

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proceso gestión de la
tecnología y la información



Año **2025**

Código SG/MIPG
Vigencia desde
Versión

127-PPGI-01
12/09/2025
9



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

BOGOTÁ



Tabla de Contenido

1. INTRODUCCIÓN.....	3
2. OBJETIVO	4
3. ALCANCE.....	4
4. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN	4
5. DEFINICIONES	5
6. RESPONSABLE DEL TRATAMIENTO.....	6
7. ORGANIZACIÓN INTERNA.....	7
8. SEPARACIÓN DE ROLES	7
9. ACUERDOS DE CONFIDENCIALIDAD.....	9
10. CUMPLIMIENTO DE OBLIGACIONES LEGALES	10
11. DERECHOS DE PROPIEDAD INTELECTUAL.....	10
12. CONTROL DE INSTALACIÓN Y USO DE SOFTWARE.....	11
13. GESTIÓN DE INCIDENTES DE PRIVACIDAD	12
14. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES:.....	14



1. INTRODUCCIÓN

La presente política obedece al mandato legal contenido en la ley 1581 de 2012 y el Decreto reglamentarios 1074 de 2015, en cuanto el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías frente a la metería, que desarrolle la Ley y la Constitución Política de Colombia.

La presente Política forma parte integral del modelo de Privacidad y Seguridad de la Información y es expedida por parte de la Defensoría del Espacio Público, en adelante el DADEP, entidad constituida como un Departamento Administrativo de la Administración Central perteneciente al Sector Gobierno de la Administración Distrital, e incorpora los controles para el Tratamiento de Datos Personales implementados a través de los procesos, políticas y directrices institucionales.

Las políticas de seguridad y privacidad de la Información deberán ser conocidas, aceptadas y cumplidas por todos los colaboradores, contratistas, proveedores y demás partes interesadas o con relaciones con el DADEP, que tengan interacción con la plataforma tecnológica y sistemas de Información, o de manera física en sus instalaciones y que entren en contacto con la documentación de la Entidad.

Para reportar un evento sospechoso o un incidente de seguridad o de privacidad de la información relacionado con las políticas aquí detalladas, los colaboradores de la Entidad pueden abrir el caso correspondiente en el Sistema de Atención de Incidentes y para la ciudadanía, a través de nuestra oficina de Atención al Ciudadano.

2. OBJETIVO

Establecer y divulgar los lineamientos para la protección de los datos personales recopilados por parte de la Defensoría del Espacio, que permitan garantizar a los titulares su derecho constitucional a conocer, actualizar y rectificar la información que se encuentre registrada en la entidad.

3. ALCANCE

La Política de Tratamiento y Protección de Datos Personales, se aplicará a todas las áreas y los aspectos administrativos, operativos, técnicos, tecnológicos y de control que deben ser cumplidas por todos los colaboradores, personal de planta y contratistas y demás entidades públicas y privadas, así como ciudadanos y demás partes interesadas.

Así mismo, La Política de Tratamiento y Protección de Datos Personales, se aplicará a todas las Bases de Datos y/o Archivos digitales y/o físicos que contengan datos personales y que sean objeto de tratamiento por parte del DADEP, considerado como responsable y/o encargado del tratamiento de los datos personales.

4. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN

La vigencia de la Política de Tratamiento de Datos Personales aplica a partir de su aprobación por la Alta Dirección del DADEP y su publicación en el Sistema Integrado de Gestión y en el sitio web institucional y su actualización deberá hacerse al menos una vez al año o cuando se den alguna (s) de las siguientes condiciones:

- Acceso a la información de formatos físicos o digitales.
- Ingreso físico a las instalaciones del DADEP o lógico, a través de cualquiera de los canales digitales a la plataforma tecnológica de la Entidad.
- Uso de equipos informáticos y de telecomunicaciones de la plataforma tecnológica.
- Uso de los servicios informáticos dispuestos por la entidad a través de los canales digitales.
- Diseño, construcción, pruebas, implementación o uso de herramientas tecnológicas o servicios informáticos dispuestos por la entidad para el desarrollo de sus funciones.
- Y cualquier otro cambio que afecte o impacte en la seguridad y privacidad de la información del Ministerio.

5. DEFINICIONES

Las siguientes definiciones están basadas en el artículo 3 de la Ley 1581 de 2012, el artículo 3 del decreto 1377 de 2013, por el cual se reglamenta parcialmente esta Ley y el artículo 3 de la Ley 1266 de 2008:

- a) Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales.
- b) Aviso de Privacidad: comunicación verbal o escrita generada por el responsable dirigido al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- c) Base de Datos: conjunto organizado de datos personales que sea objeto de Tratamiento.
- d) Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- e) Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- f) Dato semiprivado: son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información (ejemplo: dato financiero y crediticio).
- g) Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- h) Datos sensible: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- i) Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- j) Fuente de Información: es la persona, entidad u organización que recibe o conoce datos personales del Titular, en virtud de una relación comercial o de servicio o de cualquier otra índole y que en razón de autorización legal suministra sus datos a un operador de información, el que a su vez lo entregará al usuario final.
- k) 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.
- l) Sistema de información: es cualquier sistema organizado para recopilar, filtrar, procesar, crear, almacenar y distribuir datos que son utilizados para estrategias de negocio, toma de decisiones entre otros, donde se incluye las tecnologías de la información y las comunicaciones-TIC.
- m) Titular: persona natural cuyos datos personales sean objeto de Tratamiento.
- n) Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- o) Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- p) Transmisión: tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

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 al alcance de las políticas.

6. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de los datos personales regulados por medio de la presente política la Defensoría del Espacio Público – DADEP.

Datos de identificación del responsable del tratamiento:

Nombre: Departamento Administrativo de la Defensoría del Espacio Público Dirección: Avenida Carrera 30 No. 25 – 90 piso 15

Teléfono: (57+1) 382 2510.



Atención al usuario: (57+1) 3507062 | Línea gratuita 018000127700 | Línea 195
Correo electrónico: dadepbogota@dadep.gov.co
Página Web: www.dadep.gov.co

7. ORGANIZACIÓN INTERNA

Los usuarios de los servicios de tecnología, así como los colaboradores que tengan acceso a cualquier tipo de Activo de Información de la Entidad, en formato físico o digital, son responsables de la aplicación de la Política de Seguridad y Privacidad de la Información.

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC- es responsable del Gobierno de las Tecnologías de la Información, de la seguridad informática, seguridad y privacidad de la información y aseguramiento de la infraestructura tecnológica.

El Comité Institucional de Gestión y Desempeño (CIGD) es el encargado de asegurar la aprobación, implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

8. SEPARACIÓN DE ROLES

Se establece la separación de roles, responsabilidades y niveles de autoridad para todos los colaboradores, personal de planta y contratistas, con el fin de dar cabal cumplimiento a las buenas prácticas de Seguridad y Privacidad de la información. Conforme con las funciones y competencias laborales de cada quien, se debe dar cumplimiento a los siguientes lineamientos:

- Los colaboradores de la Entidad que realizan labores funcionales (usuarios de los sistemas) en los sistemas de información de la Entidad, no pueden tener a su cargo labores de administración sobre la plataforma tecnológica (sobre activos como sistemas operativos, bases de datos, programas de aplicación, software de comunicaciones, utilitarios entre otros) que sirven de soporte a la plataforma de TI.
- Los colaboradores de la Oficina de Tecnologías de la Información y las Comunicaciones -OTIC- contratistas o personal de planta, no tendrán poder de decisión sobre los datos que se procesan en los sistemas de información de la entidad ya que esta autoridad se le confiere a cada dueño de proceso.
- La administración de credenciales y cuentas privilegiadas se realizará mediante mecanismos institucionales de custodia y verificación, en concordancia con las políticas operativas específicas de seguridad y con los estándares y lineamientos nacionales aplicables.

- El personal contratista y proveedor de servicios de tecnologías de información y comunicación, solo tendrá acceso a la plataforma tecnológica de la Entidad en el marco de su objeto contractual.

Así mismo, se establece de manera independiente los roles y responsabilidades del Oficial de Seguridad y Privacidad de la Información, quien tendrá a su cargo la gestión de las Políticas de Seguridad y Privacidad de la Información descritas en el documento de Políticas Específicas, y del Oficial de Protección de datos Personales cuyas funciones están incluidas en la Política de Tratamiento de Datos Personales.

ORGANIZACIÓN INTERNA

La implementación de la Política General de Seguridad y Privacidad de la Información requiere la participación de diferentes áreas y roles dentro de la entidad. A continuación, se describen las principales responsabilidades:

1. Alta Dirección:

- Proveer los recursos necesarios (humanos, tecnológicos y financieros) para la implementación, mantenimiento y mejora de la política.
- Revisar y aprobar las actualizaciones de la política, asegurando su alineación con los objetivos estratégicos y las normativas legales aplicables.
- Fomentar una cultura organizacional orientada a la seguridad y privacidad de la información.

2. Oficina de Tecnologías de la Información y las Comunicaciones (OTIC):

- Gestionar la implementación y monitoreo de los controles tecnológicos descritos en la política.
- Administrar los activos tecnológicos, garantizando su protección y disponibilidad.
- Desactivar las cuentas de correo electrónico de los funcionarios y contratistas al finalizar su vinculación, reactivarlas con autorización formal, y configurar mensajes automáticos en cuentas inactivas.
- Coordinar la gestión de incidentes de seguridad y privacidad, incluyendo su registro, análisis y resolución.

3. Oficina Asesora Jurídica:

- Garantizar que la política cumpla con las normativas legales aplicables, especialmente en lo relacionado con la protección de datos personales.
- Incluir cláusulas de confidencialidad en contratos con proveedores y contratistas, supervisando su cumplimiento.

