

JURISDICCIÓN ESPECIAL PARA LA PAZ
JEP

SECRETARÍA EJECUTIVA

Oficina Asesora de Atención a la Ciudadanía

Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales

ESTRATEGIA INSTITUCIONAL PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE
TRATAMIENTO DE DATOS PERSONALES DE LA JEP

Contenido

INTRODUCCIÓN	3
1. Descripción de la estrategia	6
1.1. Marco de Referencia	6
1.2. Marco Normativo	9
2. Diagnóstico	13
2.1. Contexto	13
2.2. Problema Central	14
2.3. Análisis del Problema (Árbol de Problemas)	14
2.4. Representación del Árbol de Problema	15
Ilustración 1. Representación del Árbol de Problema	15
3. Objetivos generales y específicos de la estrategia	16
3.1. Objetivo General	16
3.2. Objetivos Específicos	16
4. Líneas de Acción	16
5. Implementación de la Estrategia	23

INTRODUCCIÓN

La Constitución Política de Colombia consagra un marco de garantías fundamentales que orienta el tratamiento de la información y la protección de los datos personales. En particular, el artículo 15 garantiza el derecho a la intimidad personal y familiar y al buen nombre, así como el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Asimismo, dispone que en la recolección, tratamiento y circulación de datos deben respetarse la libertad y las demás garantías consagradas en la Constitución. Por su parte, el artículo 20 reconoce el derecho a informar y recibir información veraz e imparcial, así como el derecho a la rectificación en condiciones de equidad.

En desarrollo de este mandato constitucional, se expidió la Ley Estatutaria 1581 de 2012, mediante la cual se estableció el régimen general de protección de datos personales en Colombia, definiendo los principios, derechos, deberes y procedimientos aplicables al tratamiento de la información contenida en bases de datos de naturaleza pública y privada. Esta normativa fue reglamentada inicialmente por los Decretos 1377 de 2013 y 886 de 2014, actualmente compilados en el Decreto Único Reglamentario 1074 de 2015, el cual consolida las disposiciones generales que regulan la protección de datos personales en el país. Asimismo, la Ley 1581 de 2012 fue reglamentada parcialmente por el Decreto 1081 de 2015, particularmente en lo relacionado con el acceso y tratamiento de datos personales en el marco del derecho de acceso a la información pública.

De manera complementaria, la Ley 1712 de 2014 desarrolló el derecho fundamental de acceso a la información pública, estableciendo como principio rector la publicidad de la información en poder de los sujetos obligados. En particular, el artículo 2 dispone el principio de máxima publicidad para el titular universal, según el cual toda información en posesión, bajo control o custodia de una entidad pública se presume pública, salvo las excepciones expresamente previstas en la Constitución Política o en la ley. En este contexto, las entidades públicas deben armonizar el principio de transparencia con la protección de los datos personales y la garantía de los derechos fundamentales asociados al tratamiento de la información.

De otra parte, el Acto Legislativo 01 de 2017 incorporó al ordenamiento jurídico colombiano el Sistema Integral para la Paz (SIP) y creó, mediante su artículo transitorio 5°, la Jurisdicción Especial para la Paz (en adelante la JEP o la Jurisdicción), como el componente de justicia del Sistema, con autonomía administrativa, presupuestal y técnica para administrar justicia de manera transitoria y preferente respecto de las conductas cometidas con ocasión del conflicto armado antes del 10 de diciembre de 2016. En cumplimiento de su mandato constitucional y legal, la JEP administra un volumen significativo de información, gran parte de ella clasificada como datos personales y datos sensibles, cuya gestión exige la adopción de mecanismos robustos de gobernanza, seguridad y cumplimiento normativo.

En este contexto, y en observancia del marco constitucional y legal vigente, la JEP estableció los principios generales que orientan el tratamiento de los datos personales mediante el Acuerdo AOG 030 de 2022¹. Este instrumento definió las bases institucionales para garantizar que el tratamiento de la información personal se realice conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, en armonía con la Constitución Política y la normativa vigente sobre protección de datos personales.

Posteriormente, en el año 2023, la JEP formuló la primera versión de la Estrategia Institucional para la Implementación de la Política de Tratamiento de Datos Personales, en adelante PTDP, concebida como el primer instrumento de planeación y gestión orientado a establecer los lineamientos, acciones y mecanismos necesarios para implementar de manera progresiva dicha la Política. Este instrumento permitió definir una hoja de ruta institucional para fortalecer el cumplimiento de las obligaciones legales en la materia, promover la apropiación de la cultura de protección de datos personales y orientar la implementación de acciones de prevención, seguimiento y mejora continua.

