estándares, guías y demás instrumentos emitidos por el Gobierno Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Alta Consejería Distrital de TIC o las entidades que hagan sus veces.

c) Los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y demás marcos de referencia aplicables a las entidades públicas.

d) Los requisitos establecidos en las normas técnicas, estándares y buenas prácticas adoptadas por la entidad para la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital.

e) Las obligaciones contractuales relacionadas con la protección de la información, la confidencialidad, la prestación de servicios tecnológicos y la gestión de riesgos asociados a terceros.

f) Los procedimientos, políticas, manuales, lineamientos y demás instrumentos internos que conforman el Sistema Integrado de Gestión y el Modelo de Seguridad y Privacidad de la Información de la entidad.

La entidad realizará revisiones periódicas de los requisitos normativos aplicables con el fin de identificar cambios regulatorios, nuevas obligaciones o modificaciones que puedan impactar la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital.

Los servidores públicos, contratistas, proveedores y demás terceros que tengan acceso a la información institucional o a los recursos tecnológicos del DADEP deberán cumplir las

disposiciones legales, regulatorias, contractuales e institucionales aplicables en el desarrollo de sus funciones y actividades.

El incumplimiento de los requisitos establecidos podrá dar lugar a la adopción de acciones correctivas, preventivas, disciplinarias, contractuales, administrativas, civiles o penales, según corresponda y de conformidad con la normatividad vigente.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP establecerá mecanismos para la identificación, reporte, registro, análisis, atención, seguimiento y mejora continua frente a los eventos e incidentes que puedan afectar la Seguridad y Privacidad de la Información y la Seguridad Digital de la entidad.

La gestión de incidentes deberá desarrollarse de manera oportuna, coordinada y documentada, con el propósito de minimizar los impactos sobre los activos de información, los servicios tecnológicos, la infraestructura tecnológica, los procesos institucionales y la prestación de servicios a la ciudadanía.

Todos los servidores públicos, contratistas, proveedores y terceros que identifiquen o tengan conocimiento de eventos o incidentes que puedan comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información institucional deberán reportarlos oportunamente a través de los mecanismos definidos por la entidad.

La entidad promoverá la implementación de procedimientos y controles que permitan:

a) Detectar oportunamente eventos e incidentes de Seguridad y Privacidad de la Información y Seguridad Digital.

b) Gestionar de manera adecuada los incidentes reportados, de acuerdo con su naturaleza, impacto, criticidad y nivel de riesgo.

c) Coordinar las acciones de contención, análisis, respuesta, recuperación y seguimiento necesarias para reducir los efectos derivados de los incidentes de seguridad.

d) Preservar la información requerida para el análisis, investigación y gestión de los incidentes cuando sea aplicable.

e) Identificar las causas que originaron los incidentes y establecer acciones correctivas, preventivas o de mejora orientadas a evitar su recurrencia.

f) Fortalecer la capacidad institucional para responder a eventos que puedan afectar la continuidad de la operación, la prestación de servicios o el cumplimiento de los objetivos institucionales.

g) Generar información que permita la evaluación periódica de tendencias, riesgos emergentes y oportunidades de mejora relacionadas con la Seguridad y Privacidad de la Información y la Seguridad Digital.

La gestión de incidentes deberá articularse con los procesos de gestión de riesgos, continuidad de la operación, gestión de cambios, gestión de proveedores, administración de activos de información y demás procesos institucionales que contribuyan a la protección de la información y los recursos tecnológicos.

La información derivada de los incidentes de Seguridad y Privacidad de la Información será utilizada como insumo para la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), el fortalecimiento de los controles institucionales y el desarrollo de acciones de sensibilización y fortalecimiento de capacidades en materia de Seguridad y Privacidad de la Información y Seguridad Digital.

14. SANCIONES

El incumplimiento de las disposiciones establecidas en la presente Política General de Seguridad de la Información, así como de los procedimientos, lineamientos, estándares y demás instrumentos que conforman el Modelo de Seguridad y Privacidad de la Información (MSPI), podrá dar lugar a la aplicación de las medidas administrativas, disciplinarias, contractuales, fiscales, civiles o penales a que haya lugar, de conformidad con la normatividad vigente y las competencias de las autoridades correspondientes.

