

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES 2026

Proceso Gestión Jurídica



CÓDIGO SG/MIPG

127-PPPGJ-05

VIGENCIA DESDE

13/02/2026

VERSIÓN

03

Año **2026**



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

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





TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVO GENERAL	4
3. ALCANCE	4
4. DEFINICIONES	4
5. RESPONSABILIDAD DE LIDERAZGO SOBRE PROTECCIÓN DE DATOS PERSONALES.....	6
6. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.....	8
7. TRATAMIENTO Y FINALIDADES DEL TRATAMIENTO DE LOS DATOS PERSONALES	9
8. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES.....	10
9. DEBERES DEL PERSONAL DE TRATAMIENTO DE LOS DATOS PERSONALES.....	11
10. RESPONSABILIDADES DE LA DEFENSORÍA EN CUMPLIMIENTO DE LA POLÍTICA	12
11. OTRAS RESPONSABILIDADES DE LA DEFENSORÍA EN CUMPLIMIENTO DE LA POLÍTICA	13
12. GESTIÓN DE INCIDENTES DE PRIVACIDAD.....	14
13. PROCEDIMIENTOS ADMINISTRATIVOS DEL CENTRO DE CÓMPUTO.....	14
14. SANCIONES POR INCUMPLIMIENTO.....	15
15. VIGENCIA	16
16. ACTUALIZACIÓN.....	16
17. DIVULGACIÓN	17
18. PERIODECIDAD DE VIGENCIA DE LAS BASES DE DATOS	17
19. PLAN DE ACCIÓN DE LA POLÍTICA PÚBLICA.....	17

1. INTRODUCCIÓN

El artículo 15 de la Constitución Política de Colombia consagra el derecho fundamental al habeas data, en virtud del cual todas las personas tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos de entidades públicas o privadas.

En cumplimiento de este mandato, el Departamento Administrativo de la Defensoría del Espacio Público —DADEP—, como entidad pública del orden distrital, se encuentra obligado a garantizar el respeto y la protección de los derechos de los titulares de datos personales, conforme a los principios y disposiciones establecidos en la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1081 de 2015, la jurisprudencia constitucional vigente y las directrices emitidas por la Superintendencia de Industria y Comercio.

Esta Política, elaborada bajo la responsabilidad de la Oficina Jurídica, establece los lineamientos institucionales para el tratamiento de datos personales en el DADEP, teniendo como marco de referencia el principio de responsabilidad demostrada (Accountability), e integra las buenas prácticas contenidas en la Guía expedida por la Superintendencia de Industria y Comercio para entidades públicas, con el fin de promover una cultura organizacional orientada al cumplimiento normativo, la transparencia y la protección efectiva de la información personal.

Todos los colaboradores, contratistas, proveedores y demás partes interesadas que tengan acceso a información personal en el marco de sus relaciones con el DADEP, deberán conocer, aceptar y cumplir los principios establecidos en la presente Política. Esto aplica a quienes interactúen con los sistemas de información de la entidad, así como a quienes accedan a documentación institucional en medios físicos o digitales.

Para reportar un incidente relacionado con la privacidad o el tratamiento inadecuado de los datos personales, los colaboradores pueden elevar la solicitud a través del Sistema de Gestión de Servicios. La ciudadanía podrá hacerlo mediante el canal digital “Ventanilla Virtual”, disponible en el sitio web institucional (<https://www.dadep.gov.co/form/ventanilla-virtual>) o dirigiéndose a la Oficina de Atención al Ciudadano de la entidad.

2. OBJETIVO GENERAL

Establecer y divulgar los lineamientos institucionales para la recolección, almacenamiento, uso, circulación, supresión y demás actividades relacionadas con el tratamiento de datos personales en el Departamento Administrativo de la Defensoría del Espacio Público —DADEP—, con el fin de garantizar a los titulares el pleno ejercicio de sus derechos constitucionales, en cumplimiento de los principios establecidos en la Ley 1581 de 2012 y normas concordantes.

3. ALCANCE

Esta Política se aplica a todos los tratamientos de datos personales efectuados por el DADEP en calidad de responsable y/o encargado, sobre bases de datos y archivos físicos o digitales, que contengan información personal de ciudadanos, servidores públicos, contratistas, proveedores y demás actores relacionados con la Entidad.