4. Subdirección de Gestión Corporativa:

- Diseñar y ejecutar programas de capacitación y sensibilización sobre la política para funcionarios, contratistas y terceros relevantes.
- Monitorear el cumplimiento de las políticas de seguridad y privacidad en los procesos administrativos.

5. Oficina de Control Interno:

- Realizar auditorías periódicas para evaluar el cumplimiento de la política.
- Identificar y proponer mejoras en los controles de seguridad y privacidad implementados.

6. Todos los funcionarios y Contratistas:

- Cumplir con los lineamientos de la política y los procedimientos establecidos.
- Reportar de manera inmediata cualquier incidente de seguridad o vulnerabilidad detectada.

7. Comité Institucional de Gestión y Desempeño (CIGD):

- Aprobar y supervisar la implementación de los planes relacionados con la política.
- Monitorear los indicadores de desempeño asociados a la seguridad y privacidad de la información.

Cada área y rol deberá coordinar sus actividades con las dependencias relacionadas, asegurando un enfoque integral en la implementación de la política.

9. ACUERDOS DE CONFIDENCIALIDAD

Todos los contratos de la Entidad, tanto con proveedores como con contratistas, deberán especificar las cláusulas de confidencialidad correspondientes o la suscripción de acuerdos de confidencialidad para el manejo adecuado de la información a la que tendrá acceso el contratista o proveedor durante la ejecución del contrato.

10. CUMPLIMIENTO DE OBLIGACIONES LEGALES

El DADEP dará cumplimiento a las normas y regulaciones vigentes relacionadas con los siguientes aspectos:

- Tratamiento de datos personales en todos los procesos de la Entidad, bien sea en entornos de información y comunicación institucional y tecnológico, que involucren datos personales sensibles, privados, semiprivados y públicos.
- La salvaguarda en los contratos y convenios mediante la suscripción de compromisos o acuerdos de confidencialidad sobre el manejo de la información institucional o de datos personales en cualquiera de sus formas.
- El uso de licencias de productos de software adquiridos con terceros y en los productos de software desarrollados al interior de la Entidad.
- El uso y publicación de documentos de todo tipo (textos, imágenes, videos, etc.) en formato físico o digital creados en la entidad, así como los otorgados por terceros que se requieran para documentar las actividades de la misión institucional.

11. DERECHOS DE PROPIEDAD INTELECTUAL

En cumplimiento de la legislación vigente de propiedad intelectual emitidas por la Dirección Nacional de Derechos de Autor, relacionadas con el uso de software, material filmico, fotográfico, de audio o de derechos conexos, el DADEP aplicará los mecanismos y controles requeridos para garantizar el cumplimiento de las restricciones legales al uso del material protegido, para lo cual:

- Solo se autorizará el uso de material (documentos, fotografías, imágenes, videos, audios) en cualquier formato producidos como parte del ejercicio misional, o haciendo uso de material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas con los proveedores y conforme lo dispuesto por la normativa vigente.
- La Entidad conservará de manera sistemática las pruebas y evidencias físicas y/o digitales de propiedad de licencias de software y de material documental producido o con autorización de uso por terceros.
- El DADEP Verificará que solo se instalen en sus equipos de cómputo, comunicaciones y dispositivos digitales, los productos de software propios o de terceros que cuenten con la licencia de uso por parte del fabricante.

12. CONTROL DE INSTALACIÓN Y USO DE SOFTWARE

La Defensoría del Espacio Público, a través de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), establecerá lineamientos y controles específicos para asegurar que, en las estaciones de trabajo, servidores y demás equipos institucionales únicamente se instale y utilice software debidamente autorizado y con licenciamiento vigente.

El uso de aplicaciones no autorizadas representa un riesgo crítico para la seguridad de la información, ya que puede facilitar la introducción de software malicioso, generar vulnerabilidades técnicas, incumplir la normatividad vigente en materia de propiedad intelectual y afectar la disponibilidad y confiabilidad de los servicios tecnológicos de la Entidad.

Con el fin de mitigar dichos riesgos, la OTIC implementará las siguientes medidas:

1. Políticas de restricción de instalación

- Configuración de los equipos institucionales mediante controles administrativos y técnicos (políticas de grupo, permisos restringidos y herramientas de administración centralizada) que limiten la instalación de programas únicamente a personal autorizado de OTIC.
- Mantenimiento de un listado oficial de software aprobado, el cual será revisado y actualizado periódicamente.

2. Gestión de licenciamiento

- Verificación de que todo software utilizado en la Entidad cuente con licencias válidas y legalmente adquiridas, conservando la documentación y evidencias correspondientes.
- Prohibición expresa de instalación de software sin licencia o con licenciamiento no válido.

3. Monitoreo y auditoría periódica

- Ejecución de revisiones programadas en las estaciones de trabajo y servidores para identificar la existencia de aplicaciones no autorizadas.
- Documentación de hallazgos y generación de informes para la Alta Dirección y el Comité Institucional de Gestión y Desempeño (CIGD).