Los servidores públicos, contratistas, proveedores y demás terceros que tengan acceso a los activos de información, recursos tecnológicos o servicios institucionales deberán cumplir las responsabilidades y obligaciones definidas por la entidad en materia de Seguridad y Privacidad de la Información y Seguridad Digital.

Las situaciones que evidencien incumplimientos, uso indebido de los recursos tecnológicos, accesos no autorizados, divulgación indebida de información, incumplimiento de acuerdos de confidencialidad, vulneración de controles de seguridad o cualquier otra conducta que pueda afectar la protección de la información institucional deberán ser reportadas y gestionadas conforme a los procedimientos y mecanismos definidos por la entidad.

La determinación de las acciones, medidas o sanciones aplicables se realizará respetando el debido proceso y las disposiciones legales, reglamentarias, contractuales e institucionales que resulten aplicables en cada caso.

La aplicación de medidas derivadas de incumplimientos a la presente política no excluye la adopción de acciones correctivas, preventivas o de mejora orientadas a fortalecer la gestión de la Seguridad y Privacidad de la Información y prevenir la ocurrencia de situaciones similares.

15. SEGUIMIENTO

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP realizará seguimiento permanente a la implementación, cumplimiento y efectividad de la presente Política General de Seguridad de la Información, con el fin de verificar su adecuada aplicación, identificar oportunidades de mejora y fortalecer continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI).

El seguimiento deberá realizarse mediante mecanismos de evaluación, monitoreo y control que permitan determinar el grado de cumplimiento de los objetivos de Seguridad y Privacidad de la Información y Seguridad Digital definidos por la entidad.

Para tal efecto, el DADEP podrá apoyarse en:

a) Indicadores de gestión, resultado y desempeño asociados a la Seguridad y Privacidad de la Información y Seguridad Digital.

b) Seguimiento a los planes de trabajo, programas, proyectos y actividades relacionadas con la implementación y fortalecimiento del Modelo de Seguridad y Privacidad de la Información.

c) Evaluaciones de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.

d) Seguimiento a la implementación y efectividad de controles de seguridad.

e) Resultados derivados de la gestión de eventos e incidentes de Seguridad de la Información.

f) Auditorías internas y externas, evaluaciones independientes, revisiones de cumplimiento y demás mecanismos de verificación establecidos por la entidad.

g) Planes de mejoramiento institucional, acciones correctivas, preventivas y de mejora continua relacionadas con la Seguridad de la Información.

h) Resultados de ejercicios de autoevaluación, autodiagnóstico, medición de madurez y demás instrumentos aplicables al Modelo de Seguridad y Privacidad de la Información.

Los resultados del seguimiento deberán ser analizados periódicamente por las instancias de gobierno y gestión que correspondan, con el fin de identificar desviaciones, definir acciones de mejora y fortalecer la capacidad institucional para la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital.

La información obtenida como resultado de las actividades de seguimiento servirá como insumo para la actualización de políticas, procedimientos, controles, planes de tratamiento de riesgos, programas de capacitación y demás instrumentos que conforman el Modelo de Seguridad y Privacidad de la Información.

La presente política deberá revisarse como mínimo una vez al año o cuando se presenten cambios significativos en el contexto organizacional, la normatividad aplicable, la infraestructura tecnológica, los servicios tecnológicos, los riesgos identificados o cualquier otro factor que pueda impactar la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital de la entidad.

16. IMPLEMENTACIÓN DE LA POLÍTICA

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP implementará la presente Política General de Seguridad y Privacidad de la Información mediante la definición, adopción, mantenimiento y mejora continua de los instrumentos, procesos, procedimientos, controles y mecanismos necesarios para la gestión efectiva de la Seguridad y Privacidad de la Información y la Seguridad Digital.

La implementación de la política se realizará de manera articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI), el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital y los demás instrumentos de gestión institucional aplicables.