Así mismo, será de cumplimiento obligatorio para todos los servidores públicos, contratistas y terceros que, en el marco de una relación contractual o legal, realicen actividades que involucren el tratamiento de datos personales bajo responsabilidad del DADEP

4. DEFINICIONES

Las siguientes definiciones están basadas en el artículo 3 de la Ley 1581 de 2012, el artículo 3 del Decreto 1377 de 2013, el artículo 3 de la Ley 1266 de 2008 (cuando aplica), y la Guía de Protección de Datos Personales para Entidades Públicas expedida por la Superintendencia de Industria y Comercio:

- **Autorización:** consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales.
- **Aviso de privacidad:** comunicación verbal o escrita generada por el responsable del tratamiento, dirigida al titular, mediante la cual se informa la existencia de políticas de tratamiento de información, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Base de datos:** conjunto organizado de datos personales que sea objeto de tratamiento, sin importar el medio en el que se almacenen (físico o digital).

- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** dato que no sea semiprivado, privado o sensible. Son considerados públicos, entre otros, los relativos al estado civil de las personas, a su profesión u oficio, y a su calidad de comerciante o servidor público. Por su naturaleza pueden estar contenidos en registros o documentos públicos, gacetas, boletines oficiales y sentencias ejecutoriadas que no estén sometidas a reserva.
- **Dato privado:** dato que por su naturaleza íntima o reservada solo es relevante para el titular.
- **Dato semiprivado:** información que no tiene naturaleza íntima, reservada ni pública, y cuyo conocimiento o divulgación puede interesar no solo al titular, sino a cierto grupo o a la sociedad. Su tratamiento requiere autorización expresa del titular (ejemplo: información financiera o crediticia).
- **Dato sensible:** información que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación. Incluye, entre otros, los datos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos u organizaciones sociales, los datos de salud, vida sexual y datos biométricos.
- **Encargado del tratamiento:** persona natural o jurídica, pública o privada, que realice el tratamiento de datos personales por cuenta del responsable.
- **Fuente de información (aplicable en el marco de la Ley 1266 de 2008):** persona, entidad u organización que suministra datos personales a un operador de información, en virtud de una relación contractual, comercial o legal, principalmente en contextos financieros o crediticios.
- **Responsable del tratamiento:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos personales.
- **Sistema de información:** sistema organizado para recolectar, filtrar, procesar, crear, almacenar y distribuir datos, dentro de procesos que incluyan tecnologías de la información y las comunicaciones – TIC.
- **Titular:** persona natural cuyos datos personales sean objeto de tratamiento.

- **Transferencia:** envío de datos personales a un receptor que se encuentra dentro o fuera del país, cuando quien transfiere actúa como responsable o encargado del tratamiento.
- **Transmisión:** tratamiento de datos personales que implica su comunicación dentro o fuera del territorio colombiano, cuando tenga por objeto la realización de un tratamiento por un tercero en calidad de encargado por cuenta del responsable.
- **Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales, como la recolección, almacenamiento, uso, circulación o supresión.

Igualmente, se adoptan los términos y definiciones de la familia de normas técnica ISO 27000 vigentes y de los estándares que se apliquen de acuerdo con el alcance de las políticas.

5. RESPONSABILIDAD DE LIDERAZGO SOBRE PROTECCIÓN DE DATOS PERSONALES

La Oficina Jurídica del Departamento Administrativo de la Defensoría del Espacio Público — DADEP— será la dependencia responsable de liderar y coordinar la implementación, mantenimiento y mejora continua de la presente Política de Protección de Datos Personales, en cumplimiento del principio de responsabilidad demostrada (accountability) y conforme a lo dispuesto en la Ley 1581 de 2012, sus decretos reglamentarios y demás disposiciones aplicables.

En este marco, la Oficina Jurídica asumirá, entre otras, las siguientes responsabilidades:

- Promover la cultura institucional de protección de datos personales al interior de la Entidad.
- Emitir directrices jurídicas e interpretar las disposiciones normativas relacionadas con el tratamiento de datos personales.
- Articular con las dependencias responsables el diseño e implementación de controles técnicos, administrativos y jurídicos que garanticen la protección efectiva de los datos personales.
- Coordinar, en conjunto con la Oficina de Tecnologías de la Información y las Comunicaciones —OTIC—, la gestión de incidentes de seguridad de la información que involucren datos personales.
- Acompañar los procesos de respuesta a derechos de los titulares y solicitudes elevadas ante la Superintendencia de Industria y Comercio, en materia de protección de datos.