En el marco del desarrollo de la primera Estrategia Institucional para la Implementación de la PTDP, definida en 2023, e implementada en la vigencia 2024, la JEP ha desarrollado acciones orientadas a fortalecer la gestión institucional de la protección de datos personales (PDP) y consolidar una cultura de cumplimiento en la materia. Entre los principales avances se destacan la incorporación de criterios de protección de datos personales en procedimientos, formatos y demás instrumentos utilizados por la entidad para la recolección y tratamiento de información, así como el fortalecimiento de las capacidades institucionales mediante la implementación de un curso virtual de formación ubicado en la plataforma iCampus JEP y la realización de jornadas de capacitación, talleres y espacios de sensibilización dirigidos a servidores, contratistas y demás colaboradores.

Asimismo, se inició con la gestión del riesgo asociado al inadecuado tratamiento de datos personales, mediante su identificación e incorporación en la matriz de riesgos institucional, para ello, se fortaleció la metodología institucional de administración de riesgos mediante la actualización del Manual de Administración de Riesgos de Gestión y de Corrupción (JEP-MA-02-02), incorporando el enfoque para la identificación, valoración y tratamiento de riesgos relacionados con el tratamiento de datos personales. Sobre este último se han definido controles y actividades permanentes de monitoreo y seguimiento por parte de la Oficina Asesora de Atención a la Ciudadanía (OAAC), contribuyendo al fortalecimiento del cumplimiento normativo, la gestión del riesgo y la mejora continua. Estos avances evidencian el proceso de madurez alcanzado por la entidad y constituyen la base para la actualización y fortalecimiento de la presente estrategia.

De igual manera, la entidad ha promovido mecanismos de articulación y seguimiento para fortalecer la implementación de la Política, entre ellos la conformación de una red de enlaces en las diferentes dependencias como apoyo a la gestión institucional en esta materia y la realización de espacios de

¹ Política de Tratamiento de Datos Personales de la JEP.

intercambio de conocimientos, como el conversatorio institucional “Derecho al olvido: la caducidad del dato personal “desarrollado en la vigencia 2024.

Así las cosas, la actualización de la presente estrategia responde a la necesidad de incorporar los avances alcanzados durante la implementación del instrumento formulado en 2023 e implementado desde 2024, así como de fortalecer su enfoque metodológico, ajustar su contenido al estado actual de la gestión de datos personales en la JEP y a la evolución del marco de referencia en esta materia.

En ese sentido, la presente versión conserva los referentes conceptuales esenciales, el marco normativo aplicable y las líneas de acción definidas en la estrategia anterior (2023), las cuales, por su carácter general, mantienen plena vigencia como ejes orientadores para la implementación de la PTDP. No obstante, fortalece y actualiza el marco conceptual incorporando desarrollos que, desde 2023, han adquirido un mayor nivel de consolidación y constituyen hoy referentes para la gestión de la PDP, entre ellos el principio de responsabilidad demostrada (*accountability*), el enfoque de gestión de riesgos asociado al tratamiento de datos personales y la consolidación de la privacidad desde el diseño (por defecto) como medidas proactivas de cumplimiento.

De igual forma, actualiza el diagnóstico institucional mediante la adopción de la metodología de marco lógico, tomando como insumo el análisis desarrollado en la matriz DOFA de la versión anterior y conservando aquellos aspectos que continúan vigentes, al tiempo que incorpora los avances institucionales y las nuevas oportunidades de mejora identificadas durante la implementación de la estrategia.

En consecuencia, la presente estrategia se establece como el instrumento de gestión institucional para la implementación, desarrollo y seguimiento de la Política de Tratamiento de Datos Personales (PTDP) adoptada por la JEP. Su propósito es fortalecer el cumplimiento del marco normativo aplicable, consolidar un modelo de gobernanza de datos personales e incorporar lineamientos, acciones y controles que garanticen el tratamiento adecuado de la información y el ejercicio efectivo de los derechos de los titulares. De manera complementaria, la estrategia busca promover una cultura institucional fundamentada en los principios de responsabilidad demostrada, confidencialidad, transparencia y protección de los datos personales durante todo su ciclo de vida.

La estrategia se estructura a partir de un marco conceptual y normativo que sustenta su alcance, un diagnóstico institucional sobre el estado de madurez de la gestión de datos personales en la JEP, la definición de objetivos estratégicos y específicos, las líneas de acción que orientarán su implementación y un plan de acción que establece las actividades, responsables, indicadores y mecanismos de seguimiento necesarios para asegurar su ejecución y mejora continua.

Para ello, se adopta un marco de referencia integral que articula las disposiciones constitucionales, legales y reglamentarias en materia de protección de datos personales, transparencia, acceso a la información pública y gestión institucional de la información, constituyéndose en el fundamento

para la implementación de controles, procedimientos y buenas prácticas que fortalezcan el cumplimiento normativo y la gestión del riesgo asociado al tratamiento de datos personales en la entidad.

