TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 4
2.1. OBJETIVOS ESPECÍFICOS 4
3. ALCANCE 4
4. NORMATIVIDAD 5
5. DEFINICIONES 5
6. ROLES Y RESPONSABILIDADES CONFORME A LAS LÍNEAS DE DEFENSA DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG 7
7. PRINCIPIOS ORIENTADORES 8
8. CONTEXTO INSTITUCIONAL 10
9. MARCO TEORICO 11
10. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES (RUTA DE IMPLEMENTACIÓN) 12
10.1. TRATAMIENTO Y FINALIDADES 12
10.1.1. Tratamiento de Datos Sensibles, Niños, Niñas y Adolescentes 14
10.2. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES 15
10.2.1. Transferencia de datos personales 16
10.2.2. Transmisión de datos personales 16
10.3. DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS 17
10.3.1. Derechos de los Titulares 17
10.3.2. Autorización para el Tratamiento de Datos Personales 17
10.4. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO 18
10.4.1. Deberes de los responsables del tratamiento 19
10.4.2. Deberes de los Encargados del Tratamiento 19
10.5. PROCEDIMIENTOS PARA EL TRATAMIENTO DE LOS DATOS 20
10.5.1. Procedimiento de Consultas 20
10.5.2. Procedimiento de Reclamos 21
10.5.3. Procedimiento de Gestión de Incidentes con Datos Personales 22
10.6. USO DE LA INFORMACIÓN 24
10.7. ALMACENAMIENTO DE INFORMACIÓN 25
10.7.1. Almacenamiento de Información Electrónica 25
10.7.2. Almacenamiento de Información Física 25
10.7.3. Objetivo de las medidas de seguridad 26
10.8. DISPOSICIÓN FINAL Y DESTRUCCIÓN SEGURA DE LA INFORMACIÓN 26

10.9. ATENCIÓN DE CONSULTAS, PETICIONES Y RECLAMOS 26
10.10. REGISTRO NACIONAL DE BASE DE DATOS 27
10.11. APLICABILIDAD 27
10.12. LINEAMIENTOS, REVISIÓN Y VIGENCIA 27
11. BIBLIOGRAFIA 28
12. CONTROL DE CAMBIOS 29
13. AUTORIZACIONES 29

1. INTRODUCCIÓN

El JARDÍN BOTÁNICO DE BOGOTÁ - JOSÉ CELESTINO MUTIS (en adelante JBJCM), , con domicilio en la Calle 63 No. 68 – 95 en Bogotá D.C., en cumplimiento de lo dispuesto en la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, que a su vez fue derogado parcialmente por el Decreto 1081 de 2015 así como en atención a las directrices emitidas por la Superintendencia de Industria y Comercio (SIC), en particular aquellas contenidas en el 'Instructivo para la elaboración de políticas de tratamiento de la información personal' y la 'Guía para la implementación del principio de responsabilidad demostrada (accountability)', adopta la presente Política de Tratamiento de Datos Personales., adopta la presente Política de Tratamiento de Datos Personales, con el fin de garantizar el derecho fundamental que tienen todas las personas a conocer, actualizar, rectificar, suprimir y revocar la autorización sobre la información personal que haya sido recolectada y almacenada en las bases de datos administradas por la Entidad.

Las entidades estatales que conforman las ramas del poder público[1] recolectan, usan, circulan y tratan Datos Personales. Por lo tanto, son responsables de su tratamiento y deben cumplir con todos los deberes constitucionales y legales. Es factible que para ciertas actividades acudan a terceros (contratistas, empresas de seguridad, proveedores de tecnologías, otras entidades públicas, etc.) que actúan como encargados del tratamiento.

Conforme con la normatividad vigente, las personas tienen el derecho a conocer, actualizar y rectificar toda la información que se haya recogido sobre ellas en bases de datos o archivos de entidades públicas y privadas. Además, señala que "en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución". Esta disposición fue desarrollada por la Ley Estatutaria 1581 de 2012, la cual no solo es aplicable a las entidades públicas, sino que define "tratamiento" como: *"cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"*.

La presente política se expide como parte del fortalecimiento institucional en materia de seguridad de la información y protección de datos personales, con el objetivo de establecer lineamientos claros y unificados que orienten a la Entidad en el cumplimiento de sus deberes legales y misionales, y contribuya a generar confianza entre los grupos de interés, asegurando que el tratamiento de su información se realiza con responsabilidad, ética y conforme al marco legal vigente.

En este sentido, el JBJCM, realizará el tratamiento de los datos personales de manera legal, leal, transparente, segura, confidencial y conforme a los principios establecidos en la normativa vigente, exclusivamente para los fines autorizados y en el marco de sus funciones legales y misionales.

Esta política tiene aplicación obligatoria para todos los funcionarios, contratistas y terceros, entendidos estos últimos como toda persona natural o jurídica, diferente al titular de los datos y a los funcionarios o contratistas del JBJCM, que, por razón de una relación contractual, comercial, administrativa o legal, realicen actividades que involucren el Tratamiento de Datos personales en nombre de la Entidad.

Por lo tanto, el JBJCM se compromete a adoptar las medidas técnicas, administrativas y jurídicas necesarias para proteger la integridad, confidencialidad y disponibilidad de los datos personales, minimizando los riesgos que puedan afectar los derechos y libertades de los titulares. Así mismo, promoverá la cultura de la protección de datos personales dentro de la organización y velará que toda

[1] Cfr. Artículo 113 de la Constitución Política de Colombia.

persona natural o jurídica que acceda a dicha información cumpla con los estándares de seguridad y privacidad definidos por la Entidad.

2. OBJETIVO

Proporcionar la información necesaria a los distintos grupos de interés y establecer los lineamientos que aseguren la protección de los datos personales que son objeto de tratamiento por parte del JBJCM. A través de esta política, la Entidad se compromete a cumplir con la legislación vigente, así como con las políticas y procedimientos establecidos para garantizar los derechos de los titulares de los datos; y se establecen criterios claros sobre la recolección, almacenamiento, uso, circulación y supresión de los datos personales, en cumplimiento de los estándares de privacidad y seguridad establecidos.

2.1. OBJETIVOS ESPECÍFICOS

1. Proteger la privacidad de los visitantes, funcionarios, contratistas y terceros, mediante la adopción de medidas que salvaguarden la confidencialidad de los datos personales, con el fin de garantizar su tratamiento adecuado, conforme a los principios de legalidad, lealtad y respeto por los derechos y libertades de los titulares.
2. Establecer principios y directrices claras para el Tratamiento de Datos personales que orienten las actividades de recolección, almacenamiento, uso, circulación y disposición de dichos datos, con el fin de asegurar prácticas institucionales alineadas con el marco normativo vigente y con el respeto de los derechos de los titulares.
3. Cumplir con las obligaciones legales y normativas aplicables en materia de protección de datos personales, mediante la implementación de políticas, procedimientos y controles internos, con el fin de demostrar la responsabilidad de la entidad y evidenciar el cumplimiento ante entes de control y supervisión.
4. Generar confianza y transparencia, frente a los titulares de los datos personales, mediante la divulgación clara y oportuna de las prácticas adoptadas por el JBJCM para el tratamiento de la información, con el fin de fortalecer las relaciones institucionales con visitantes, funcionarios, contratistas y demás grupos de interés.
5. Garantizar la seguridad de la información personal objeto de tratamiento, mediante la implementación de medidas técnicas, administrativas y organizativas adecuadas, con el fin de prevenir el acceso no autorizado, la pérdida, alteración, divulgación o destrucción de los datos personales.

3. ALCANCE

La presente Política de Protección de Datos Personales aplica a todas las bases de datos, sistemas de información, archivos físicos y/o digitales que contengan datos personales en poder del JBJCM, independientemente del medio, soporte o modalidad de recolección o almacenamiento utilizado, y que sean objeto de tratamiento por parte de la entidad.

Su alcance se extiende a todos los datos personales de personas naturales, ya sean empleados, contratistas, proveedores, visitantes, usuarios, participantes de actividades institucionales, entre otros titulares, sin perjuicio de que también pueda involucrar datos relacionados con personas jurídicas, en los casos en que sea aplicable conforme a la normatividad vigente.

El cumplimiento de esta política es de carácter obligatorio y vinculante para todos los integrantes de la Entidad, incluyendo, pero sin limitarse a:

- Directivos y funcionarios públicos de planta y provisionales.
- Contratistas vinculados mediante órdenes de prestación de servicios.
- Proveedores y aliados estratégicos con acceso a bases de datos o sistemas que contengan información personal.
- Cualquier tercero que, en virtud de una relación contractual, legal o institucional, tenga acceso, directa o indirectamente, a datos personales tratados por el JBJCM.

Esta política implica el acatamiento de las obligaciones legales y administrativas relacionadas con la protección de datos personales, así como la adopción de comportamientos que aseguren la confidencialidad, integridad, disponibilidad y legalidad en el tratamiento de la información. En caso de posibles incumplimientos, el JBJCM propenderá por adelantar las acciones necesarias para su identificación, análisis y corrección, en el marco de la mejora continua y la responsabilidad institucional. No obstante, cuando se configuren faltas que contravengan la normatividad vigente, podrán dar lugar a las acciones disciplinarias, contractuales y/o legales correspondientes, conforme a lo previsto en el ordenamiento jurídico aplicable.