- Apoyar el diseño y actualización de los avisos de privacidad, cláusulas contractuales y demás instrumentos jurídicos necesarios para el cumplimiento normativo.
- Realizar seguimiento a la implementación de la política y de los procedimientos relacionados, en el marco de los planes institucionales y el Modelo Integrado de Planeación y Gestión —MIPG—.

Todas las dependencias de la Entidad, en el marco de sus funciones, deberán apoyar el cumplimiento de esta política y adoptar las medidas que sean necesarias para garantizar el tratamiento adecuado de los datos personales bajo su responsabilidad o custodia.

A continuación, se presenta un resumen de los roles y responsabilidades asignadas frente al tratamiento de datos personales, en el marco de la presente política:

Tabla 1. Roles y responsabilidades en la protección de datos personales

Rol o cargo	Responsabilidad frente a los datos personales
Oficina Jurídica	Liderar la implementación, actualización y socialización de esta política. Emitir conceptos jurídicos relacionados con el tratamiento de datos personales, y apoyar la resolución de consultas y conflictos sobre el tema.
Oficial de Protección de Datos Personales (OPDP)	Coordinar la implementación del principio de responsabilidad demostrada (accountability), articular la gestión de riesgos, promover buenas prácticas y atender peticiones de titulares.
Jefes de área	Garantizar que los procesos y procedimientos bajo su responsabilidad cumplan con esta política y con la normativa vigente sobre protección de datos personales.
Oficina TIC (OTIC)	Implementar y mantener controles técnicos y medidas de seguridad en los sistemas de información que almacenan o tratan datos personales.
Contratistas y proveedores	Cumplir con los acuerdos de confidencialidad y cláusulas contractuales sobre tratamiento de datos. Ejecutar actividades conforme a los lineamientos del DADEP.
Todos los servidores públicos	Conocer y aplicar esta política. Evitar el uso indebido, la divulgación o el tratamiento inadecuado de datos personales. Reportar incidentes al Oficial de Protección de Datos Personales -OPDP.

Esta tabla puede ser actualizada en función de los cambios organizacionales o normativos vigentes.

6. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

En el desarrollo, interpretación y aplicación de la presente política, se observarán los siguientes principios rectores, conforme a lo establecido en la Ley Estatutaria 1581 de 2012 y demás normas concordantes:

- **Principio de legalidad:** el tratamiento de datos personales es una actividad reglada que debe sujetarse a lo dispuesto en la ley y demás disposiciones que la desarrollen.
- **Principio de finalidad:** el tratamiento debe obedecer a una finalidad legítima, la cual debe ser informada de manera previa, clara y expresa al titular de los datos personales.
- **Principio de libertad:** El tratamiento solo puede llevarse a cabo con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos ni divulgados sin autorización, salvo en los casos expresamente previstos por la ley.
- **Principio de veracidad o calidad:** La información objeto de tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe expresamente el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de transparencia:** En todo momento debe garantizarse al titular el derecho a obtener del responsable del tratamiento, información clara y suficiente respecto del uso que se da a sus datos personales.
- **Principio de acceso y circulación restringida:** Los datos personales únicamente podrán ser accedidos por las personas autorizadas por el titular o por quienes estén facultados legalmente. Salvo la información pública, los datos personales no podrán estar disponibles en medios masivos de comunicación o divulgación, salvo que el acceso sea técnicamente controlable y garantice un conocimiento restringido.
- **Principio de seguridad:** La información sujeta a tratamiento deberá ser manejada con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, con el fin de prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, incluso después de finalizada su relación con alguna de las labores que comprenden el tratamiento.

Estos principios se aplican de manera transversal y obligatoria en todos los procesos, procedimientos y actividades institucionales en los cuales se efectúe tratamiento de datos personales, y deben ser observados por todos los servidores públicos, contratistas y terceros que intervengan en dicha gestión, bajo el liderazgo de la Oficina Jurídica como responsable del diseño, seguimiento y actualización de esta política.