Ahora bien, a partir de la estructura del Modelo de Gestión de la JEP, esta estrategia se enmarca principalmente en la Dimensión de Arquitectura Institucional, específicamente en el elemento Gestión Jurídica Pública, por cuanto la implementación de la PTDP en la JEP constituye un instrumento de gobierno y cumplimiento normativo que desarrolla las obligaciones constitucionales y legales en esta materia. Su implementación establece reglas, responsabilidades y controles para el tratamiento de la información personal, garantizando el respeto por los derechos de los titulares y fortaleciendo la seguridad jurídica, la responsabilidad institucional y la gestión del riesgo.

Cabe señalar que, de manera complementaria, la PTDP y su estrategia de implementación, tienen un carácter transversal, al apoyar el fortalecimiento del marco estratégico, la cultura organizacional, la transformación digital y la confianza de los grupos de interés en la gestión de la JEP, por lo que se colige que, aunque su asociación principal está en la Gestión Jurídica Pública, su implementación impacta todas las dimensiones del Modelo de Gestión de la JEP.

1. Descripción de la estrategia

1.1. Marco de Referencia

La protección de datos personales constituye un derecho fundamental autónomo, reconocido por la Constitución Política de Colombia y desarrollado por la jurisprudencia constitucional y la legislación nacional. El artículo 15 de la Constitución consagra el derecho de todas las personas a conocer, actualizar y rectificar la información que sobre ellas repose en bases de datos o archivos de entidades públicas y privadas, estableciendo el denominado derecho al *habeas data*, entendido como la facultad que tiene toda persona para controlar el tratamiento de su información personal.

La Corte Constitucional ha señalado que el *habeas data* comprende el poder de disposición y control que tiene el titular sobre sus datos personales, lo que implica que cualquier tratamiento debe respetar los principios constitucionales de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad (Sentencias C-748 de 2011 y C-1011 de 2008). Estos principios constituyen el eje sobre el cual se estructura el régimen colombiano de protección de datos personales.

En desarrollo del mandato constitucional, la Ley Estatutaria 1581 de 2012 estableció el Régimen General de Protección de Datos Personales y definió las obligaciones de los responsables y encargados del tratamiento, así como los derechos de los titulares. Posteriormente, el Decreto 1074 de 2015 compiló la reglamentación relacionada con el tratamiento de datos personales y fijó los

procedimientos para garantizar su cumplimiento. En el ámbito del sector público, estas disposiciones deben armonizarse con los principios de la función administrativa previstos en el artículo 209 de la Constitución, particularmente los de transparencia, eficacia, responsabilidad y publicidad.

En las entidades públicas, la protección de datos personales adquiere una connotación especial debido a que el tratamiento de la información no responde únicamente a relaciones contractuales o comerciales, sino al ejercicio de funciones constitucionales y legales. En consecuencia, si bien el consentimiento del titular constituye la regla general para el tratamiento de datos personales, la Ley 1581 de 2012 prevé excepciones cuando dicho tratamiento sea necesario para el ejercicio de funciones legales o constitucionales de las entidades públicas, sin que ello exonere a la administración del cumplimiento de los principios de seguridad, proporcionalidad, confidencialidad y responsabilidad.

Por su parte, la Superintendencia de Industria y Comercio (SIC), como autoridad nacional de protección de datos personales, ha señalado que el cumplimiento de la normativa no se limita a la expedición de una política institucional, sino que requiere la implementación de medidas administrativas, técnicas y organizacionales que permitan demostrar el cumplimiento del principio de responsabilidad demostrada (*accountability*). Este enfoque implica que las organizaciones deben gestionar los riesgos asociados al tratamiento de datos personales, documentar sus procedimientos, capacitar permanentemente a sus servidores y adoptar mecanismos de mejora continua.

Este principio de responsabilidad demostrada fue incorporado por la SIC mediante la "Guía para la Implementación del Principio de Responsabilidad Demostrada (*accountability*)", la cual promueve que las entidades desarrollen programas integrales de gestión de datos personales basados en el análisis de riesgos, el monitoreo permanente y la cultura organizacional. Este enfoque resulta especialmente pertinente para una estrategia institucional, pues trasciende el cumplimiento formal de la norma y orienta la gestión hacia la prevención de incidentes y la protección efectiva de los derechos de los titulares.

Desde una perspectiva internacional, la Organización para la Cooperación y el Desarrollo Económico (OCDE) identifica la responsabilidad (*accountability*) como uno de los principios esenciales para la gobernanza de la privacidad, señalando que las organizaciones deben ser capaces de demostrar el cumplimiento de las obligaciones relacionadas con el tratamiento de datos personales. De igual manera, el Reglamento General de Protección de Datos de la Unión Europea (RGPD), referente internacional en la materia, consolidó el enfoque de protección de datos desde el diseño (*privacy by design*) y por defecto (*privacy by default*), orientado a incorporar la protección de la

información desde la planificación de los procesos institucionales y no únicamente como un mecanismo correctivo.