4. NORMATIVIDAD

La normatividad asociada al desarrollo de este documento se encuentra en el Normograma del Jardín Botánico José Celestino Mutis - JBJCM

5. DEFINICIONES

- **Autorización:** Es el consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales. Fuente: Superintendencia de Industria y Comercio. (2013). Guía para la implementación del principio de autorización del titular de la información[2].
- **Aviso de privacidad:** Es una de las opciones de comunicación verbal o escrita que brinda la ley para darle a conocer a los titulares de la información, la existencia y las formas de acceder a las políticas de tratamiento de la información y el objetivo de su recolección y uso. Fuente: Superintendencia de Industria y Comercio. (2013). Guía para la implementación del principio de autorización del titular de la información.
- **Base de Datos:** Conjunto organizado de datos personales que son objeto de tratamiento. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012 -[3].
- **Dato personal:** Se trata de cualquier información vinculada o que pueda asociarse a una persona determinada, como su nombre o número de identificación, o que pueda hacerla determinable, como sus rasgos físicos. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Corte Constitucional de Colombia. (2011). Sentencia T-729 de 2002.
- **Dato público:** Es uno de los tipos de datos personales existentes. 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. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Corte Constitucional de Colombia. (2011). Sentencia T-729 de 2002.

---

2 https://www.sic.gov.co/sites/default/files/files/Proteccion_de_datos_personales/Guia%20autorizacion%20titular%20de%20la%20informacion.pdf

3 http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

- **Dato semiprivado:** Son los datos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o a la sociedad en general. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Corte Constitucional de Colombia. (2011). Sentencia T-729 de 2002.
- **Dato sensible:** Son aquellos que afectan la intimidad del titular o pueden dar lugar a que lo discriminen, es decir, aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, entre otros. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Corte Constitucional de Colombia. (2011). Sentencia T-729 de 2002.
- **Dato privado:** Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. Los gustos o preferencias de las personas, por ejemplo, corresponden a un dato privado. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Corte Constitucional de Colombia. (2011). Sentencia T-729 de 2002.
- **Derecho Habeas Data:** El derecho de hábeas data es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada. La Corte Constitucional lo definió como el derecho que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información. Fuente: Corte Constitucional de Colombia. (2002). Sentencia T-729 de 2002. Congreso de Colombia. (2012). Ley 1581 de 2012.
- **Encargado del tratamiento:** Es la persona natural o jurídica que realiza el Tratamiento de Datos personales, a partir de una delegación que le hace el responsable, recibiendo instrucciones acerca de la forma en la que deberán ser administrados los datos.
- **Grupo de interés:** Ciudadanos, usuarios o grupos de interés": aquellas personas, colectivos, organizaciones o entidades que, de manera directa o indirecta, participan, se ven afectadas o tienen interés en un proyecto, programa o actividad de la entidad
- **Incidente de seguridad:** Evento que afecta o puede afectar la confidencialidad, integridad o disponibilidad de los datos personales. Puede implicar el acceso no autorizado, la pérdida, modificación, divulgación, destrucción o uso indebido de datos personales, ya sea de forma intencionada o accidental. *Fuente; "Guía para la Gestión de Incidentes de Seguridad de la Información que involucren Datos Personales", 2021*[4]*.*
- **Responsable del tratamiento:** Es la persona natural o jurídica, pública o privada, que decide sobre la finalidad de las bases de datos y/o el tratamiento de los mismos. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. [5].
- **Titular:** Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de dato y son objeto del tratamiento. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Presidencia de la República. (2013). Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581 de 2012.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Fuente: Congreso de

[4] https://www.sic.gov.co/sites/default/files/guias/Guia_Incidentes_Seguridad_Datos_Personales.pdf
[5] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Colombia. (2012). Ley 1581 de 2012. Presidencia de la República. (2013). Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581 de 2012.

- **Transferencia:** Se trata de la operación que realiza el responsable o el encargado del tratamiento de los datos personales, cuando envía la información a otro receptor, que, a su vez, se convierte en responsable del tratamiento de esos datos. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Presidencia de la República. (2013). Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581 de 2012.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio colombiano cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del Responsable. Fuente: Congreso de Colombia. (2012). Ley 1581 de 2012. Presidencia de la República. (2013). Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581 de 2012.

6. ROLES Y RESPONSABILIDADES CONFORME A LAS LÍNEAS DE DEFENSA DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

En este numeral, se establecen los roles y las responsabilidades en todas las instancias y niveles para la gestión institucional, para la implementación y adopción de la presente política.

LINEA ESTRATEGICA	
RESPONSABLE	**ROLES**
Dirección del JBJCM	Proporcionar los recursos necesarios para la implementación y mantenimiento del Programa de Protección de Datos Personales (recursos económicos, formación y recursos tecnológicos).
Comité Institucional de Gestión y Desempeño	Asegurar el cumplimiento de las normativas y políticas relacionadas con la protección de datos personales en el JBJCM.
PRIMERA LINEA DE DEFENSA	
RESPONSABLE	**ROLES**
Secretaria General – Proceso Gestión de la Tecnología	Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de Seguridad de la Información relacionados con Datos Personales.
Secretaria General – Proceso Gestión del Talento Humano	Coordinar con el proceso de Seguridad de la Información el Plan de Inducción, Capacitación y Sensibilización en Protección de Datos Personales en JBJCM, con el fin de promover la toma de conciencia sobre las responsabilidades de cada funcionario y/o contratista de acuerdo con las políticas y procedimientos establecidos.
Oficina Jurídica – Proceso Gestión Contractual	Procurar la protección de datos personales que puedan verse involucrados en los procesos contractuales de la entidad.
Líderes de proceso:	Implementar las políticas y procedimientos que se definan dentro del Programa de Protección de Datos Personales.
Funcionarios, contratistas y terceros	• Apoyar a los líderes de proceso en el desarrollo de tareas relacionadas con el Tratamiento de Datos Personales. • Cumplir las políticas, lineamientos y procedimientos de Protección de Datos personales. • Informar sobre cualquier incidente de Protección de Datos Personales por los canales establecidos. y asistir a las sensibilizaciones en temas de Protección de Datos Personales.
SEGUNDA LINEA DE DEFENSA	
RESPONSABLE	**ROLES**
Oficina Asesora de Planeación – Proceso	• Velar por el cumplimiento de la normativa de Protección de Datos Personales, incluyendo la Ley 1581 de 2012 y sus normas reglamentarias. • Coordinar las actividades relacionadas con el Tratamiento de Datos Personales

Seguridad de la Información	dentro de la Entidad. • Realizar evaluaciones periódicas de riesgos y vulnerabilidades en relación con el Tratamiento de Datos Personales, y tomar medidas para mitigar dichos riesgos. • Mantener actualizado el Registro Nacional de Bases de Datos (RNBD) ante la SIC incluyendo la información relacionada con las bases de datos administradas por la Entidad y los tratamientos de datos personales realizados, conforme a lo establecido en la normatividad vigente. • Asesorar a la organización en materia de protección de datos personales y ofrecer capacitación y orientación al personal sobre sus responsabilidades en relación con la protección de datos. • Coordinar la atención de consultas, solicitudes y reclamos relacionados con la protección de datos personales. • Actuar como enlace entre la organización y la SIC, en su calidad de autoridad de protección de datos personales, para atender requerimientos, facilitar auditorías y garantizar el cumplimiento de la normativa aplicable. • Supervisar el cumplimiento de las políticas y procedimientos establecidos en la organización en relación con la protección de datos personales. • Colaborar con otras áreas de la entidad en la implementación de medidas de seguridad y privacidad de los datos personales.
TERCERA LINEA DE DEFENSA	
RESPONSABLE	**ROLES**
Oficina de Control Interno	Realizar seguimiento al cumplimiento con lo establecido en la presente política según lo programado en el plan de auditoría de la vigencia.

7. PRINCIPIOS ORIENTADORES

Tomando en cuenta las disposiciones, descritas en el capítulo 5 de este documento, que actualmente define la Superintendencia de Industria y Comercio -SIC, el desarrollo, interpretación y aplicación de la ley, regulaciones, y normatividad vigente, se aplicarán, de manera armónica e integral, los siguientes principios:

- **Principio de legalidad en materia de tratamiento de datos:** El Tratamiento de Datos Personales establece que dicha actividad debe llevarse a cabo de acuerdo con lo estipulado en la Ley 1581 del 17 de octubre de 2012, así como en los decretos reglamentarios y demás disposiciones que la complementen y desarrollen. Esto implica que el Tratamiento de Datos debe ser realizado dentro de los límites legales establecidos, respetando los derechos de los titulares y cumpliendo con las obligaciones y procedimientos establecidos por la legislación vigente en materia de protección de datos. Es fundamental que la Entidad se adhiera a estos marcos legales para garantizar la legalidad y transparencia en el manejo de la información personal.

- **Principio de finalidad:** El Tratamiento debe tener una finalidad legítima, de acuerdo con lo establecido en la Constitución y la Ley. Esta finalidad debe ser clara, específica y previamente informada al titular de los datos. En otras palabras, se debe informar al titular cómo y con qué propósito se utilizarán sus datos personales antes de llevar a cabo el tratamiento. Esto busca garantizar que los datos sean utilizados de manera justa y acorde con los derechos y expectativas de privacidad de los titulares.

- **Principio de libertad:** El Tratamiento establece que dicho tratamiento solo puede llevarse a cabo con el consentimiento previo, expreso e informado del titular de los datos. Esto implica que

los datos personales no pueden ser obtenidos o divulgados sin la autorización previa del titular, a menos que exista un mandato legal o judicial que releve la necesidad de obtener dicho consentimiento. Es fundamental respetar la voluntad y la autonomía de las personas en el manejo de sus datos personales, asegurando que estén plenamente informadas sobre cómo se utilizarán y que tengan la opción de otorgar o denegar su consentimiento de manera libre.

- **Principio de veracidad o calidad:** La información sujeta a dicho tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se requiere que los datos sean fieles a la realidad y estén completos, sin omitir información relevante. Además, deben estar actualizados y reflejar la situación más reciente del titular de los datos. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que puedan inducir a error. Este principio busca garantizar la calidad y confiabilidad de los datos tratados, evitando la manipulación o distorsión de la información personal.