4. Gestión correctiva y preventiva

- Eliminación inmediata de aplicaciones no autorizadas encontradas en los equipos institucionales.
- Ajuste de configuraciones de seguridad para evitar reincidencias.
- Registro de las acciones correctivas y preventivas adoptadas.

5. Responsabilidades de los usuarios

- Los colaboradores y contratistas deberán abstenerse de instalar software no autorizado y reportar de manera inmediata cualquier intento de instalación o hallazgo de programas que no hagan parte del inventario oficial.
- El incumplimiento de esta disposición será considerado una falta grave que puede derivar en acciones disciplinarias y/o contractuales, según corresponda.

De esta forma, la Entidad garantiza el cumplimiento de la normatividad vigente en materia de propiedad intelectual y la protección de la información, reduciendo la exposición a riesgos tecnológicos y fortaleciendo la seguridad de la infraestructura institucional.

13. GESTIÓN DE INCIDENTES DE PRIVACIDAD

Para la adecuada gestión de los incidentes de privacidad de la información, se aplicará el siguiente procedimiento:

- Los colaboradores y contratistas de la Entidad deberán reportar en el Sistema de Atención de Incidentes cualquier situación, evento o escenario que evidencie un riesgo materializado, amenaza o vulnerabilidad detectada en los servicios de aplicación o tecnológicos y que pueden tener impacto en la seguridad y privacidad de la información en los Activos de Información o los servicios tecnológicos de la Entidad.
- Proveedores y partes interesadas deberán reportar el caso vía correo electrónico a su contacto en el DADEP, quien, a su vez, aplicará el procedimiento descrito en el numeral anterior.
- El Administrador del Sistema de Incidencias, asignará el caso al Oficial de seguridad de la Información, o quien haga sus veces, quien dará el trámite correspondiente a la incidencia.

CONSIDERACIONES GENERALES:

- En caso que el Titular de datos personales deba registrar información personal en al menos uno de los sistemas de información de la Defensoría del Espacio Público - DADEP, el acceso a la información personal proporcionada por el Titular estará asegurada por una contraseña de acceso que solo él conocerá. Por tanto, es el único responsable de mantener en secreto su contraseña de acuerdo con las políticas de seguridad y privacidad de la información de la entidad.
- Para todas las bases, los datos serán transferidos sin necesidad de mediar autorización, en caso de que se presenten solicitudes por parte de autoridades

competentes en cumplimiento de sus funciones legales, en los términos del artículo 10 de la Ley 1581 de 2012.

- La Defensoría del Espacio Público - DADEP, ha adoptado los niveles de seguridad de protección de los datos personales legalmente requeridos, implementando los controles físicos y lógicos necesarios para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de datos facilitados, en consecuencia, la Defensoría del Espacio Público - DADEP, no se responsabiliza por cualquier consecuencia derivada de ingreso indebido de terceros a la base de datos y/o conservación de datos en los sistemas de información de la entidad.
- La Defensoría del Espacio Público - DADEP cuando trate datos personales de carácter sensible se circunscribirá estrictamente a lo determinado por los artículos 5 y 6 de la Ley 1581 de 2012, así como lo contenido en los decretos reglamentarios vigentes y aplicables para la materia.
- La Defensoría del Espacio Público - DADEP cuando trate datos personales de los niños, niñas y adolescentes se circunscribirá estrictamente a lo determinado por la Ley 1581 de 2012 así como lo contenido en los decretos reglamentarios vigentes y aplicables para la materia.
- Los datos personales de los Titulares y en general todo dato personal contenido en cualquier base de datos bajo responsabilidad de la Defensoría del Espacio Público - DADEP deben ser usados únicamente para los fines y propósitos establecidos por la Defensoría del Espacio Público - DADEP en sus formatos de autorización y aviso de privacidad, así como lo establecido en el numeral 9 de la presente Política. Así mismo, el tratamiento de los datos personales se debe circunscribir a la finalidad y alcance contenida en dichos documentos de autorización y aviso de privacidad entregada por los Titulares de los datos personales en el marco de la Ley 1581 de 2012 y sus decretos reglamentarios vigentes y aplicables cuando aplique dicha autorización, en la ley en cumplimiento de sus funciones misionales y más específicamente en los principios contenidos en el artículo 4 de la ley 1581 de 2012.
- La Defensoría del Espacio Público - DADEP, exclusivamente para el desarrollo de sus funciones legales, podrá transmitir, datos misionales que haya recolectado y tenga bajo su custodia, para lo cual se debe suscribir un contrato o convenio de trasmisión de datos en los términos del artículo 2.2.2.25.5.2 del Decreto 1074 de 2015.
- Eventualmente, la Defensoría del Espacio Público - DADEP en aplicación de los principios de coordinación y colaboración armónica establecidos en la Constitución Política, intercambiará información que contenga datos personales con las entidades públicas que así lo soliciten y hagan uso de la misma para el