En Colombia, el Documento CONPES 3995 de 2020, "Política Nacional de Confianza y Seguridad Digital", fortalece este enfoque al promover el desarrollo de capacidades institucionales para la gestión de riesgos digitales, la protección de la información y la consolidación de una cultura de seguridad digital en las entidades públicas. Esta política reconoce que la protección de los datos personales constituye un elemento indispensable para fortalecer la confianza ciudadana en las instituciones del Estado y garantizar la transformación digital de la administración pública.

En este contexto, la JEP enfrenta retos particulares en materia de protección de datos personales debido a la naturaleza de la información que administra. Como Entidad integrante del Sistema Integral para la Paz, trata información correspondiente a víctimas, comparecientes, testigos, servidores públicos, contratistas y demás grupos de interés, incluyendo datos sensibles relacionados con condiciones de salud, pertenencia étnica, orientación política, hechos victimizantes, procesos judiciales y demás categorías cuya divulgación indebida podría generar riesgos para los derechos fundamentales de las personas.

Así las cosas, con el propósito de garantizar un tratamiento adecuado de esta información la JEP avanzó en la estructuración específica de su modelo de protección de datos personales mediante la expedición de la Resolución No. 204 del 3 de marzo de 2022, cuyo objeto fue designar al Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales de la JEP y establecer las responsabilidades institucionales requeridas para garantizar la implementación, sostenibilidad y mejora continua de la gestión de protección de datos personales.

Entre sus principales disposiciones se encuentran:

- La designación del Departamento de Atención al Ciudadano (hoy denominada Oficina Asesora de Atención a la ciudadanía-OAAC) en cabeza de su jefe o quien haga sus veces, como Oficial de Cumplimiento de la PTDP de la JEP.
- La definición de las actividades que debe desarrollar dicho oficial para asegurar el cumplimiento de la normativa de protección de datos personales.
- La articulación de esfuerzos institucionales para implementar, mantener y mejorar continuamente la gestión de protección de datos personales.

Así mismo, la JEP adoptó la PTDP mediante el Acuerdo AOG No. 030 de 2022, aplicable a todos los servidores públicos, contratistas, judicantes, pasantes y terceros que intervengan en el tratamiento de datos personales. La política define conceptos como responsable y encargado del tratamiento,

base de datos, titular, tratamiento y datos personales, así como las obligaciones institucionales relacionadas con la recolección, almacenamiento, uso, circulación y supresión de la información, bajo los principios de finalidad, legalidad, libertad, transparencia, acceso restringido, seguridad y confidencialidad.

Desde esta perspectiva, la presente estrategia asume un enfoque de cumplimiento normativo basado en la gestión del riesgo y la responsabilidad demostrada, entendiendo que la protección de datos personales no depende exclusivamente de la existencia de una política institucional, sino de su apropiación por parte de los servidores públicos y contratistas, judicantes, pasantes de la JEP y terceros que intervengan en el tratamiento de datos personales, y de la incorporación de controles técnicos, administrativos y culturales que garanticen la protección efectiva de los derechos de los titulares. En este sentido, la PTDP de la JEP constituye el instrumento mediante el cual la entidad formaliza su compromiso institucional con el cumplimiento del marco constitucional y legal aplicable, estableciendo los principios, responsabilidades y lineamientos que orientan el tratamiento de los datos personales; es decir, define “**qué**” debe hacer la entidad para garantizar este derecho fundamental.

Por su parte, la presente estrategia desarrolla el “**cómo**” hacer efectivo ese compromiso, mediante la definición de acciones, mecanismos e iniciativas orientadas a fortalecer las capacidades institucionales, promover la apropiación de la política por parte de los servidores públicos, contratistas y demás actores involucrados, y consolidar una cultura organizacional de protección de datos personales basada en la prevención, la gestión del riesgo, el mejoramiento continuo y la responsabilidad demostrada, en concordancia con el marco jurídico nacional y las mejores prácticas internacionales en materia de privacidad y gobernanza de la información.

En otras palabras, la PTDP de la JEP establece el marco de gobernanza y los lineamientos institucionales, mientras que la presente estrategia se constituye como el instrumento de implementación que operacionaliza dichos lineamientos mediante acciones concretas, indicadores, responsables y mecanismos de seguimiento.

1.2. Marco Normativo

La presente estrategia se fundamenta en un marco normativo integrado por disposiciones constitucionales, legales, reglamentarias, políticas públicas y lineamientos técnicos que orientan el tratamiento y la protección de los datos personales en las entidades públicas.

Con el propósito de facilitar su comprensión y evidenciar la forma en que respaldan la implementación de la estrategia, este marco se organiza en cuatro niveles: (i) el fundamento

constitucional, que reconoce la protección de los datos personales como un derecho fundamental, (ii) el régimen jurídico de protección de datos personales, que establece los principios, derechos, obligaciones y procedimientos aplicables al tratamiento de la información, (iii) las políticas públicas y modelos de gestión, que incorporan enfoques de seguridad digital, gestión del riesgo y fortalecimiento institucional, y (iv) el marco institucional de la JEP conformado por las disposiciones que regulan sus competencias y por la PTDP adoptada por la entidad, la cual constituye el referente específico que la presente estrategia desarrolla mediante acciones orientadas a su implementación, seguimiento y mejora continua.