- **Principio de transparencia:** En el Tratamiento debe garantizar el derecho del titular a obtener, en cualquier momento y sin restricciones, información acerca de la existencia de datos personales que le conciernan. Tanto el responsable del tratamiento como el encargado del tratamiento tienen la obligación de proporcionar esta información de manera clara, accesible y comprensible para el titular. Esto implica que el titular tiene el derecho de conocer qué datos personales se están tratando, con qué finalidad, cómo se obtuvieron y cuáles son los derechos que le asisten respecto a dichos datos. La transparencia en el tratamiento de datos es esencial para fomentar la confianza y permitir que los titulares ejerzan efectivamente su derecho a controlar y proteger su información personal.

- **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que derivan de la naturaleza de dichos datos, así como de las disposiciones de la ley y la Constitución. En este sentido, el tratamiento solo puede ser realizado por personas autorizadas por el titular de los datos y/o por aquellas personas que estén previstas en la ley. Los datos personales, a excepción de la información pública, no deben estar disponibles en Internet u otros medios de divulgación o comunicación masiva, a menos que el acceso a ellos sea técnicamente controlable para garantizar que solo los titulares de los datos o terceros autorizados puedan acceder a ellos de manera restringida. Es fundamental que los responsables del tratamiento implementen medidas de seguridad y control adecuadas para proteger los datos personales y asegurar que solo las personas autorizadas puedan acceder a ellos.

- **Principio de seguridad:** La información sujeta a tratamiento por parte del responsable o encargado del tratamiento debe ser manejada con las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los registros. Esto implica implementar medidas de seguridad adecuadas para prevenir la adulteración, pérdida, consulta, uso, acceso no autorizado o fraudulento de los datos personales. Las medidas de seguridad pueden incluir tecnologías y procedimientos de protección, controles de acceso, encriptación, políticas de seguridad de la información, capacitación del personal y auditorías internas, entre otros. El objetivo es proteger la integridad y confidencialidad de los datos personales, así como evitar cualquier tipo de incidente o vulneración de la seguridad.

- **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de Datos personales, incluyendo funcionarios y contratistas, están obligadas a garantizar la reserva y confidencialidad de la información. Esta obligación se mantiene incluso después de finalizada

su relación con las labores relacionadas con el Tratamiento de Datos. En el caso del JBJCM, se compromete a tratar los datos personales de los titulares de manera absolutamente confidencial, tal como lo define la Ley 1581 de 2012. Estos datos serán utilizados exclusivamente para las finalidades indicadas previamente, siempre y cuando el titular no se haya opuesto a dicho tratamiento.

- **Principio de Temporalidad:** Los datos personales deben ser conservados únicamente durante el tiempo razonable y necesario para cumplir las finalidades para las cuales fueron recopilados. Esto implica que se deben tener en cuenta las disposiciones aplicables a la materia en cuestión, así como los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Los datos personales serán conservados cuando sea necesario para cumplir con una obligación legal o contractual. Una vez que se haya cumplido la finalidad del tratamiento y los términos establecidos, se procederá a la supresión de los datos de manera segura y adecuada.

- **Interpretación Integral de los Derechos Constitucionales:** Los derechos deben ser interpretados de manera armoniosa y en equilibrio con el derecho a la información consagrado en el artículo 20 de la Constitución, así como con otros derechos constitucionales aplicables. Esto significa que, al analizar y aplicar los derechos constitucionales, se debe tener en cuenta la importancia y el valor del derecho a la información, buscando encontrar un equilibrio que garantice la protección de los derechos individuales y colectivos sin menoscabar el acceso a la información relevante y necesaria para el ejercicio pleno de otros derechos. La interpretación integral de los derechos constitucionales busca evitar conflictos o contradicciones entre los diferentes derechos reconocidos en la Constitución, promoviendo una visión coherente y armónica de los mismos. Así, se busca proteger tanto la privacidad y los derechos individuales como la transparencia, la participación ciudadana y el acceso a la información pública, reconociendo la importancia de cada uno de estos aspectos en una sociedad democrática.

- **Principio de Necesidad:** Los datos personales tratados deben ser los estrictamente necesarios para cumplir las finalidades previstas con la base de datos. Esto implica que se deben recopilar y utilizar únicamente aquellos datos que sean pertinentes, adecuados y proporcionales para lograr los objetivos del tratamiento. Al aplicar el principio de necesidad, se busca evitar la recopilación y el uso indiscriminado de datos personales, limitando la cantidad y la diversidad de información obtenida a lo que resulte esencial para alcanzar las finalidades establecidas. Esto garantiza que el Tratamiento de Datos se realice de manera justa, proporcionada y ajustada a los propósitos legítimos perseguidos.

8. CONTEXTO INSTITUCIONAL

El JBJCM es una Entidad pública descentralizada del orden distrital, que fue reconocida por el Ministerio de Ciencia, Tecnología e Innovación como Centro de Investigación hasta mayo de 2025 a través de la Resolución 469 del 17 de mayo de 2022 y que actualmente se encuentra en proceso de reacreditación. Su misión se centra en la investigación, conservación y divulgación de la diversidad vegetal, con énfasis en los ecosistemas altoandinos y de páramo, contribuyendo al desarrollo sostenible y a la adaptación al cambio climático en Bogotá y la región. Como parte de su gestión, el JBJCM desarrolla programas de educación ambiental, restauración ecológica y arborización urbana, además de mantener colecciones vivas que albergan más de 900 especies de plantas, muchas de ellas en riesgo de extinción.

En el cumplimiento de sus funciones, la Entidad recolecta y trata datos personales de ciudadanos, visitantes, investigadores, funcionarios y contratistas. Por esta razón, adopta medidas técnicas, administrativas y legales para garantizar la privacidad, confidencialidad y seguridad de la información, en concordancia con la Ley 1581 de 2012 y demás normativas aplicables. Esta política refleja el compromiso institucional de actuar con transparencia y responsabilidad, asegurando que el tratamiento de los datos personales se realice de manera ética y conforme a los principios de legalidad, finalidad, libertad, veracidad, acceso y circulación restringida, seguridad y confidencialidad.

9. MARCO TEORICO

El tratamiento de datos personales constituye una actividad regulada por el Ordenamiento Jurídico Colombiano, dado su impacto en el goce efectivo de los derechos fundamentales a la intimidad, el buen nombre, el habeas data y la protección de la información personal. La creciente digitalización de procesos, la interoperabilidad entre entidades públicas y privadas, y el uso de tecnologías de la información exigen establecer medidas claras y robustas que garanticen el adecuado uso, almacenamiento, circulación y eliminación de datos personales.

La Ley Estatutaria 1581 de 2012, es la norma central que regula el Tratamiento de Datos Personales en Colombia. Esta ley establece los principios, derechos, deberes y procedimientos que deben ser observados por quienes recolectan, almacenan o procesan datos personales. Adicionalmente, la Ley 1266 de 2008 regula el habeas data financiero, mientras que los Decretos 1377 de 2013 y 1081 de 2015, reglamentan aspectos operativos como la obtención del consentimiento del titular, la implementación de políticas institucionales y la inscripción de las bases de datos en el Registro Nacional de Bases de Datos (RNBD).

Desde el plano internacional, Colombia ha sido aceptada como miembro observador del Convenio 108 del Consejo de Europa, lo que implica un compromiso formal con los estándares internacionales en materia de protección de datos, orientados por principios como el consentimiento informado y la finalidad específica del tratamiento. Estos principios también están alineados con marcos de referencia reconocidos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y las Directrices de la OCDE sobre privacidad.

Por lo tanto, el Tratamiento de Datos Personales se soporta en el reconocimiento de la autonomía informativa, entendida como la facultad de toda persona de conocer, actualizar, rectificar y controlar la información que le concierne. Este concepto de autonomía informativa ha sido ampliamente desarrollado por la jurisprudencia constitucional colombiana, en particular por la Corte Constitucional a través de sentencias como la C-1011 de 2008 y la C-748 de 2011, donde se define el habeas data como un derecho autónomo. Dichas decisiones también establecen los límites al tratamiento de datos personales, especialmente en lo relacionado con datos sensibles o de menores de edad

En el contexto institucional, el Tratamiento de Datos Personales es transversal a los procesos estratégicos, misionales, de apoyo y de evaluación. Esta política, por tanto, se fundamenta en la necesidad de aplicar un enfoque preventivo, sistemático y ético en la gestión de la información personal, con el fin de fortalecer la confianza pública, prevenir incidentes de seguridad y garantizar el respeto por los derechos fundamentales de los titulares de los datos.

10. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES (RUTA DE IMPLEMENTACIÓN)

A continuación, se establece la ruta para la ejecución de la Política de Tratamiento de Datos Personales, de acuerdo con las disposiciones normativas vigentes y los principios orientadores previamente definidos. Esta ruta contempla las acciones que deben adoptarse para garantizar el cumplimiento de las obligaciones legales en materia de recolección, almacenamiento, uso, circulación, supresión, transmisión y transferencia de datos personales. Así mismo, busca proporcionar claridad a todos los actores institucionales sobre los procedimientos, roles y mecanismos de protección aplicables, con el fin de consolidar una cultura organizacional basada en la ética, la legalidad y la salvaguarda de los derechos fundamentales de los titulares.

10.1. TRATAMIENTO Y FINALIDADES

De conformidad con lo establecido en la Ley 1581 de 2012, sus decretos reglamentarios y las directrices de la Superintendencia de Industria y Comercio, el JBJCM en calidad de responsable del tratamiento, llevará a cabo diversas operaciones relacionadas con la recolección, almacenamiento, uso, circulación y supresión de datos. Estas actividades de Tratamiento de Datos se realizarán exclusivamente para las finalidades autorizadas y establecidas en la presente política, así como en las autorizaciones específicas otorgadas por los titulares.