- cumplimiento de sus funciones legales, para lo cual la Defensoría del Espacio Público - DADEP suscribirá acuerdos en los cuales se garantice la seguridad de la información, confidencialidad y las condiciones de uso, sin que sea necesario la autorización del titular de acuerdo al literal a) del artículo 10 de la Ley 1581 de 2012.
- La Defensoría del Espacio Público - DADEP aplicará las mejores prácticas y su mayor esfuerzo en la seguridad, custodia y confidencialidad de los datos personales de los Titulares, todo lo anterior, con el más alto nivel de confidencialidad y seguridad. Para el mejor cumplimiento de lo anterior, la Entidad cuenta con una política específica de Seguridad.
- La Defensoría del Espacio Público - DADEP administra las bases de datos para usuarios, empleados, contratistas, aspirantes a trabajadores, proveedores y público en general, las cuales son gestionadas por las respectivas dependencias de la entidad, para los fines establecidos en la presente Política.
- El tratamiento se efectuará conforme a los parámetros establecidos en la presente Política, siempre bajo la respectiva confidencialidad y seguridad, así como lo establecido en la Ley y la Constitución.
- La autorización para el tratamiento de los datos personales debe estar circunscrita estrictamente a los principios establecidos en la Ley 1581 de 2012, los derechos de los titulares, la finalidad establecida en la autorización y la pertinencia y adecuación con dicha finalidad. Así mismo, la autorización es una facultad que sólo les compete a los Titulares, la cual debe ser previa, expresa e informada conteniendo en ella, la finalidad clara y expresa de dicha autorización.

Características de la autorización:

- a) Previa: tomada antes de efectuar el tratamiento de los datos personales.
- b) Expresa: que dicha autorización que pueda ser objeto de consulta posterior o ante cualquier requerimiento.
- c) Informada: en la autorización informarle los datos personales que serán recolectados, así como todas las finalidades específicas del Tratamiento para las cuales se obtiene la autorización.

14. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES:

Los principios que rigen el tratamiento de los datos personales en la presente política son los establecidos en el artículo 4 de la Ley 1581 de 2012 así:

- a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen

- b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernen.
- f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.
- g) Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.
- h) Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- i) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

}

Finalidad en el tratamiento de los datos.

La Defensoría del Espacio Público para el cumplimiento de sus actividades misionales podrá recolectar, eliminar, actualizar, modificar, utilizar, almacenar, transferir y en general, realizar diversas operaciones referidas al tratamiento de los datos personales sin el requerimiento de autorización de conformidad con el literal a) del artículo 10 de la ley 1581 de 2012. La Defensoría del Espacio Público, los encargados o terceros que tengan acceso a estos datos por virtud de la ley, por el ejercicio de sus funciones o por el cumplimiento de las obligaciones inmersas en los contratos respecto del tratamiento de los datos personales deberán someterse a las finalidades que señalan a continuación:

- a) Para efectos de relación con la ciudadanía, informar aspectos inherentes al desarrollo de las actividades misionales del DADEP prestados a la ciudadanía.
- b) Tratamiento relativo a la nómina de personal de la Defensoría del Espacio Público, así como todos los procedimientos internos de la entidad relacionados con la relación laboral.
- c) Procesos de vinculación y contratación de personal que labora con la Defensoría del Espacio Público, procedimientos internos relacionados con el personal de planta de la entidad, registros de ingreso de visitantes en cada la (s) sedes de la de la Defensoría del Espacio Público, videos de registro de seguridad utilizados en los circuitos cerrados de televisión-CCTV, entre otros. El titular podrá modificar o actualizar la información suministrada en cualquier momento.
- d) Para todos los procedimientos internos de contratación de la entidad relacionados con la relación contractual, así como, surtir los trámites requeridos en el Sistema Electrónico de Contratación Pública – SECOP II.
- e) Con el fin de contactar y contratar con proveedores productos o servicios que la Defensoría del Espacio Público requiera para el normal funcionamiento de su operación y para la adecuada dotación de sus instalaciones, servicios y oficinas.
- f) Para la seguridad de las personas, la seguridad de la entidad, así como para efectos de atención de emergencias para la ciudadanía en general en las instalaciones de la Defensoría del Espacio Público.
- g) Para todos los procedimientos internos de la entidad relacionados con los cumplimientos misionales y funcionamiento de esta a través de los sistemas de información de la Defensoría del Espacio Público.
- h) Para el intercambio con entidades terceras a la Defensoría del Espacio Público cuando se requiera para el cumplimiento de la misionalidad de este.

- i) Para el cumplimiento de las funciones asignadas a la Defensoría del Espacio Público en el Acuerdo 18 de 1992 y sus decretos reglamentarios.