En la siguiente tabla se presenta el esquema citado, la relación con la estrategia y el aporte para su implementación:

Tabla 1. Marco Normativo

Norma	Objeto	Relación con la estrategia	Aporte para la implementación
Constitución Política de Colombia (Artículo 15)	Reconoce el derecho fundamental al habeas data y a la protección de los datos personales.	Constituye el fundamento constitucional de la estrategia.	Orienta todas las acciones dirigidas a garantizar los derechos de los titulares y el tratamiento legítimo de la información personal.
Ley Estatutaria 1581 de 2012	Establece el régimen general de protección de datos personales.	Es la norma principal que regula el tratamiento de datos personales en Colombia.	Define principios, derechos, deberes y obligaciones que la estrategia busca implementar y fortalecer dentro de la JEP.
Decreto 1074 de 2015	Reglamenta parcialmente la Ley 1581 de 2012 y compila la normativa del sector Comercio, Industria y Turismo.	Desarrolla aspectos operativos del tratamiento de datos personales.	Proporciona los procedimientos y lineamientos que deben incorporarse en la implementación de la política institucional.
Ley 1712 de 2014	Regula el derecho de acceso a la información pública y el principio de transparencia.	Exige armonizar el acceso a la información pública con la protección de datos personales.	La estrategia debe garantizar el equilibrio entre la publicidad de la información y la protección de los datos personales.
Ley 594 de 2000 (Ley General de Archivos)	Regula la función archivística del Estado.	El tratamiento de datos personales está estrechamente relacionado con la gestión documental.	Orienta la administración, conservación, disposición y eliminación de documentos que contienen datos personales.
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector Función Pública.	Promueve el fortalecimiento institucional y la gestión por procesos.	Respalda la incorporación de responsabilidades institucionales, controles y procesos relacionados con la protección de datos personales.

Norma	Objeto	Relación con la estrategia	Aporte para la implementación
Documento Conpes 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.	Promueve la gestión de riesgos y la protección de la información en las entidades públicas.	Sirve de referente para incorporar una cultura de seguridad digital y gestión del riesgo en la estrategia.
Modelo Integrado de Planeación y Gestión (MIPG) - Decreto 1499 de 2017	Establece el modelo para fortalecer la gestión y el desempeño institucional.	La estrategia se integra con las políticas de Gestión Documental, Gobierno Digital, Servicio al Ciudadano, Transparencia y Control Interno.	Facilita la incorporación de la protección de datos dentro del modelo de gestión institucional de la JEP.
Política de Gobierno Digital (MinTIC)	Define lineamientos para la transformación digital del Estado.	La protección de datos constituye un componente transversal de los servicios digitales.	Favorece la incorporación de controles de seguridad y privacidad en los procesos digitales de la entidad.
Ley 1957 de 2019 (Ley Estatutaria de Administración de Justicia en la JEP)	Regula la organización y funcionamiento de la Jurisdicción Especial para la Paz.	Establece las competencias constitucionales y legales de la JEP para el tratamiento de información en el ejercicio de sus funciones judiciales y administrativas.	Justifica el tratamiento de datos personales en cumplimiento de las funciones propias de la jurisdicción, bajo criterios de legalidad, necesidad y proporcionalidad.
Resolución 204 del 3 de marzo de 2022.	Por la cual se designa el Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales de la Jurisdicción Especial para la Paz	Establece el Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales de la Jurisdicción Especial para la Paz	Establece las actividades a cargo del Oficial de Cumplimiento de la Política de Tratamiento de Datos de la JEP y las responsabilidades de las áreas frente a la implementación y sostenibilidad de la gestión de la protección de datos personales.
Acuerdo AOG 030 de 2022 - JEP	Adopta la Política de Tratamiento de Datos Personales de la JEP.	Constituye el principal referente institucional de la estrategia.	Define los principios, responsabilidades y lineamientos que la estrategia operacionaliza mediante acciones concretas de implementación, seguimiento y mejora continua.
Guía para la Implementación del Principio de Responsabilidad Demostrada (SIC)	Desarrolla el principio de <i>Accountability</i> .	Proporciona un modelo de gestión basado en riesgos y mejora continua.	Orienta la implementación de controles, capacitación, monitoreo y evidencia del cumplimiento normativo.
Guía sobre el Tratamiento de Datos Personales en Entidades Estatales (SIC)	Establece buenas prácticas para las entidades públicas.	Sirve como referente técnico para el diseño de procedimientos institucionales.	Apoya la definición de roles, responsabilidades y mecanismos para garantizar el tratamiento adecuado de los datos personales.

Esta organización muestra una progresión clara: la estrategia se fundamenta en la Constitución, desarrolla el régimen legal de protección de datos, se alinea con las políticas nacionales de gestión pública y finalmente operacionaliza esos mandatos en el contexto específico de la JEP, evidenciando la coherencia entre el marco jurídico y la implementación práctica.