El tratamiento se llevará a cabo respetando en todo momento los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, garantizando el ejercicio pleno del derecho fundamental al habeas data por parte de los titulares.
Así mismo, el JBJCM podrá llevar a cabo el Tratamiento de Datos Personales sin autorización previa del titular en los casos expresamente permitidos por la Ley Estatutaria 1581 de 2012, como cuando medie una orden judicial, exista una obligación legal, los datos sean de naturaleza pública o estén relacionados con información histórica, estadística o científica, debidamente anonimizada, siempre cumpliendo con el Manual de Políticas Específicas del Modelo de Seguridad y Privacidad de la Información SDI.PR.01.M.02. del JBJCM
En cumplimiento de su objeto misional, el JBJCM tratará los datos personales de acuerdo con los grupos de interés y en proporción a las finalidades específicas de cada tratamiento, tal como se describe a continuación:

- **A. CIUDADANOS:** El Tratamiento de Datos Personales para este grupo de interés tendrá las siguientes finalidades:

1. Controlar y gestionar las solicitudes relacionadas con los servicios prestados por el JBJCM.
2. Responder a consultas y derechos de petición presentados por los titulares de los datos.
3. Realizar trámites, servicios y otros procedimientos administrativos solicitados por los interesados.
4. Enviar comunicaciones y notificaciones de actos administrativos emitidos por las áreas de la Entidad.
5. Realizar campañas, actividades de divulgación y capacitaciones, tanto presenciales como virtuales.
6. Desarrollar e implementar programas relacionados con la misión del JBJCM.
7. Actualizar y gestionar bases de datos, incluyendo la validación, depuración, enriquecimiento y homogenización de datos, en cumplimiento de las exigencias legales.
8. Permitir el acceso y Tratamiento de Datos por parte de proveedores y contratistas involucrados en trámites y servicios definidos en sus contratos.

9. Elaborar estadísticas, estudios, encuestas y análisis de tendencias relacionados con los servicios prestados por la Entidad.
10. Presentar informes a entidades externas para cumplir con las obligaciones legales aplicables al JBJCM.
11. Gestionar la información necesaria para el cumplimiento de obligaciones tributarias, contractuales, comerciales y registros requeridos por la Entidad.
12. Transferir información a terceros encargados nacionales o internacionales que provean servicios necesarios para el funcionamiento adecuado del Jardín Botánico.
13. Prestar servicios de información a través de diferentes medios de contacto.
14. Evaluar la calidad de los servicios prestados mediante la grabación de imágenes u otros registros de eventos y audiencias.
15. Mejorar las iniciativas y actualización de productos y/o servicios ofrecidos por el JBJCM.
16. En caso de datos biométricos capturados a través de sistemas de videovigilancia o grabación, el tratamiento de dichos datos tendrá como finalidad la identificación, seguridad y prevención, en cumplimiento de las disposiciones legales y en resguardo de la integridad y seguridad de la Entidad.
17. Atender cualquier otra finalidad legítima y proporcional informada al momento de la recolección de los datos y enmarcada en las competencias legales de la Entidad.
18. Las demás finalidades determinadas durante la obtención de datos personales, siempre en cumplimiento de la ley y en el marco de las funciones atribuibles a la Entidad.

- **B. FUNCIONARIOS:** El Tratamiento de Datos Personales para este grupo de interés tendrá las siguientes finalidades

1. Realizar las actividades necesarias para cumplir con las obligaciones legales relacionadas con los funcionarios y exfuncionarios de la Entidad, incluyendo la gestión de información personal y laboral requerida por la normativa aplicable.
2. Controlar el cumplimiento de los requisitos establecidos en el Sistema General de Seguridad Social, tanto para los funcionarios como para los beneficiarios, con el fin de garantizar el cumplimiento de las obligaciones legales y la protección de los derechos de los involucrados.
3. Publicar un directorio corporativo con la finalidad de facilitar el contacto entre los empleados y fomentar la comunicación interna dentro de la Entidad.
4. En caso de datos biométricos capturados a través de sistemas de videovigilancia o grabación, el tratamiento de dichos datos tendrá como finalidad la identificación, seguridad y prevención de fraudes internos y externos, en cumplimiento de las disposiciones legales y en resguardo de la integridad y seguridad de la Entidad.
5. Tratar los datos personales de niños, niñas y adolescentes únicamente cuando dicho tratamiento sea necesario para el cumplimiento de obligaciones legales relacionadas con su protección integral, bienestar, desarrollo armónico y el ejercicio de sus derechos, conforme a lo establecido en la normatividad vigente.
6. En el caso de los participantes en convocatorias de selección, los datos personales tratados tendrán como finalidad gestionar los procesos de selección, respetando el principio de acceso restringido para garantizar la confidencialidad de la información.
7. Informar y comunicar de manera general los eventos desarrollados por la Entidad, utilizando los medios y las formas que se consideren convenientes para llegar a los destinatarios de dicha información.
8. Gestionar la cadena presupuestal de la Entidad, lo que incluye el registro y control de los pagos efectuados, la emisión de certificados de ingresos y retenciones para personas naturales y jurídicas, así como la elaboración de relaciones de pagos, con el fin de garantizar la trazabilidad, el cumplimiento normativo y la adecuada ejecución del presupuesto institucional.

9. Gestionar el proceso contable de la Entidad, asegurando el registro oportuno, veraz y ordenado de la información financiera y contable, conforme a las normas contables vigentes y principios de contabilidad pública, con el propósito de facilitar la toma de decisiones, el control interno y la rendición de cuentas.
10. Realizar otras finalidades que sean determinadas en los procesos de obtención de datos personales, siempre y cuando estén de acuerdo con la ley y se enmarquen en las funciones atribuibles a la Entidad

- **C. PROVEEDORES/CONTRATISTAS:** El Tratamiento de Datos Personales para este grupo de interés tendrá las siguientes finalidades:

1. Utilizar los datos personales con fines relacionados con los procesos de selección, tanto para la evaluación de candidatos como para la celebración de contratos o cualquier otro aspecto vinculado a estos procesos.
2. Realizar los trámites internos necesarios y cumplir con las obligaciones contables, tributarias y legales correspondientes, utilizando los datos personales en el marco de estas actividades.
3. Gestionar la cadena presupuestal de la Entidad, lo cual incluye los pagos realizados, la emisión de certificados de ingresos y retenciones tanto para personas naturales como jurídicas, así como la elaboración de relaciones de pagos necesarias para el adecuado registro y control financiero.
4. Gestionar el proceso contable de la Entidad, asegurando el correcto registro y control de la información financiera y contable en cumplimiento de las normas y principios contables aplicables.
5. Realizar todas las actividades necesarias para el cumplimiento de las diferentes etapas contractuales en las relaciones con proveedores y contratistas, lo cual implica el uso de datos personales en el marco de dichas gestiones.
6. Expedir las certificaciones contractuales solicitadas por los contratistas de la Entidad o por entes de control competentes, utilizando los datos personales pertinentes para dichas certificaciones.
7. Mantener un archivo digital que permita contar con la información correspondiente a cada contrato, lo cual incluye el almacenamiento y gestión de los datos personales relacionados con dichos contratos.
8. Realizar otras finalidades que sean determinadas en los procesos de obtención de datos personales, siempre y cuando estén de acuerdo con la ley y se enmarquen en las funciones atribuibles a la Entidad.

10.1.1. Tratamiento de Datos Sensibles, Niños, Niñas y Adolescentes

Los datos sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelan el origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, datos de salud, vida sexual o datos biométricos.

En cumplimiento de lo establecido en la Ley 1581 de 2012, el JBJCM se abstiene de realizar Tratamiento de Datos Sensibles, salvo cuando se configure alguna de las excepciones expresamente permitidas por la ley, y se garantice en todo momento el respeto de los derechos fundamentales de los titulares, de acuerdo con las siguientes condiciones:

- El titular haya dado su autorización explícita para el tratamiento de los datos sensibles, o, en el caso de niños, niñas y adolescentes, dicha autorización sea otorgada por su representante legal, a menos que exista una excepción legal en la que no se requiera dicha autorización. El tratamiento de datos sensibles sea necesario para salvaguardar el interés vital del titular y este

se encuentre física o jurídicamente incapacitado. En estos casos, se requerirá la autorización del representante legal.

- El tratamiento de datos sensibles esté relacionado con información necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento de datos sensibles tenga una finalidad histórica, estadística o científica. En este caso, se deben tomar las medidas necesarias para garantizar la supresión de la identidad de los titulares de los datos sensibles.

En todos los casos, se aplicarán medidas técnicas, organizativas y jurídicas que garanticen la seguridad, confidencialidad, integridad y reserva de la información tratada.

- Adicionalmente, el Tratamiento de Datos Personales de niños, niñas y adolescentes está generalmente prohibido, salvo en los casos expresamente autorizados por la Ley 1581 de 2012 y el Decreto 1377 de 2013. En estos casos, el tratamiento - incluyendo tanto datos personales como datos sensibles - solo será permitido cuando: El tratamiento de los datos debe responder y respetar el interés superior de los niños, niñas y adolescentes. Esto implica que se debe garantizar su bienestar y protección en todas las actividades de Tratamiento de Datos en las que estén involucrados.
- El Tratamiento de Datos debe asegurar el respeto de los derechos fundamentales de los niños, niñas y adolescentes. Esto incluye el derecho a la intimidad, la privacidad, la identidad y la no discriminación, entre otros.

El tratamiento de datos personales de niños, niñas y adolescentes requerirá la autorización expresa del representante legal del menor, conforme a lo previsto en la Ley 1581 de 2012 y demás normatividad aplicable. Adicionalmente, y en cumplimiento del principio del interés superior del menor y del respeto por su autonomía progresiva, deberá asegurarse que el niño, niña o adolescente sea escuchado y su opinión valorada, en la medida en que su nivel de madurez, desarrollo evolutivo y capacidad para comprender el objeto del tratamiento lo permitan.