PARÁGRAFO 1. En caso de que el titular de datos personales deba registrar información personal en al menos uno de los sistemas de información del DADEP, el acceso a la información personal proporcionada por el titular estará asegurada por una contraseña de acceso que solo él conocerá. Por tanto, es el único responsable de mantener en secreto su contraseña de acuerdo con las políticas de seguridad y privacidad de la información de la entidad.

PARÁGRAFO 2. Para todas las bases, los datos serán transferidos sin necesidad de mediar autorización, en caso que se presenten solicitudes por parte de autoridades competentes en cumplimiento de sus funciones legales, en los términos del artículo 10 de la Ley 1581 de 2012.

PARÁGRAFO 3. La Defensoría del Espacio Público – DADEP, ha adoptado los niveles de seguridad de protección de los datos personales legalmente requeridos, implementando los controles físicos y lógicos necesarios para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de datos facilitados, en consecuencia, la Defensoría del Espacio Público – DADEP, no se responsabiliza por cualquier consecuencia derivada de ingreso indebido de terceros a la base de datos y/o conservación de datos en los sistemas de información de la entidad.

PARÁGRAFO 4. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN. La autorización del Titular no será necesaria cuando se trate de:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial
- b) Datos de naturaleza pública.
- c) Casos de urgencia médica o sanitaria
- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- e) Datos relacionados con el Registro Civil de las Personas.

La Defensoría del Espacio Público – DADEP, exclusivamente para el desarrollo de sus funciones legales, podrá transmitir a los proveedores misionales, datos misionales que haya recolectado y tenga bajo su custodia, para lo cual se debe suscribir un convenio y/o contrato de transmisión de datos en los términos del artículo 2.2.2.25.5.2 del Decreto 1074 de 2015.



Eventualmente, el DADEP en aplicación de los principios de coordinación y colaboración armónica establecidos en la Constitución Política, intercambiará información que contenga datos personales con las entidades públicas que así lo soliciten y hagan uso de la misma para el cumplimiento de sus funciones legales, para lo cual el DADEP suscribirá acuerdos en los cuales se garantice la seguridad de la información, confidencialidad y las condiciones de uso, sin que sea necesario la autorización del titular de acuerdo al literal a) del artículo 10 de la Ley 1581 de 2012.

Derechos del titular de los datos personales

Los titulares de los datos personales tienen derecho a:

- a) Conocer, actualizar y rectificar sus datos personales frente a la Defensoría del Espacio Público o sus Encargados. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- b) Solicitar prueba de la autorización otorgada a la Defensoría del Espacio Público salvo las excepciones de la Ley 1581 de 2012.
- c) Ser informado por la Defensoría del Espacio Público o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley vigente y aplicable para la protección de datos personales.
- e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento la Defensoría del Espacio Público o el Encargado ha incurrido en conductas contrarias a la Ley y a la Constitución. No obstante, la solicitud de supresión de datos no procederá cuando el titular tenga un deber legal o contractual de permanecer en la(s) base(s) de datos o la supresión de los datos represente un impedimento en actuaciones administrativas o judiciales relacionadas.
- f) a obligaciones fiscales, investigación de delitos o actualización de sanciones administrativas.

- g) Acceder en forma gratuita a los datos personales que hayan sido objeto de Tratamiento por parte de la Defensoría del Espacio Público.

Área responsable de la atención de consultas y reclamos.

El Área responsable en la Defensoría del Espacio Público – DADEP para la atención de consultas y reclamos referente al ejercicio de los derechos de los Titulares de los datos personales es la Subdirección Administrativa y Financiera a través de la Dirección de Atención al Ciudadano.

Procedimiento para ejercer los derechos de los titulares.

Para el efectivo y adecuado ejercicio de los derechos de los Titulares, referente a los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, la Defensoría del Espacio Público – DADEP las atenderá a través de los canales establecidos por la entidad.

a) Consultas:

La consulta será atendida por parte del DADEP en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

b) Reclamos:

El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en las normas que regulan la Protección de los datos Personales, podrán presentar un reclamo ante el DADEP o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

El reclamo se formulará mediante solicitud dirigida al DADEP o al Encargado del Tratamiento, con:

- Identificación del Titular,
- Descripción de los hechos que dan lugar al reclamo,
- Dirección (Física o electrónica), y,
- Acompañando los documentos que se quiera hacer valer.



Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda e informará de la situación al interesado.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el responsable del Tratamiento o Encargado del Tratamiento.

PARÁGRAFO. El canal determinado por el DADEP para la interposición de consultas y reclamos será el determinado por la Subdirección Administrativa y Financiera.

SEGURIDAD, CUSTODIA, TRANSPARENCIA, CALIDAD Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES.

El DADEP aplicará las mejores prácticas y su mayor esfuerzo en la seguridad, custodia y confidencialidad de los datos personales de los titulares, todo lo anterior, con el más alto nivel de confidencialidad y seguridad. Para el mejor cumplimiento de lo anterior, la Entidad cuenta con una política específica de Seguridad.