Para el cumplimiento de la presente política, la entidad promoverá, entre otras, las siguientes acciones:

a) La identificación, clasificación, valoración y protección de los activos de información institucionales.

b) La gestión de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.

c) La definición e implementación de controles administrativos, técnicos, físicos y organizacionales acordes con los riesgos identificados.

d) El fortalecimiento de las capacidades institucionales mediante actividades de capacitación, sensibilización y apropiación de buenas prácticas de Seguridad de la Información.

e) La gestión de eventos e incidentes de Seguridad y Privacidad de la Información y Seguridad Digital.

f) La protección de la infraestructura tecnológica, los servicios tecnológicos, los servicios en la nube y demás recursos que soportan la operación institucional.

g) La gestión de accesos, identidades digitales y privilegios de acuerdo con las necesidades institucionales y los principios de mínimo privilegio y necesidad de negocio.

h) La gestión de proveedores y terceros que tengan acceso a activos de información o recursos tecnológicos institucionales.

i) La implementación de mecanismos de seguimiento, evaluación, auditoría y mejora continua que permitan fortalecer el desempeño del Modelo de Seguridad y Privacidad de la Información.

j) La definición e implementación de acciones orientadas a fortalecer la continuidad de la operación, la resiliencia institucional y la capacidad de respuesta frente a eventos que puedan afectar la Seguridad y Privacidad de la Información y la Seguridad Digital.

La implementación de la presente política es una responsabilidad compartida entre la Alta Dirección, las dependencias de la entidad, los servidores públicos, contratistas, proveedores y demás partes interesadas, de acuerdo con los roles y responsabilidades definidos por el DADEP.

17. APROBACIÓN DE LA POLÍTICA

La presente Política General de Seguridad y Privacidad de la Información del Departamento Administrativo de la Defensoría del Espacio Público – DADEP ha sido elaborada en el marco de los lineamientos establecidos para la gestión de la Seguridad y Privacidad de la Información y la Seguridad Digital, y forma parte integral del Modelo de Seguridad y Privacidad de la Información (MSPI) de la entidad.

La política será revisada por las instancias competentes y aprobada de conformidad con los mecanismos de gobierno, gestión y control definidos por la entidad para los documentos que conforman el Sistema Integrado de Gestión.

Una vez aprobada, la presente política será divulgada a las partes interesadas correspondientes y será de obligatorio cumplimiento para todos los servidores públicos, contratistas, proveedores y terceros que tengan acceso a los activos de información, recursos tecnológicos o servicios institucionales del DADEP.

La presente política entrará en vigor a partir de la fecha de su aprobación y permanecerá vigente hasta que sea modificada, actualizada o derogada conforme a los procedimientos institucionales establecidos.

Toda actualización, modificación o ajuste a la presente política deberá ser gestionada mediante el procedimiento de control documental definido por la entidad, garantizando su trazabilidad, revisión, aprobación y divulgación correspondiente.

Actualizó: Sandra Marcela Venegas Páez - Contratista
Revisó: Hugo Roberto Hernández Díaz - jefe OTIC.
Aprobó: Hugo Roberto Hernández Díaz - jefe OTIC.

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
7	17/06/2023	Se incluyen los siguientes apartados: Vigencia, Organización Interna, Separación de Roles, Acuerdos de Confidencialidad, Cumplimiento de Obligaciones Legales, Gestión de Incidentes de Privacidad, Derechos de Propiedad Intelectual y redistribución del contenido de los ámbitos de aplicación en el alcance. Así mismo, se actualiza la descripción y responsabilidades asociadas al rol del Oficial de Seguridad y Privacidad de la Información con el fin de fortalecer su participación dentro del marco de gestión de la Seguridad y Privacidad de la Información.
8	3/01/2025	Se actualiza la Política General de Seguridad y Privacidad de la Información mediante la incorporación de la sección "Actividades para la Implementación de la Política", el fortalecimiento de las responsabilidades institucionales en materia de seguridad de la información, la alineación con el formato documental institucional 2024 y la actualización de lineamientos conforme a requisitos normativos, estándares internacionales y objetivos estratégicos de la entidad.
9	12/09/2025	Se incorporan lineamientos relacionados con el control de instalación y uso de software institucional, así como el fortalecimiento de las medidas de administración, custodia y verificación de credenciales y cuentas privilegiadas en cumplimiento de observaciones de control y políticas institucionales de seguridad de la información.
10	05/06/2026	Actualización integral de la Política General de Seguridad y Privacidad de la Información, fortaleciendo su estructura, alcance, roles y responsabilidades, gestión de incidentes, seguimiento y demás lineamientos institucionales, en alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y la norma ISO/IEC 27001:2022.