El JBJCM garantizará que el Tratamiento de Datos Personales de niños, niñas y adolescentes se realice conforme a los principios de legalidad, proporcionalidad y necesidad, respetando siempre el interés superior del menor. Para ello, además del cumplimiento de los requisitos establecidos en la Ley 1581 de 2012 y el Decreto 1377 de 2013, la Entidad implementará acciones de sensibilización dirigidas al personal involucrado y controles reforzados de seguridad de la información, con el fin de asegurar que dicho tratamiento sea transparente, justificado y se limite estrictamente a los fines específicos que motivaron su recolección.

10.2. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

El JBJCM, en el marco de sus funciones legales y contractuales, podrá realizar la transferencia y transmisión de datos personales a terceros, nacionales o internacionales, cuando ello sea necesario para el adecuado desarrollo de sus actividades, la ejecución de procesos operativos, administrativos, científicos, educativos o contractuales, y en cumplimiento de obligaciones legales o decisiones judiciales.

En todos los casos, la Entidad se asegurará de que el tratamiento de los datos personales transferidos o transmitidos cumpla con los principios, finalidades y garantías establecidos en la Ley 1581 de 2012, sus normas reglamentarias, la presente política y los estándares internacionales suscritos por Colombia en materia de protección de datos personales.

10.2.1. Transferencia de datos personales

Se entiende como aquella operación mediante la cual el responsable del tratamiento, es decir el JBJCM, remite la información a otro responsable, dentro o fuera del país, quien a su vez realizará un tratamiento autónomo de dichos datos.

Esta operación solo podrá realizarse cuando:

- Exista autorización previa, expresa e informada por parte del titular, o cuando la ley expresamente lo autorice.
- Se garantice un nivel adecuado de protección por parte del receptor de los datos, especialmente si se encuentra fuera del territorio colombiano.
- Se cumplan los requisitos exigidos por la Superintendencia de Industria y Comercio y las demás autoridades competentes.

10.2.2. Transmisión de datos personales

Se refiere al tratamiento que realiza un encargado, por cuenta del JBJCM como responsable, para cumplir una finalidad específica previamente autorizada.

Cuando la transmisión de datos personales se realice a encargados del tratamiento ubicados dentro o fuera del territorio colombiano, el JBJCM suscribirá un contrato de transmisión o incluirá cláusulas contractuales específicas que regulen dicha transmisión. Este instrumento deberá garantizar que el encargado del tratamiento trate los datos personales únicamente conforme a las instrucciones del JBJCM, observe estrictamente los principios y obligaciones establecidos en la Ley 1581 de 2012, y asegure la implementación de medidas técnicas, humanas y administrativas necesarias para la protección de la información con al menos, las siguientes disposiciones:

- El alcance y duración del tratamiento autorizado.
- Las actividades específicas que el encargado podrá realizar respecto de los datos.
- Las obligaciones del encargado frente al responsable y frente al titular de los datos.
- Las medidas técnicas, organizativas y jurídicas que garanticen la seguridad, confidencialidad, integridad, conservación y uso legítimo de la información.

A través de este contrato, el encargado se comprometerá a cumplir con las obligaciones establecidas por el responsable en su Política de Tratamiento de la Información y a realizar el Tratamiento de Datos de acuerdo con la finalidad autorizada por los titulares y las leyes aplicables. Además de las obligaciones establecidas por las normas aplicables y dentro del contrato mencionado, se deben incluir las siguientes obligaciones para el encargado:

- Tratar los datos personales exclusivamente bajo las instrucciones del JBJCM y conforme a la legislación vigente.
- Abstenerse de utilizar los datos para finalidades distintas a las establecidas contractualmente.
- Implementar y mantener medidas de seguridad adecuadas para evitar accesos no autorizados, pérdida, alteración o divulgación indebida.
- Garantizar la confidencialidad y reserva de la información, incluso una vez finalizada la relación contractual.

Estas medidas contractuales y técnicas buscan asegurar que la transferencia o transmisión de datos personales no vulnere los derechos fundamentales de los titulares y que las operaciones asociadas a terceros se realicen bajo criterios de transparencia, trazabilidad y responsabilidad demostrada.

10.3. DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

El respeto y garantía de los derechos de los titulares constituye uno de los pilares fundamentales del régimen de protección de datos personales en Colombia. A continuación, se establecen los derechos que asisten a los titulares respecto del tratamiento de su información personal, así como las condiciones de legalidad que deben observarse por parte del JBJCM en su calidad de responsable del tratamiento. En concordancia con la Ley 1581 de 2012, sus decretos reglamentarios y las directrices de la Superintendencia de Industria y Comercio, se detallan las garantías, procedimientos y requisitos necesarios para asegurar un tratamiento legítimo, transparente y respetuoso de los datos personales en poder de la Entidad.

10.3.1. Derechos de los Titulares

En el Tratamiento de Datos Personales por parte del JBJCM se respetarán en todo momento los derechos de los titulares. A continuación, se describen los derechos que podrán ejercer:

a. Derecho de Acceso: Tiene derecho a solicitar y obtener información sobre los datos personales que el JBJCM tiene almacenados y cómo se están utilizando.
b. Derecho de Actualización y Rectificación: Puede solicitar la actualización o corrección de sus datos personales si son inexactos, incompletos o han cambiado.
c. Derecho de Supresión: También conocido como derecho al olvido, puede solicitar la eliminación de sus datos personales cuando considere que ya no son necesarios para los fines para los que fueron recopilados, cuando haya revocado su consentimiento o cuando se haya cumplido el plazo de conservación establecido por la ley.
d. Derecho de Oposición: Tiene derecho a oponerse al tratamiento de sus datos personales por motivos relacionados con su situación particular. El JBJCM dejará de procesar sus datos, a menos que existan motivos legítimos imperiosos para continuar con el tratamiento.
e. Derecho de Portabilidad: Puede solicitar la transferencia de sus datos personales a otra entidad o recibirlos en un formato estructurado, de uso común y lectura mecánica, cuando sea técnicamente posible.
f. Derecho de Limitación del Tratamiento: Puede solicitar la restricción del procesamiento de sus datos personales en determinadas circunstancias, por ejemplo, cuando impugne la exactitud de los datos o se haya realizado un tratamiento ilegal.
g. Derecho a Presentar una Queja: Si el titular considera que el JBJCM ha infringido sus derechos en el Tratamiento de Datos Personales, tiene derecho a presentar una queja ante la autoridad de protección de datos competente.

10.3.2. Autorización para el Tratamiento de Datos Personales

El Tratamiento de Datos Personales por parte del JBJCM, se realizará siempre con base en la autorización previa, expresa e informada otorgada por el titular, salvo las excepciones previstas legalmente. Esta autorización podrá otorgarse por medios escritos, orales o mediante conductas inequívocas que permitan concluir de forma razonable que el titular consiente el tratamiento, siempre que exista un medio verificable que permita probar la existencia y contenido de dicha autorización (por ejemplo, grabaciones, actas, o constancias documentadas)
Al momento de la recolección de los datos personales, la Entidad informará al titular sobre:

- La finalidad específica del tratamiento.
- El carácter facultativo de responder preguntas sobre datos sensibles de niños, niñas y adolescentes.
- Los derechos que le asisten como titular.
- Los canales y medios habilitados para consultas, reclamos o solicitudes.
- El acceso a la presente Política de Tratamiento de Datos.

El titular tiene el derecho de revocar la autorización en cualquier momento, mediante una solicitud presentada a través de los canales establecidos por el JBJCM para atender consultas, peticiones y reclamos, los cuales se encuentran descritos en el Capítulo 10.9 ATENCIÓN DE CONSULTAS, PETICIONES Y RECLAMOS del presente documento La revocación de la autorización puede implicar la supresión o modificación total o parcial de los datos, siempre y cuando se cumpla con las siguientes condiciones:

a. La revocación es una decisión unilateral, libre y voluntaria del titular de los datos personales.
b. No exista una obligación legal o contractual que exija al titular permanecer en la base de datos.
c. No se respeten los principios, derechos y garantías constitucionales y legales en el tratamiento de los datos, y la autoridad competente, como la Superintendencia de Industria y Comercio, haya determinado que el responsable o encargado del tratamiento han incurrido en conductas contrarias a la normativa aplicable.

En estos casos, el JBJCM deberá proceder a la supresión o modificación de los datos personales de acuerdo con la solicitud del titular.

Nota: La autorización del Titular, no será necesaria en los casos expresamente establecidos en el artículo 10 de la Ley 1581 de 2012, los cuales incluyen:

a. Información requerida por la Entidad, 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.

Sin embargo, el acceso a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley 1581 de 2012 y demás normas concordantes y vigentes.

10.4. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

El cumplimiento riguroso de los deberes legales y administrativos por parte de quienes intervienen en el Tratamiento de Datos personales es esencial para garantizar la protección efectiva de los derechos de los titulares. Por lo tanto, a continuación, se definen las obligaciones que debe observar el JBJCM, en su calidad de responsable del tratamiento, así como los deberes que asumen los encargados a quienes se les delegue dicho tratamiento. Estas responsabilidades, enmarcadas en la Ley 1581 de 2012, buscan asegurar que todas las operaciones sobre datos personales se ejecuten bajo condiciones de legalidad, seguridad, confidencialidad, trazabilidad y respeto por los principios rectores del régimen de Protección de Datos Personales en Colombia.