Jurisprudencia Clave

De manera complementaria al marco normativo, la jurisprudencia de la Corte Constitucional ha desempeñado un papel fundamental en la interpretación y desarrollo del derecho fundamental a la protección de los datos personales y al *habeas data*. A través de sus decisiones, la Corte ha precisado el alcance de este derecho, los principios que orientan el tratamiento de la información personal y las obligaciones de las entidades públicas y privadas encargadas de su tratamiento. En este contexto, las siguientes providencias constituyen referentes jurisprudenciales relevantes para la implementación de la presente estrategia:

- Sentencia C-1011 de 2008: desarrolla el alcance constitucional del *habeas data*.
- Sentencia C-748 de 2011: revisa la constitucionalidad de la Ley 1581 de 2012 y desarrolla los principios del tratamiento de datos.
- Sentencia T-729 de 2002: uno de los fallos fundacionales sobre autodeterminación informática y *habeas data*.

Sentencia SU-458 de 2012: consolida el alcance del derecho fundamental al *habeas data*.

Articulación con las dimensiones y elementos del Modelo de Gestión para la Administración de Justicia de la JEP (Acuerdo AOG No. 005 de 2022).

A partir de la estructura del Modelo de Gestión de la JEP, la PTDP y su estrategia de implementación se ubican principalmente en la Dimensión de Arquitectura institucional, específicamente en el elemento de Gestión Jurídica Pública. Sin embargo, por su carácter transversal, inciden en otras dimensiones y elementos del modelo, como se presenta a continuación:

Tabla 2. Relación de la estrategia con el Modelo de Gestión para la Administración de Justicia de la JEP

Dimensión	Elemento	Relación con la estrategia para la implementación de la política de Protección de Datos personales
Estratégica	Marco Estratégico	La política hace parte del marco institucional de gobierno y contribuye al cumplimiento de los objetivos estratégicos relacionados con la transparencia, confianza institucional, gestión del riesgo y cumplimiento normativo
	Control y Evaluación	La política exige seguimiento al cumplimiento, auditorías, indicadores, gestión de incidentes y acciones de mejora continua.

Dimensión	Elemento	Relación con la estrategia para la implementación de la política de Protección de Datos personales
Arquitectura Institucional	Diseño Organizacional	La política requiere una estructura organizacional que defina roles, responsabilidades, líneas de autoridad, responsables y encargados del tratamiento, así como mecanismos de coordinación institucional.
	Gestión Jurídica Pública	Es la relación más directa. La política de protección de datos constituye un instrumento de cumplimiento normativo que desarrolla las obligaciones derivadas de la Constitución, la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas aplicables. Define responsabilidades institucionales, procedimientos para el tratamiento de datos y mecanismos para garantizar los derechos de los titulares.
	Justicia Digital	La protección de datos es un componente esencial de la seguridad de la información y de la gestión de la información digital, especialmente en los sistemas judiciales y administrativos de la JEP.
Humana y Cultura Institucional	Cultura y Liderazgo	La eficacia de la política depende de la apropiación por parte de los servidores públicos mediante capacitación, sensibilización y generación de una cultura de protección de datos.
Acceso a la Justicia y Grupos de Interés	Justicia Abierta	La política permite equilibrar la transparencia con la protección de la información personal de víctimas, comparecientes, testigos y demás titulares de datos.
	Relacionamiento	El relacionamiento con grupos de valor vincula la PTDP, ya que las interacciones realizadas a través de los canales de atención, los mecanismos de participación y la gestión de trámites y servicios implica el tratamiento de información personal. Por ello, estas actividades deben desarrollarse garantizando los derechos de los titulares de los datos.

No obstante, la estrategia para la implementación de la PTDP se enmarca principalmente en la Dimensión de Arquitectura Institucional, específicamente en el elemento Gestión Jurídica Pública, por cuanto constituye un instrumento de gobierno y cumplimiento normativo que desarrolla las obligaciones constitucionales y legales en materia de protección de datos personales.

2. Diagnóstico

Con base en la metodología del Marco Lógico (CEPAL²), el siguiente diagnóstico responde básicamente a cuatro elementos: (i) contexto, (ii) problema central, (iii) causas del problema, y (iv) efectos del problema. A continuación, se presenta el desarrollo de la citada metodología.

2.1. Contexto

La JEP en desarrollo de sus funciones constitucionales y legales, realiza el tratamiento de datos personales de diversos grupos de interés, entre ellos víctimas, comparecientes, testigos, apoderados, servidores públicos, contratistas, proveedores y ciudadanía en general. Como se indicó en párrafos anteriores, la naturaleza de la información administrada por la entidad implica el tratamiento de datos personales de diferentes categorías, incluidos datos sensibles y de especial protección

² Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas, CEPAL 2005.

constitucional, lo que exige el cumplimiento riguroso del marco jurídico vigente y la adopción de medidas que garanticen la protección de los derechos de sus titulares.