7. TRATAMIENTO Y FINALIDADES DEL TRATAMIENTO DE LOS DATOS PERSONALES

El Departamento Administrativo de la Defensoría del Espacio Público —DADEP—, en su calidad de responsable del tratamiento de datos personales, recolecta, almacena, utiliza, circula, transmite, transfiere, suprime y, en general, realiza cualquier operación o conjunto de operaciones sobre datos personales de conformidad con los principios, deberes y obligaciones consagrados en el régimen legal vigente.

Los datos personales serán tratados exclusivamente para las finalidades legítimas y necesarias en el ejercicio de las funciones legales y misionales asignadas al DADEP, conforme a su marco normativo, entre ellas:

- Gestionar trámites, servicios, solicitudes, peticiones, quejas, reclamos y denuncias (PQRD) presentadas por la ciudadanía.
- Realizar procesos de contratación, selección y vinculación de servidores públicos o contratistas, así como gestionar la ejecución contractual y el control disciplinario.
- Efectuar el registro y control de ingreso a las instalaciones físicas y/o a los sistemas tecnológicos de información institucionales.
- Desarrollar actividades propias de los procesos de planeación, estadística, evaluación de políticas, formulación de indicadores y control de gestión institucional.
- Ejecutar actividades relacionadas con la administración de bienes inmuebles del espacio público, procesos de recuperación, legalización, inspección y vigilancia.
- Adelantar acciones de comunicación institucional, divulgación de actividades y gestión documental.

- Atender requerimientos de organismos de control y autoridades judiciales o administrativas en ejercicio de sus competencias.
- Cumplir con los principios de publicidad, transparencia y acceso a la información pública conforme al marco legal aplicable.

El tratamiento de datos personales se realizará con estricta observancia de los derechos fundamentales de los titulares y bajo medidas adecuadas de seguridad, confidencialidad y custodia. En todos los casos, el tratamiento obedecerá a una finalidad legítima y será informado previamente al titular, salvo las excepciones previstas en la ley.

8. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

De conformidad con lo establecido en la ley 1581 de 2012, el Decreto 1377 de 2013, y demás normas que regulan la materia, el Departamento Administrativo de la Defensoría del Espacio Público —DADEP— garantiza a los titulares de los datos personales los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente al DADEP, en su condición de responsable del tratamiento.
- Solicitar prueba de la autorización otorgada al DADEP, salvo cuando no sea requerida conforme a la Ley.
- Ser informado, previa solicitud, respecto del uso que se ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la normatividad vigente en materia de protección de datos.
- Revocar la autorización y/o solicitar la supresión de sus datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento por parte del DADEP.

El ejercicio de estos derechos podrá realizarse por el titular, su representante legal o sus causahabientes, a través de los canales de atención habilitados por la entidad, ya sea de manera presencial, electrónica o escrita, conforme con el procedimiento dispuesto en el numeral 11 de la presente política. Para tal fin, deberá presentarse solicitud con la debida identificación del titular y, cuando aplique, la acreditación de la calidad en la que actúa el solicitante, indicando con claridad el derecho que se desea ejercer.

9. DEBERES DEL PERSONAL DE TRATAMIENTO DE LOS DATOS PERSONALES

Todo funcionario, contratista o tercero que, en el ejercicio de sus funciones o actividades, tenga acceso a datos personales tratados por el DADEP, deberá cumplir con los siguientes deberes, sin perjuicio de las disposiciones legales aplicables:

- Garantizar al titular el pleno y efectivo ejercicio del derecho de habeas data, en los términos previstos en la ley.
- Conservar la información bajo condiciones de seguridad, protegiéndola contra pérdida, alteración, acceso no autorizado o uso indebido, conforme a los protocolos establecidos por la Entidad.
- Tratar los datos personales conforme a los principios establecidos en la Ley 1581 de 2012 y demás normas aplicables, así como los lineamientos definidos en esta Política.
- Actualizar la información cuando sea necesario, comunicando oportunamente cualquier novedad al área competente para garantizar la integridad y veracidad de los datos.
- Rectificar la información cuando sea incorrecta o incompleta, a solicitud del titular o por verificación interna.
- Abstenerse de circular información que esté siendo controvertida por el titular, o cuya supresión haya sido solicitada, cuando no exista autorización legal para continuar con el tratamiento.
- Evitar el acceso no autorizado y el uso indebido de los datos personales, aplicando las medidas de seguridad físicas, técnicas y administrativas establecidas por el DADEP.