10.4.1. Deberes de los responsables del tratamiento

En cumplimiento de lo establecido en el Artículo 17 de la Ley 1581 de 2012, el JBJCM en su calidad de responsable del Tratamiento, deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

- Garantizar el pleno ejercicio del derecho de habeas data por parte del titular en todo momento.
- Solicitar y conservar copia de la autorización otorgada por el titular en las condiciones establecidas por la ley.
- Informar adecuadamente al titular sobre la finalidad de la recolección de datos y los derechos que le corresponden en virtud de la autorización otorgada.
- Mantener la información bajo condiciones de seguridad que eviten su alteración, pérdida, acceso no autorizado o fraude.
- Indicar el carácter facultativo de responder a las preguntas que versen sobre datos sensibles o datos de niñas, niños y adolescentes.
- Informar sobre los derechos que le asisten al titular.
- Garantizar que la información suministrada al encargado del tratamiento sea veraz, completa, precisa, actualizada y comprensible.
- Actualizar la información suministrada al encargado del tratamiento y comunicarle cualquier novedad o cambio pertinente.
- Rectificar la información cuando sea incorrecta y notificar al encargado del tratamiento al respecto.
- Suministrar al encargado del tratamiento únicamente los datos autorizados previamente de acuerdo con la ley.
- Exigir al encargado del tratamiento el cumplimiento de las condiciones de seguridad y privacidad de la información del titular.
- Atender las consultas y reclamos presentados por los titulares de acuerdo con lo establecido en la ley.
- Adoptar procedimientos específicos para garantizar el cumplimiento de la ley y el adecuado manejo de consultas y reclamos.
- Informar al encargado del tratamiento cuando cierta información se encuentre en disputa por parte del titular, una vez se haya presentado una reclamación y el proceso correspondiente no haya finalizado.
- Proporcionar al titular, a solicitud de este, información sobre el uso de sus datos personales.
- Informar a la autoridad de protección de datos en caso de violaciones a los códigos de seguridad y riesgos en la administración de la información de los titulares.

10.4.2. Deberes de los Encargados del Tratamiento

Los encargados del Tratamiento de Datos, incluyendo el JBJCM cuando actúe como encargado, tienen los siguientes deberes:

a. Garantizar al titular el pleno ejercicio del derecho de habeas data en todo momento.
b. Realizar de manera oportuna la actualización, rectificación o supresión de los datos de acuerdo con lo establecido en la Ley 1581 de 2012 y demás normas aplicables.
c. Actualizar la información relacionada con los datos personales, que le sea proporcionada por el responsable del tratamiento, en un plazo máximo de cinco (5) días hábiles desde su recepción, especialmente cuando corresponda a solicitudes de actualización, rectificación o supresión realizadas por el titular.

d. Tramitar las consultas y reclamos presentados por los titulares de acuerdo con los términos y condiciones establecidos en la Política de Tratamiento de Datos.
e. Gestionar la trazabilidad y respuesta dentro de los plazos establecidos, para las consultas, reclamos y solicitudes presentadas por los titulares, según lo dispuesto en la normativa aplicable y en la Política de Tratamiento de Datos.
f. Contar con lineamientos, procedimientos internos u otro mecanismo documentado que permita garantizar el cumplimiento de la ley en lo relacionado con el Tratamiento de Datos Personales, especialmente en lo relacionado con la atención de consultas y reclamos de los titulares.
g. Registrar en las bases de datos la leyenda "reclamo en trámite" de acuerdo con las disposiciones legales correspondientes.
h. Incluir en la base de datos la leyenda "información en discusión judicial" una vez notificado por la autoridad competente sobre procesos judiciales relacionados con la calidad de los datos personales.
i. Abstenerse de circular información que esté siendo objeto de controversia por parte del titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j. Permitir el acceso a la información únicamente a las personas autorizadas para ello.
k. Informar a la Superintendencia de Industria y Comercio en caso de violaciones a los códigos de seguridad y existencia de riesgos en la administración de la información de los titulares.
l. Cumplir con las instrucciones y requerimientos impartidos por la Superintendencia de Industria y Comercio.
m. Verificar que el responsable del tratamiento cuente con la autorización correspondiente para el tratamiento de los datos personales del titular.
n. Designar un área o persona encargada de la función de protección de datos personales.
o. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 de 2012 y atender consultas y reclamos.

10.5. PROCEDIMIENTOS PARA EL TRATAMIENTO DE LOS DATOS

El Tratamiento de Datos Personales por parte del JBJCM se realiza conforme a los procedimientos definidos a continuación, que garantizan el cumplimiento de los principios rectores establecidos por la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás disposiciones complementarias). A continuación, se describen los criterios operativos para la recolección, almacenamiento, uso, circulación, actualización, supresión y transmisión de los datos personales bajo custodia de la entidad. Dichos procedimientos buscan asegurar la transparencia, legalidad, seguridad y trazabilidad en el manejo de la información, así como facilitar el ejercicio de los derechos por parte de los titulares y la debida atención de consultas, quejas o reclamos.

10.5.1. Procedimiento de Consultas

Los documentos de archivo, tanto en soportes físicos como en formatos electrónicos, se pondrán a disposición de los interesados conforme al cumplimiento de las disposiciones legales vigentes sobre acceso a la información. Este acceso estará sujeto a las restricciones que establezca la ley, por lo que los documentos deberán estar debidamente calificados como información pública, clasificada o reservada, de acuerdo con lo consignado en el “Índice de Información Clasificada y Reservada”, y en articulación con los demás instrumentos de la gestión de la información pública.

El JBJCM y/o los encargados se comprometen a garantizar a los titulares de datos personales el derecho de consultar la información contenida en su registro individual, así como cualquier información relacionada con su identificación, de acuerdo con la Política de Tratamiento de Datos Personales. El Oficial de Protección de Datos Personales del JBJCM será el encargado de recibir y gestionar las

solicitudes de consulta, siguiendo los plazos y condiciones establecidos en la Ley 1581 de 2012 y en la presente política.

Para realizar una consulta al JBJCM, se deben proporcionar los siguientes datos mínimos en la solicitud:

1. Nombres y apellidos del titular de los datos, su representante o sus causahabientes.
2. Descripción clara y precisa de la información que desea consultar.
3. Dirección física, dirección de correo electrónico y número de teléfono de contacto del titular de los datos, su representante o sus causahabientes.
4. Firma del solicitante, número de identificación o medio de validación equivalente.
5. La solicitud debe ser presentada a través de los canales de atención habilitados por el JBJCM**.**

Una vez recibida la solicitud de consulta de información por parte del titular de los datos, su representante o un tercero debidamente autorizado, a través de los canales establecidos los cuales se encuentran descritos en el Capítulo 10.9 ATENCIÓN DE CONSULTAS, PETICIONES Y RECLAMOS del presente documento, remitirá la solicitud a la Oficina Asesora de Planeación. Luego, esta oficina la trasladará al Oficial de Protección de Datos Personales, quien verificará el cumplimiento de los requisitos y la legitimación del solicitante. Si la solicitud está incompleta o presenta inconsistencias, se requerirá al interesado para que subsane los defectos dentro de los cinco (5) días hábiles siguientes.

El término máximo para atender consultas es de diez (10) días hábiles contados a partir de la fecha de recepción, de acuerdo con lo establecido en la Ley 1581 de 2012. Si no fuere posible responder dentro de dicho término, se informará al solicitante antes de su vencimiento, expresando los motivos de la demora y señalando la fecha estimada de respuesta, que en ningún caso podrá superar cinco (5) días hábiles adicionales.

La información será suministrada por medios seguros, accesibles y en formato comprensible, protegiendo la confidencialidad y seguridad de los datos personales consultados.

10.5.2. Procedimiento de Reclamos

El JBJCM y/o los Encargados garantizan a los titulares de datos personales el derecho a solicitar la corrección o actualización de los datos personales que se encuentren en sus bases de datos. Así mismo, se garantiza el derecho de solicitar la revocatoria de la autorización o la supresión de la información contenida en el registro individual del titular o cualquier información vinculada a su identificación, cuando se cumplan los parámetros establecidos por la ley o los establecidos en la Política de Tratamiento de Datos Personales.

El Oficial de Protección de Datos Personales del JBJCM es el responsable de recibir y gestionar las solicitudes de reclamos de acuerdo con los términos, plazos y condiciones establecidas en la Ley 1581 de 2012 y en las políticas vigentes.

Para presentar un reclamo al JBJCM, se deben proporcionar los siguientes datos mínimos en la solicitud:

1. Nombres y apellidos del titular, su representante o causahabiente.
2. Descripción clara del reclamo: corrección, actualización, supresión de datos o revocatoria de la autorización.
3. Dirección física, correo electrónico y número de teléfono de contacto.

4. Firma del solicitante, número de identificación o medio de validación equivalente.
5. Documentos que acrediten la representación legal, si aplica.
6. Radicación a través de los canales oficiales definidos por la Entidad para la atención de solicitudes.

Una vez recibida la solicitud de reclamo presentada por parte del titular de los datos, su representante o un tercero debidamente autorizado - relacionada con la corrección, actualización, supresión de datos, revocatoria de la autorización u otro asunto relacionado con el tratamiento de sus datos personales - a través de los canales establecidos, el área correspondiente remitirá la solicitud a la Oficina Asesora de Planeación. Luego, esta Oficina la trasladará al Oficial de Protección de Datos Personales, quien verificará que la solicitud cumpla con todos los requisitos necesarios para evaluar si el derecho se ejerce por parte de un interesado legítimo o su representante, asegurando así la legitimidad legal del reclamo.

Si el reclamo se presenta sin el cumplimiento de los requisitos legales mencionados anteriormente, se solicitará al reclamante que subsane las fallas y presente la información o documentos faltantes dentro de los cinco (5) días siguientes a la recepción del reclamo. Si el solicitante no presenta la información requerida dentro de los dos (2) meses siguientes a la fecha del requerimiento, se considerará que ha desistido del reclamo, de conformidad con lo previsto en el artículo 15 de la Ley 1581 de 2012.