ADMINISTRACIÓN DE LAS BASES DE DATOS.

El DADEP administra las bases de datos para usuarios, empleados, contratistas, aspirantes a trabajadores, proveedores y público en general, las cuales son gestionadas por las respectivas dependencias de la entidad, para los fines establecidos en la presente Política.

El tratamiento se efectuará conforme a los parámetros establecidos en la presente resolución, siempre bajo la respectiva confidencialidad y seguridad y bajo la égida de la Constitución Política, la ley 1581 de 2012 y sus decretos reglamentarios.

DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES.

El área que ejercerá las funciones y como oficial de protección de datos personales es la Oficina Asesora Jurídica, quien designará al Oficial de Protección de Datos Personales, quien ejercerá las siguientes funciones:

- a) Coordinar con las áreas de la Entidad para asegurar una implementación transversal del PIGDP.
- b) Impulsar una cultura de Protección de Datos Personales dentro de la Defensoría del Espacio Público.
- c) Mantener un inventario de las bases de datos personales en poder de la Defensoría del Espacio Público y clasificarlas según su tipo.
- d) Actualizar las bases de datos de la Defensoría del Espacio Público en el Registro Nacional de Bases de Datos el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
- e) Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
- f) Revisar los contenidos de los contratos relacionados con la protección de datos personales que se suscriban con Encargados.
- g) Analizar las responsabilidades de cada cargo de la Defensoría del Espacio Público, para diseñar un programa de entrenamiento en PDP específico para cada uno de ellos.
- h) Realizar un entrenamiento general en PDP para todos los empleados de la Defensoría del Espacio Público.
- i) Realizar el entrenamiento necesario a los nuevos empleados y contratistas, que tengan acceso por las condiciones de su empleo o contrato, a datos personales gestionados por la Defensoría del Espacio Público.
- j) Integrar la política de Protección de Datos Personales dentro de las actividades de las demás áreas de la Defensoría del Espacio Público.
- j) Medir la participación, y calificar el desempeño, en los entrenamientos de Protección de Datos Personales.

- k) Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre Protección de Datos Personales.
- l) Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.
- k) Acompañar y asistir a la Defensoría del Espacio Público en la atención de las visitas y los requerimientos que realice la SIC.
- l) Realizar seguimiento al PIGDP.

Para el efectivo cumplimiento de las funciones asignadas al área de protección de datos, se establece que las solicitudes elevadas por esta a las distintas dependencias de la Defensoría del Espacio Público se les dé prioridad, y deberán ser respondidas en el término establecido por el área de protección de datos en la respectiva solicitud.

Las funciones que requieran apoyo de las distintas dependencias de la Defensoría del Espacio Público deberán ser desarrolladas en conjunto, y el área involucrada debe prestar todo el apoyo necesario al área de protección de datos para la efectiva consecución de los objetivos.

EVALUACIÓN Y CONTROL.

El DADEP, desplegará una supervisión y revisión semestral de lo establecido en el presente documento, dando cuenta del cumplimiento del mismo, así como de la ejecución de los aspectos establecidos para el tratamiento de las bases de datos. Como resultado de la evaluación, la Entidad determinará si se considera necesario o no tomar medidas para actualizar la presente política.

ACTIVIDADES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA

Para garantizar la adecuada implementación de la Política General de Seguridad y Privacidad de la Información, se desarrollarán las siguientes actividades:

1. **Revisión y actualización de la política:**
 - Realizar revisiones periódicas de la política para garantizar su alineación con las normativas legales, los estándares internacionales aplicables y las necesidades estratégicas de la entidad.
 - Documentar las actualizaciones realizadas en el sistema de gestión de calidad y comunicarlas a todos los colaboradores.

2. Capacitación y Sensibilización:

- Diseñar e implementar programas de capacitación periódicos para todos los colaboradores contratistas y partes interesadas sobre los principios, procedimientos y lineamientos establecidos en la política.
- Realizar campañas de sensibilización para promover una cultura de seguridad y privacidad de la información en toda la organización.

3. Gestión de Riesgos de Seguridad de la Información

- Identificar, analizar y evaluar los riesgos asociados a la seguridad y privacidad de la información en los procesos misionales y de soporte.
- Implementar planes de tratamiento de riesgos con controles adecuados para minimizar las amenazas identificadas.

4. Gestión de Incidentes de Seguridad y Privacidad:

- Establecer procedimientos claros para la identificación, reporte, gestión y resolución de incidentes de seguridad y privacidad de la información.
- Mantener un sistema de registro y seguimiento de los incidentes para evaluar su impacto y mejorar continuamente las medidas de prevención.

5. Gestión de Activos de Información:

- Inventariar, clasificar y proteger los activos de información conforme a su valor estratégico para la entidad.
- Implementar controles tecnológicos y administrativos para garantizar la confidencialidad, integridad y disponibilidad de los activos.