- Informar al área jurídica o al Oficial de Protección de Datos Personales sobre cualquier incidente de seguridad relacionado con el tratamiento de datos personales.
- Guardar confidencialidad respecto a la información personal tratada, incluso después de finalizada su relación contractual o laboral con la Entidad

10. RESPONSABILIDADES DE LA DEFENSORÍA EN CUMPLIMIENTO DE LA POLÍTICA

El departamento Administrativo de la Defensoría del Espacio Público —DADEP—, como responsable del tratamiento de datos personales, se compromete a garantizar el cumplimiento de las disposiciones contenidas en la presente política, y asume las siguientes responsabilidades institucionales:

- Designar un Oficial de Protección de Datos Personales (OPDP) dentro de la Oficina Jurídica, con el fin de supervisar la implementación, seguimiento y mejora continua de esta política, en cumplimiento del principio de responsabilidad demostrada (accountability).
- Adoptar medidas administrativas, jurídicas, organizacionales y técnicas necesarias para garantizar la seguridad y confidencialidad de los datos personales tratados por la entidad.
- Garantizar el ejercicio pleno de los derechos de los titulares de la información, disponiendo de canales accesibles, procedimientos claros y personal capacitado para la atención de consultas, reclamos o solicitudes de supresión o actualización.
- Promover la formación y sensibilización del personal de planta y contratistas, respecto de las obligaciones y buenas prácticas en el tratamiento de datos personales.
- Revisar y actualizar esta política de forma periódica, o cuando se presenten cambios normativos, tecnológicos o institucionales que lo ameriten.
- Implementar controles de cumplimiento normativo mediante auditorías internas, seguimiento de incidentes y acciones de mejora, para asegurar el respeto de los derechos de los titulares.

- Velar por la confidencialidad, integridad y disponibilidad de la información personal, tanto en formato físico como digital, durante todas las etapas del ciclo de vida de los datos.

11. OTRAS RESPONSABILIDADES DE LA DEFENSORÍA EN CUMPLIMIENTO DE LA POLÍTICA

Además de las responsabilidades enunciadas en el numeral anterior, el DADEP asume las siguientes obligaciones complementarias para asegurar la aplicación efectiva de esta política y la protección de los datos personales tratados por la entidad:

- Incluir cláusulas de protección de datos personales en los contratos que suscriba con terceros que, en desarrollo de sus actividades, accedan, almacenen, procesen o traten datos personales por cuenta del DADEP.
- Implementar controles en los procesos de gestión documental y archivo, asegurando que los documentos que contienen datos personales sean tratados conforme a los principios de seguridad, confidencialidad y conservación, de acuerdo con la normativa archivística vigente.
- Incorporar la política de protección de datos personales en los procesos institucionales, procedimientos internos, sistemas de información, y demás componentes del Modelo Integrado de Planeación y Gestión —MIPG—, para garantizar su transversalidad en la operación de la entidad.
- Revisar los registros de actividades de tratamiento de datos personales, con el fin de asegurar su actualización, coherencia y alineación con lo dispuesto en la Ley 1581 de 2012 y la guía de la Superintendencia de Industria y Comercio.
- Articular con la Alta Consejería Distrital TIC y otras instancias competentes del Distrito Capital, acciones para fortalecer el cumplimiento del régimen de protección de datos personales en el marco del Modelo de Seguridad y Privacidad de la Información —MSPI— y las normas de gobierno digital.

12.GESTIÓN DE INCIDENTES DE PRIVACIDAD

El Departamento Administrativo de la Defensoría del Espacio Público —DADEP— reconoce que la gestión adecuada de los incidentes de privacidad es fundamental para garantizar la protección efectiva de los datos personales bajo su custodia y mitigar los riesgos asociados a accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas de información.

Por lo anterior, la Entidad adoptará procedimientos internos para:

- Detectar, reportar y documentar oportunamente cualquier incidente que afecte la confidencialidad, integridad o disponibilidad de los datos personales tratados por el DADEP.
- Notificar a la Superintendencia de Industria y Comercio, dentro de los términos establecidos en la normativa vigente, aquellos incidentes de seguridad que puedan comprometer de forma significativa los derechos de los titulares de la información.
- Realizar análisis de causa raíz y planes de mejora, con el fin de prevenir la repetición de eventos similares y fortalecer los controles institucionales.
- Mantener un registro actualizado de incidentes de privacidad, que permita evidenciar la trazabilidad de las acciones tomadas y la responsabilidad demostrada (accountability) de la entidad.