Si bien la JEP adoptó una PTDP (AOG No. 030 de 2022), estableciendo los principios, responsabilidades y lineamientos institucionales para el tratamiento de la información personal, esta constituye únicamente el punto de partida para garantizar el cumplimiento efectivo de la normativa, siendo necesario desarrollar mecanismos que permitan su apropiación, implementación, seguimiento y mejora continua en todos los procesos institucionales.

En este contexto, se identifica la necesidad de fortalecer la gestión institucional de la protección de datos personales mediante una estrategia que articule acciones de sensibilización, capacitación, fortalecimiento de controles, gestión del riesgo y seguimiento, orientadas a consolidar una cultura organizacional basada en el principio de responsabilidad demostrada y en la protección efectiva de los derechos de los titulares.

2.2. Problema Central

La implementación de la Política de Tratamiento de Datos Personales (PTDP) presenta dificultades y limitaciones de apropiación, articulación institucional, aplicación uniforme y seguimiento, lo que puede afectar la consolidación de una gestión integral en el adecuado tratamiento de los datos personales en la JEP.

2.3. Análisis del Problema (Árbol de Problemas)

Con base en el contexto descrito, se realizó el análisis del problema mediante la técnica del Árbol de Problemas de la Metodología de Marco Lógico, con el propósito de identificar las principales causas que originan la necesidad de fortalecer la implementación de la PTDP en la JEP y los efectos que esta situación puede generar sobre la gestión institucional y la garantía de los derechos de los titulares de la información. Este análisis constituye el fundamento para la definición de los objetivos, las líneas de acción y las actividades previstas en la presente estrategia.

Tabla 3. Análisis del Problema: causas

CAUSAS
- Causa 1: baja apropiación de los lineamientos de la Política de Tratamiento de Datos Personales por parte de servidores públicos, contratistas y demás actores involucrados en el tratamiento de datos personales. - Causa 2: insuficiente articulación institucional para la implementación, seguimiento y mejora continua de la Política de Tratamiento de Datos Personales. - Causa 3: debilidades en la gestión de los riesgos asociados al tratamiento de datos personales. - Causa 4: ausencia de mecanismos sistemáticos para verificar el cumplimiento y la efectividad de la Política de Tratamiento de Datos Personales en los procesos institucionales. - Causa 5: baja sensibilización frente a las implicaciones legales, disciplinarias y reputacionales de la vulneración del derecho fundamental a la intimidad y de la divulgación de información con carácter reservado.