Una vez recibido el reclamo de manera completa, el JBJCM incluirá en la base de datos donde se encuentren los datos personales del titular una leyenda que indique "reclamo en trámite" y el motivo del reclamo. Esta leyenda se mantendrá hasta que el reclamo sea resuelto.

El plazo máximo para atender los reclamos es de quince (15) días hábiles a partir del día siguiente a la fecha de su recepción. Si no es posible atender el reclamo dentro de ese plazo, se informará al interesado sobre los motivos de la demora y la fecha en que se atenderá su reclamo, que no podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer plazo.

Si la reclamación resulta procedente y se requiere la supresión de los datos personales, el JBJCM realizará la eliminación de manera que la información no pueda ser recuperada. Sin embargo, es posible que cierta información deba mantenerse en registros históricos debido al cumplimiento de obligaciones legales de la organización, y la supresión se realizará en relación con el tratamiento activo de los datos y de acuerdo con la solicitud del titular.

En caso de que el JBJCM reciba un reclamo dirigido a otra organización, se remitirá al destinatario correspondiente en un plazo máximo de cinco (5) días hábiles y se informará al reclamante sobre la situación.

10.5.3. Procedimiento de Gestión de Incidentes con Datos Personales

Se considera un incidente de seguridad cualquier anomalía que pueda comprometer la seguridad de las bases de datos o la información contenida en ellas. Es responsabilidad de los funcionarios y contratistas, al detectar o conocer una incidencia, informar de inmediato al Oficial de Protección de Datos Personales.

El Oficial de Protección de Datos Personales, una vez notificado de la incidencia, tomará las medidas oportunas para abordarla y minimizar cualquier impacto negativo. Además, deberá informar sobre la incidencia en el módulo de Mesa de ayuda habilitado para tal efecto dentro de un plazo de 15 días a partir de la fecha en que haya tenido conocimiento de la misma. Esta comunicación permite llevar un

registro adecuado de las incidencias y facilita la gestión y respuesta a situaciones de seguridad de los datos personales.

Las incidencias pueden afectar tanto a bases de datos digitales como físicas y generarán las siguientes actividades:

- **Notificación de Incidentes:** Cualquier funcionario, contratista, o tercero vinculado a la Entidad que identifique o tenga conocimiento de un posible incidente de seguridad deberá reportarlo de inmediato al Oficial de Protección de Datos Personales mediante los canales internos establecidos. El reporte debe realizarse independientemente de si el incidente compromete bases de datos físicas o digitales y deberá seguir lo dispuesto en el Procedimiento: Gestión de Incidentes y/o Evento de Seguridad de la Información – SDI.PR.01.
- **Gestión de Incidentes:** Es responsabilidad de todos los funcionarios, contratistas, consultores o terceros reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que puedan afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de la Entidad.
- **Identificación:** Todos los eventos sospechosos o anormales que puedan comprometer la reserva o confidencialidad de la información deben ser evaluados para determinar si constituyen un incidente. En caso de que se requiera involucrar a las autoridades de investigación y judiciales, la decisión debe tomarse en conjunto entre el Oficial de Protección de Datos Personales y la Oficina Jurídica. La comunicación con dichas autoridades será realizada por ellos mismos.
- **Reporte:** El Oficial de Protección de Datos Personales debe asegurarse de que todos los incidentes y eventos sospechosos sean reportados de manera oportuna a través de los canales internos establecidos por el JBJCM. Esto incluye la pérdida de información sensible o confidencial, divulgación a personal no autorizado o cualquier sospecha de estos eventos. Por lo tanto, el Oficial de Protección de Datos Personales debe ser notificado de inmediato en tales casos. Además, los funcionarios deben reportar cualquier daño o pérdida de computadoras u otros dispositivos que contengan datos personales bajo la responsabilidad de la Entidad. La divulgación de información sobre sistemas de cómputo y redes afectadas por delitos informáticos o abuso de sistema solo debe realizarse si hay una solicitud debidamente razonada y justificada de la autoridad competente, y la Oficina Jurídica debe brindar el asesoramiento adecuado en estos casos.
- **Contención, Investigación y Diagnóstico:** El Oficial de Protección de Datos Personales y el Proceso de Gestión de la Tecnología debe trabajar articuladamente en la toma de acciones para investigar y diagnosticar las causas que generaron el incidente. Además, deben asegurarse de que todo el proceso de gestión del incidente se documente adecuadamente. En caso de que se identifique un delito informático de acuerdo con lo establecido en la Ley 1273 de 2009, el Oficial de Protección de Datos Personales y la Oficina Jurídica deben reportar dicha información a las autoridades de investigaciones judiciales correspondientes. Durante los procesos de investigación, se debe garantizar la "Cadena de Custodia" con el fin de preservarla en caso de que sea necesario para establecer una acción legal.
- **Solución:** La Oficina Asesora de Planeación, en colaboración con el Proceso de Gestión de la Tecnología y cualquier otra área involucrada, así como las dependencias o procesos que realizan Tratamiento de Datos Personales deben trabajar para prevenir la recurrencia del incidente de seguridad. Esto implica corregir todas las vulnerabilidades existentes y tomar las medidas necesarias para fortalecer la protección de los datos.
- **Cierre de Incidente y Seguimiento:** El Proceso de Gestión de la Tecnología, en conjunto con el Oficial de Protección de Datos Personales y las áreas que utilizan o requieren la información, serán responsables de iniciar y documentar todas las tareas de revisión de las acciones llevadas

a cabo para remediar el incidente de seguridad. Además, el Oficial de Protección de Datos Personales preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán para desarrollar campañas de concientización que ayuden a reducir la probabilidad de incidentes futuros.

- **Reporte de incidentes ante la SIC como autoridad de control:** Los incidentes de seguridad que afecten la base de datos deben ser reportados como novedades. Para ello, en el menú de cada base de datos registrada en el sistema, se presentarán dos opciones:
    - En caso de violación de los códigos de seguridad, pérdida, robo o acceso no autorizado de información en una base de datos administrada por el Responsable del Tratamiento o su Encargado, se deben reportar al Registro Nacional de Bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que sean detectados y puestos en conocimiento de la persona o área encargada de atenderlos.
    - Los líderes de proceso y/o propietarios de activos de información deben reportar internamente los incidentes asociados a datos personales al Oficial de Protección de Datos Personales, quien deberá reportarlos al Registro Nacional de Bases de Datos dentro del plazo legal establecido.

10.6. USO DE LA INFORMACIÓN

La información de carácter personal contenida en las bases de datos administradas por JBJCM, deberá ser utilizada exclusivamente para las finalidades previamente definidas y autorizadas, conforme a lo dispuesto en el Capítulo 11.1 de la presente política.
Cualquier nuevo uso de los datos personales que no se encuentre previsto en esta política deberá ser notificado a la Oficina Asesora de Planeación por parte de las dependencias, procesos, funcionarios y/o contratistas que propongan o pretendan implementar dicho tratamiento, la cual evaluará su pertinencia y, de ser procedente, gestionará su inclusión en la política de Tratamiento de Datos Personales, garantizando la trazabilidad, el cumplimiento normativo y la transparencia institucional.

Con el fin de salvaguardar los principios de finalidad, legalidad y confidencialidad, deberán observarse las siguientes directrices:

- **Reutilización de datos por otras áreas:** Si un área diferente a la que inicialmente recolectó los datos personales requiere hacer uso de dicha información, solo podrá hacerlo cuando el nuevo uso sea previsible en relación con las funciones de la Entidad y se ajuste a las finalidades autorizadas por el titular y descritas en la presente política.
- **Reciclaje de documentos físicos**: Está prohibido reciclar documentos que contengan información personal o confidencial, como hojas de vida, títulos académicos, certificados laborales, resultados de exámenes médicos, entre otros. Toda eliminación de estos documentos debe hacerse mediante procesos seguros que garanticen la destrucción definitiva de los datos.
- **Restricción de uso entre áreas y encargados:** Cuando una base de datos es entregada por un encargado o procesador de datos a un área interna para una finalidad específica, dicha área no podrá utilizar la información para propósitos distintos. Al finalizar la actividad, la base de datos deberá ser eliminada conforme a los lineamientos de protección y conservación definidos por la Entidad.
- **Decisiones con base en datos personales:** Ningún funcionario podrá tomar decisiones significativas que afecten los derechos del titular (tales como decisiones legales, laborales o administrativas) basándose exclusivamente en información almacenada en sistemas. En todos los casos, deberá validarse dicha información por medios físicos, documentales o mediante contacto directo con el titular.

- **Control de accesos y privilegios:** El acceso, modificación o eliminación de datos personales solo podrá ser realizado por funcionarios o contratistas expresamente autorizados. Los permisos de acceso serán gestionados por el Proceso de Gestión de la Tecnología, con base en los perfiles funcionales definidos por los líderes de proceso responsables del uso de la información.
- **Consultas excepcionales:** Cualquier uso de la información que no esté previsto o se aparte de lo estipulado en esta política deberá ser consultado y autorizado previamente por la Oficina Asesora de Planeación, para verificar su legalidad y conveniencia institucional.

Estas disposiciones buscan garantizar un uso adecuado y responsable de la información personal, prevenir accesos indebidos, y asegurar el cumplimiento de los principios de protección de datos personales, conforme a la normativa vigente.

10.7. ALMACENAMIENTO DE INFORMACIÓN

El JBJCM reconoce la importancia de garantizar que el almacenamiento de los datos personales bajo su custodia se realice en entornos que cumplan con estándares adecuados de seguridad, tanto para soportes digitales como físicos. En este sentido, la Entidad se encuentra en un proceso de fortalecimiento progresivo de sus mecanismos de protección, con el objetivo de preservar la integridad, confidencialidad y disponibilidad de la información, conforme a los principios establecidos en la normativa vigente.