Todo incidente deberá ser atendido de manera coordinada entre las dependencias responsables del tratamiento de datos personales, la Oficina Jurídica, la Oficina de Tecnologías de la Información y las demás áreas que correspondan según la naturaleza del evento.

13.PROCEDIMIENTOS ADMINISTRATIVOS DEL CENTRO DE CÓMPUTO

La protección de los datos personales en el Departamento Administrativo de la Defensoría del Espacio Público -DADEP- también exige la implementación de procedimientos administrativos y técnicos adecuados en los entornos donde se alojan, procesan o resguardan estos datos.

En este sentido, el DADEP establecerá lineamientos específicos en los procedimientos del centro de cómputo que incluyan, pero no se limiten a:

- Control de acceso físico a las áreas donde se encuentran los servidores, bases de datos o cualquier infraestructura crítica que soporte el tratamiento de datos personales.
- Gestión segura del almacenamiento y respaldo de información, garantizando la disponibilidad y la integridad de los datos personales frente a fallos técnicos o eventos adversos.
- Manejo adecuado de soportes físicos y digitales, asegurando su custodia, transporte, reutilización y eliminación conforme a políticas de seguridad y privacidad de la información.
- Registro y monitoreo de actividades administrativas y operativas relacionadas con el procesamiento de datos personales, con el fin de mantener trazabilidad y detectar posibles vulnerabilidades o anomalías.

Estos procedimientos deberán ser revisados periódicamente y estar alineados con las Políticas de Seguridad de la Información adoptadas por la Entidad, así como con las directrices de la Superintendencia de Industria y Comercio y las mejores prácticas en la gestión de activos tecnológicos.

14.SANCIONES POR INCUMPLIMIENTO

El incumplimiento de los lineamientos establecidos en la presente Política de Protección de Datos Personales, así como de las disposiciones legales y reglamentarias que regulan la materia, dará lugar a la aplicación de las sanciones disciplinarias, contractuales, administrativas o legales que correspondan, conforme al régimen aplicable a los servidores públicos y contratistas del Departamento Administrativo de la Defensoría del Espacio Público —DADEP—.

Las conductas susceptibles de sanción incluyen, entre otras:

- El tratamiento de datos personales sin autorización del titular, cuando esta sea requerida.
- La omisión en la implementación de medidas de seguridad técnicas, humanas o administrativas necesarias para proteger los datos personales.

- La vulneración de los principios rectores del tratamiento establecidos en la Ley 1581 de 2012.
- La divulgación no autorizada de información personal o el acceso indebido a bases de datos.
- El incumplimiento de los procedimientos internos establecidos para garantizar el ejercicio de los derechos de los titulares.
- En todos los casos, el DADEP actuará conforme al debido proceso y a lo estipulado en el Código Disciplinario Único, en las normas contractuales aplicables o en cualquier otra disposición legal vigente

15.VIGENCIA

La presente Política de Protección de Datos Personales rige a partir de su publicación en la página Web Institucional del Departamento Administrativo de la Defensoría del Espacio Público -DADEP- y deroga todas aquellas disposiciones internas que le sean contrarias.

Su revisión y actualización se realizará por parte del Oficial de Protección de Datos Personales, designado en el área jurídica, de manera periódica o cuando se presenten cambios normativos, tecnológicos, organizacionales o de cualquier índole que lo ameriten, con el fin de garantizar su eficacia y alineación con las disposiciones legales vigentes.

16.ACTUALIZACIÓN

La presente política será revisada y actualizada cuando se presenten cambios normativos, jurisprudenciales, institucionales o tecnológicos que lo requieran, o cuando así lo determine la Oficina Jurídica en coordinación con el Oficial de Protección de Datos Personales.

Las versiones actualizadas serán debidamente publicadas en los medios oficiales del Departamento Administrativo de la Defensoría del Espacio Público —DADEP—, asegurando su divulgación a todos los funcionarios, contratistas y terceros vinculados con el tratamiento de datos personales en la entidad.