6. Gestión de Cuentas de Correo Electrónico:

- Desactivar las cuentas de correo de los funcionarios y contratistas al finalizar su vinculación con la entidad.
- Reactivar cuentas únicamente con autorización formal del líder del proceso o delegado.
- Configurar mensajes de respuesta automática en cuentas desactivadas y eliminar buzones conforme a los periodos definidos.

7. Monitoreo y Auditoría:

- Implementar mecanismos de monitoreo continuo para evaluar el cumplimiento de la política y la efectividad de los controles establecidos.
- Realizar auditorías internas y externas periódicas para identificar áreas de mejora y fortalecer el modelo de seguridad y privacidad.

8. Gestión de Proveedores y Contratistas

- Verificar que los contratos con proveedores y contratistas incluyan cláusulas de confidencialidad y compromisos para cumplir con los lineamientos de seguridad y privacidad.
- Evaluar periódicamente el desempeño de los proveedores en cuanto a la gestión de la información.

9. Protección de Datos personales

- Garantizar que el tratamiento de datos personales cumpla con las disposiciones legales aplicables, protegiendo los derechos de los titulares.
- Mantener actualizado el registro de bases de datos en el Registro Nacional de Bases de Datos (RNBD).

10. Implementación de Controles Tecnológicos:

- Aplicar controles técnicos como cifrado, autenticación multifactorial y monitoreo de acceso para garantizar la seguridad de la información en los sistemas y plataformas de la entidad.

11. Evaluación de Impacto:

- Realizar evaluaciones de impacto sobre la seguridad y privacidad de la información para proyectos tecnológicos y procesos nuevos.

Estas actividades deberán ser ejecutadas conforme a un cronograma definido y supervisadas por las áreas responsables, con el apoyo de la Alta Dirección y las dependencias correspondientes.

COMPROMISOS

La Defensoría del Espacio Público DADEP, se compromete al respeto y protección de los datos personales que recojan o manejen durante el desarrollo del objeto y sus funciones, así como a brindar los recursos, económicos y de personal, necesarios para mantener las políticas, procedimientos y medidas de seguridad definidos para el tratamiento de los datos personales.

De igual manera se compromete a desarrollar, implementar y velar por el cumplimiento de la presente Política.

Poner en conocimiento al público y Titulares de los datos, las modificaciones a la presente Política.



Brindar educación a los empleados sobre la política y procedimientos de tratamiento a las bases de datos de la entidad.

VIGENCIA Y CUMPLIMIENTO.

La presente POLÍTICA es de obligatorio cumplimiento para todo el personal de la entidad, funcionarios, contratistas, proveedores y en general todo Titular de datos personales a los que la Entidad efectúe el tratamiento de sus datos personales y entrará a regir a partir de la publicación en la página Web y en el sitio que se determine por la directora de la Defensoría del Espacio Público.

La presente POLÍTICA mantendrá su vigencia indefinidamente, mientras el DADEP desarrolle su objeto y funciones y mientras sea necesario para asegurar el cumplimiento de obligaciones de carácter legal.

Las modificaciones a la presente POLÍTICA se harán de forma escrita y su vigencia entrará a regir desde el momento en que se efectúe la publicación en la página Web e intranet de la Entidad.

Actualizó: Sandra Marcela Venegas Páez - Contratista *Mausenhaus*

Revisó: Hugo Roberto Hernández Díaz - jefe OTIC. *H.R.H.*

Aprobó: Hugo Roberto Hernández Díaz - jefe OTIC. *H.R.H.*

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, Redistribución del contenido de los Ámbitos de Aplicación en el Alcance.
7.2	15/11/2023	Se actualiza la descripción del rol de Oficial de Seguridad de la Información
8	3/01/2025	Se agregó la sección "Actividades para la Implementación de la Política", incorporando procedimientos detallados sobre la gestión integral de la política, tales como la desactivación y reactivación de cuentas de correo electrónico, gestión de incidentes, capacitación, monitoreo y auditorías. Se actualizó la sección "Organización Interna" para consolidar las responsabilidades de las diferentes áreas involucradas en la política, con especial atención en la gestión de cuentas de correo por parte de la OTIC y otras responsabilidades estratégicas. Se ajustó el documento al formato oficial de documentos 2024, alineándolo con las nuevas directrices institucionales. Se aseguró la alineación de las actividades descritas con normativas legales, estándares internacionales y objetivos estratégicos de la entidad.
9	12/09/2025	<ul style="list-style-type: none"> Se incorpora el numeral 12. Control de instalación y uso de software, en cumplimiento de la observación de Control Interno, con el fin de formalizar la restricción de instalación de aplicaciones no autorizadas en los equipos institucionales, establecer revisiones periódicas de software y documentar la eliminación de programas no autorizados. Se adiciona lineamiento en el numeral 8. Separación de roles, indicando que la administración de credenciales y cuentas privilegiadas debe realizarse mediante mecanismos institucionales de custodia y verificación, con referencia a las políticas operativas específicas.