10.7.1. Almacenamiento de Información Electrónica

La información en formato digital es almacenada en sistemas y redes seguras, con medidas de protección implementadas que incluyen, entre otras:

- Infraestructura con control de acceso lógico.
- Mecanismos de autenticación y autorización con base en perfiles definidos.
- Cifrado de datos en tránsito y en reposo, cuando aplique.
- Firewalls, antivirus corporativos y políticas de actualización permanente.

Estas medidas permiten mitigar riesgos de acceso no autorizado, pérdida, fuga, alteración o uso indebido de los datos personales administrados por la Entidad.
Así mismo, la preservación digital a largo plazo aplica a los documentos electrónicos de archivo en cualquier etapa del ciclo de vida documental. Esta preservación busca garantizar las características de autenticidad, integridad, inalterabilidad, fiabilidad y disponibilidad de los documentos a lo largo del tiempo. Para ello deberán aplicar el Plan de Preservación Digital a largo plazo, conforme a los lineamientos establecidos por la normativa vigente.

10.7.2. Almacenamiento de Información Física

La información contenida en documentos físicos es resguardada en áreas con acceso restringido y controlado, ya sea en instalaciones propias del JBJCM o en centros documentales gestionados por terceros que cumplan con los niveles de seguridad exigidos por la Entidad. Las medidas incluyen:

- Espacios físicos con cerraduras y vigilancia.
- Custodia documental por personal autorizado.
- Procedimientos definidos para el archivo, conservación y disposición final de documentos.

- Condiciones ambientales adecuadas para la conservación de documentos (temperatura, humedad, iluminación).

10.7.3. Objetivo de las medidas de seguridad

Las medidas adoptadas por el JBJCM tienen como objetivo principal prevenir la adulteración, pérdida, consulta, acceso o uso no autorizado o fraudulento de los datos personales, asegurando el cumplimiento de los principios rectores del tratamiento: legalidad, seguridad, confidencialidad, acceso restringido y circulación controlada.

Cualquier tercero que administre sistemas de información o gestione repositorios físicos por encargo del JBJCM deberá cumplir con las mismas medidas de seguridad exigidas a la Entidad, en virtud de los contratos de transmisión o acuerdos de confidencialidad suscritos.

10.8. DISPOSICIÓN FINAL Y DESTRUCCIÓN SEGURA DE LA INFORMACIÓN

De acuerdo con la valoración documental registrada en las Tablas de Retención Documental (TRD) para la totalidad de las series y subseries documentales sin importar el soporte físico o los formatos electrónicos que las conformen, El JBJCM adoptará medidas técnicas y organizativas para garantizar la destrucción segura e irreversible de los soportes que contengan datos personales, una vez cumplida su finalidad o expirado el término de conservación establecido, siempre que dicha destrucción no contravenga disposiciones legales o contractuales vigentes.

Tanto la destrucción de medios físicos como electrónicos se realiza de forma segura y confiable para garantizar la eliminación completa de la información contenida en ellos. Esto implica el uso de métodos apropiados, como la trituración o el borrado seguro de los medios electrónicos, que aseguran que los datos no puedan ser recuperados o accedidos indebidamente.

Es importante destacar que este proceso de destrucción se aplica tanto a los medios físicos y electrónicos en posesión del JBJCM como a aquellos que se encuentren en poder de terceros, siempre y cuando exista una relación contractual o legal que establezca la responsabilidad del JBJCM sobre dicha información.

Además, se asegura la trazabilidad de la acción de destrucción mediante el correspondiente registro documental establecido en el procedimiento de disposición final de documentos del proceso de Gestión Documental de la Entidad o en los inventarios de activos de información, según el tipo de soporte, este registro debe documentar de manera clara el procedimiento utilizado, los medios destruidos, la fecha de ejecución, los responsables de la acción y cualquier otra información que permita verificar que la destrucción se realizó conforme a los protocolos establecidos. Esta medida busca prevenir accesos no autorizados, divulgación indebida o uso fraudulento de los datos personales gestionados por el JBJCM.

10.9. ATENCIÓN DE CONSULTAS, PETICIONES Y RECLAMOS

El JBJCM, pone a disposición los siguientes canales para la atención de consultas, peticiones y reclamos referentes al Tratamiento de Datos Personales.

- Presencial: Calle 63 # 68 - 95 Bogotá D.C. a través de la ventanilla única de correspondencia en la misma dirección.
- Telefónico: 6014377060.

- Correo electrónico: correspondencia@jbb.gov.co

10.10. REGISTRO NACIONAL DE BASE DE DATOS

De conformidad con el artículo 25 de la Ley 1581 de 2012, el Decreto 886 de 2014 y demás disposiciones reglamentarias, el JBJCM, en su calidad de responsable del Tratamiento de Datos Personales, se compromete a realizar el registro de sus bases de datos ante el Registro Nacional de Bases de Datos (RNBD), administrado por la SIC.

El registro, actualización y reporte de novedades será gestionado por el Oficial de Protección de Datos Personales del JBJCM, en coordinación con las dependencias responsables de cada base de datos, y se realizará de manera oportuna, conforme a los plazos y condiciones definidos por la SIC. Adicionalmente, cualquier modificación sustancial en el contenido de las bases de datos, los encargados o las finalidades deberá ser registrada dentro del término legal correspondiente.

El cumplimiento de esta obligación tiene como objetivo principal garantizar la transparencia en el tratamiento de los datos personales y permitir el ejercicio efectivo del derecho de hábeas data por parte de los titulares.

10.11. APLICABILIDAD

La presente Política de Tratamiento de Datos Personales, junto con sus objetivos, lineamientos, procedimientos, manuales y demás documentos complementarios o derivados, es de obligatorio cumplimiento para todos los actores que intervienen directa o indirectamente en el Tratamiento de Datos Personales en el JBJCM. De conformidad a lo establecido en el alcance del presente documento

Esto incluye, sin excepción, a:

- Servidores públicos de planta y provisionales.
- Contratistas y consultores externos.
- Proveedores que actúen como encargados del tratamiento.
- Terceros con los que exista una relación contractual, legal o funcional que implique el acceso, uso, almacenamiento, transmisión o eliminación de datos personales en poder de la Entidad.

El incumplimiento de los lineamientos aquí contenidos podrá dar lugar a sanciones disciplinarias, contractuales o legales, conforme a la normatividad vigente aplicable.

10.12. LINEAMIENTOS, REVISIÓN Y VIGENCIA

Las directrices contenidas en la presente política constituyen el marco general que orienta el Programa de Protección de Datos Personales del JBJCM. Cada una de ellas deberá ser desarrollada mediante instrumentos operativos, procedimientos internos, protocolos de seguridad y campañas de formación, que permitan la aplicación práctica, coherente y verificable del régimen de protección de datos.

La presente política será objeto de revisión periódica, o cuando se presenten cambios normativos, tecnológicos, organizacionales o de contexto que así lo exijan, garantizando que su contenido sea siempre oportuno, suficiente y eficaz.

Este proceso será liderado por el Jefe de la Oficina Asesora de Planeación, o por quien se designe formalmente, quien deberá asegurar la participación de las áreas responsables del Tratamiento de Datos y del Oficial de Protección de Datos Personales.

11. BIBLIOGRAFIA

- Modelo de Seguridad y Privacidad de la Información. (28 de Octubre de 2021). *Ministerio de Tecnologías de la Información y las Comunicaciones MSPI.* Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

- Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995]. (01 de 07 de 2020). *Departamento Nacional de Planeación.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

- Ley 1712. (6 de 03 de 2014). *https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

- ISO/CEI 27000. (30 de 02 de 2018). *Organización Internacional para la Estandarización ISO*. Obtenido de https://www.iso.org/standard/73906.html

- Ley Estatutaria 1581. Art 3. (18 de octubre de 2012). *EL CONGRESO DE COLOMBIA.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

- Superintendencia de Industria y Comercio. (Sin Fecha). *Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability).* Obtenido de Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability): https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

- Superintendencia de Industria y Comercio. (Sin Fecha). Guía sobre el tratamiento de datos personales en las entidades estatales. Obtenido de Guía sobre el tratamiento de datos personales en las entidades estatales: https://www.sic.gov.co/content/guía-sobre-el-tratamiento-de-datos-personales-en-las-entidades-estatales

- Corte Constitucional de Colombia. (2008). Sentencia C-1011 de 2008. M.P. Jaime Araújo Rentería. Bogotá D.C.

- Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011. M.P. Jorge Iván Palacio. Bogotá D.C.

- Corte Constitucional de Colombia. (2002). Sentencia T-729 de 2002. M.P. Rodrigo Escobar Gil. Bogotá D.C.

12. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
13/10/2023	1	Política de Tratamiento de Datos Personales.
22/08/2025	2	Actualización de Política de Tratamiento de Datos personales, alineada con las directrices institucionales de control de calidad y el marco normativo vigente, incluyendo ampliaciones y ajustes necesarios, con el fin de mejorar la gestión de riesgos asociados al tratamiento de datos personales.

13. AUTORIZACIONES

PROCESO		
ELABORÓ	**APROBÓ**	
Nombre(s): Paola Ambrosio	**Nombre(s):** Sandra Marcela Torres	
Cargo(s): Contratista – Oficina Asesora de Planeación	**Cargo(s):** Jefe Oficina Asesora Planeación	

OFICINA ASESORA DE PLANEACIÓN					
REVISÓ		**APROBÓ**		**PUBLICÓ**	
Nombre(s):	José David Hernández M. Jennsy Paola Borrero R	**Nombre(s):**	Sandra Marcela Torres	**Nombre(s):**	José David Hernández M.
Cargo(s): Contratistas MIPG - SIG Oficina Asesora de Planeación		**Cargo(s):** Jefe Oficina Asesora Planeación		**Cargo(s):** Contratista MIPG - SIG Oficina Asesora de Planeación	