17.DIVULGACIÓN

Con el fin de garantizar la transparencia institucional y el cumplimiento del principio de divulgación contemplado en la normativa de protección de datos personales, la presente Política de Protección de Datos Personales será publicada en el sitio web oficial del Departamento Administrativo de la Defensoría del Espacio Público —DADEP—, así como en los medios internos que aseguren su conocimiento por parte de los servidores públicos, contratistas y terceros relacionados.

18.PERIORIZACIÓN DE VIGENCIA DE LAS BASES DE DATOS

El Departamento administrativo de la Defensoría del Espacio Público —DADEP—, a través del(a) Oficial de Protección de Datos Personales y las áreas responsables del tratamiento, revisará periódicamente las bases de datos personales bajo su custodia, con el fin de verificar su vigencia, pertinencia y necesidad conforme a las finalidades previamente autorizadas.

Las bases de datos se mantendrán activas únicamente mientras subsista la finalidad que justificó su recolección y tratamiento. Una vez dicha finalidad se haya cumplido o extinguido, o cuando el término legal de conservación haya expirado, los datos deberán ser eliminados, anonimizados o archivados conforme a lo establecido en la normatividad vigente sobre protección de datos personales, archivo y gestión documental.

Esta revisión se realizará al menos una vez al año, y su resultado deberá documentarse como parte de las acciones de mejora continua y cumplimiento de la presente política.

19.PLAN DE ACCIÓN DE LA POLÍTICA PÚBLICA

Con el fin de garantizar la implementación efectiva de la presente política, el Departamento Administrativo de la Defensoría del Espacio Público —DADEP— definirá anualmente un plan de acción con actividades orientadas a promover la protección de datos personales, el cumplimiento normativo y el fortalecimiento de la cultura institucional en esta materia.

A continuación, se presenta un ejemplo de plan de acción, el cual podrá ser ajustado y aprobado según lo determine la Oficina Jurídica o el Comité Institucional correspondiente:

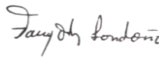
Tabla 2. Plan de Acción para la Implementación y Seguimiento de la Política de Protección de Datos Personales

Actividad	Responsable	Periodicidad	observaciones
Socialización de la política al interior del DADEP	Oficina Jurídica / Talento Humano/ OTIC	Anual o cuando se actualice la política	A través de jornadas de sensibilización y medios institucionales
Actualización del inventario de bases de datos personales	Oficina Jurídica / Responsables del tratamiento	Anual	Según el ciclo de gestión documental y revisión de registros
Verificación del cumplimiento de los principios y deberes del tratamiento	Oficina Jurídica	Semestral	A través de informes de revisión o auditorías internas
Atención de peticiones, quejas o reclamos relacionados con datos personales	Oficina Jurídica / OPDP	Permanente	Aplicando el procedimiento vigente de habeas data
Evaluación y actualización de la política	Oficina Jurídica / OPDP	Anual o cuando se modifique la normatividad	Requiere validación por la instancia directiva correspondiente

Este plan deberá articularse con los demás instrumentos institucionales de planeación, gestión de la información y control interno, conforme a las disposiciones legales vigentes.

Actualizó:

Fanny Ortiz Londoño - Oficial de Protección de Datos Personales
Sandra Marcela Venegas Páez – Oficial de Seguridad de la Información OTIC




Revisó:

Geovanny Andrés Cárdenas Mogollón, Jefe Oficina Jurídica
Hugo Roberto Hernández Jefe Oficina OTIC




Aprobó:

Geovanny Andrés Cárdenas Mogollón, Jefe Oficina Jurídica





CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
1	16/01/2019	Versión inicial del documento.
2	26/04/2023	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, Redistribución del contenido de los Ámbitos de Aplicación en el Alcance y se actualizó formato. Se adicionan los Planes de Acción y el cargo del Oficial de Tratamiento de Datos Personales. Se especifican los roles de los Oficiales de Seguridad de la Información y del Oficial de Tratamiento de Datos Personales, se actualizo los deberes del responsable del tratamiento de los datos personales
3	13/02/2026	Versión actualizada de la política. Se incorporaron nuevos lineamientos conforme al MSPI, se ajustaron roles y responsabilidades institucionales, se incluyó el Plan de Acción y se fortalecieron los apartados sobre tratamiento, derechos y gestión de incidentes de privacidad