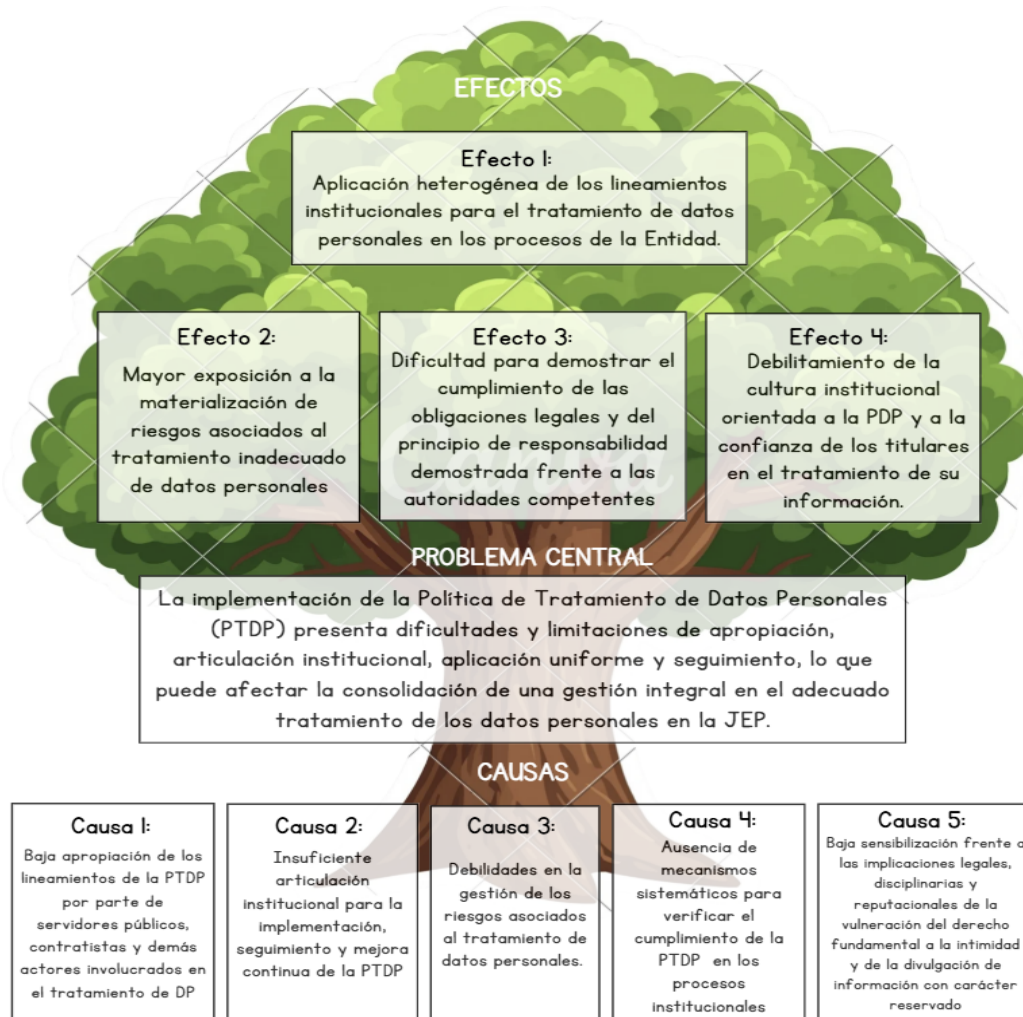
Tabla 4. Análisis del Problema: efectos

EFFECTOS
- Efecto 1: aplicación heterogénea de los lineamientos institucionales para el tratamiento de datos personales en los procesos de la Entidad. - Efecto 2: mayor exposición a la materialización de riesgos asociados al tratamiento inadecuado de datos personales. - Efecto 3: dificultad para demostrar el cumplimiento de las obligaciones legales y del principio de responsabilidad demostrada frente a las autoridades competentes. - Efecto 4: debilitamiento de la cultura institucional orientada a la protección de datos personales y a la confianza de los titulares en el tratamiento de su información.

2.4. Representación del Árbol de Problema

A continuación, se presenta el árbol de problemas que representa de manera esquemática el problema central, sus causas y sus efectos.

Ilustración 1. Representación del Árbol de Problema



3. Objetivos generales y específicos de la estrategia

3.1. Objetivo General

Consolidar una gestión integral de la protección de datos personales en la Jurisdicción Especial para la Paz, mediante la implementación de la Política de Tratamiento de Datos Personales, el fortalecimiento de la cultura institucional y la aplicación de mecanismos de seguimiento y mejora continua que garanticen su apropiación.

3.2. Objetivos Específicos

1. Consolidar la apropiación institucional de la Política de Tratamiento de Datos Personales mediante el fortalecimiento de las capacidades, conocimientos y prácticas relacionadas con la protección de datos personales.
2. Fortalecer la gestión de riesgos asociados al tratamiento de datos personales y promover la consolidación de una cultura institucional de prevención.
3. Consolidar la articulación institucional entre las diferentes órganos y dependencias de la Jurisdicción que intervienen en el tratamiento de datos personales.
4. Fortalecer los mecanismos de seguimiento y evaluación para la implementación de la Política de Tratamiento de Datos Personales.

4. Líneas de Acción

4.1. Línea de acción A. Promover el conocimiento y la formación en materia de tratamiento de datos personales entre servidores, servidoras, contratistas, judicantes, pasantes, practicantes y auxiliares Ad-honorem de todos los órganos y dependencias de la Jurisdicción.

El fortalecimiento de las capacidades institucionales en materia de protección de datos personales constituye un elemento esencial para la implementación efectiva de la Política de Tratamiento de Datos Personales de la JEP. En este sentido, promover el conocimiento, la sensibilización y la formación de los servidores públicos, contratistas y demás actores que participan en el tratamiento de datos personales favorece la apropiación de los principios, responsabilidades y obligaciones establecidos en el marco constitucional, legal e institucional, permitiendo que estos sean incorporados de manera transversal en el desarrollo de los procesos y actividades de la entidad.

Esta línea de acción responde al principio de responsabilidad demostrada (*accountability*), en virtud del cual el cumplimiento de la normativa en materia de protección de datos personales no se limita a la existencia de políticas y procedimientos, sino que exige el fortalecimiento permanente de las competencias del talento humano y la consolidación de una cultura organizacional orientada a la prevención de riesgos y a la protección efectiva de los derechos de los titulares de la información.

De igual manera, la formación contribuye a que quienes intervienen en el tratamiento de datos personales comprendan la importancia de aplicar criterios de legalidad, finalidad, proporcionalidad, confidencialidad y seguridad durante todo el ciclo de vida de la información, desde su recolección hasta su disposición final. Esto favorece la adopción de buenas prácticas institucionales, la estandarización de procedimientos y la disminución de riesgos asociados al tratamiento inadecuado de datos personales.

Asimismo, esta línea de acción fortalece la transparencia institucional y la confianza de la ciudadanía, al promover una gestión responsable de la información personal y *el respeto por los derechos de los titulares*. De esta manera, la JEP no solo da cumplimiento a las obligaciones previstas en la Ley Estatutaria 1581 de 2012 y demás disposiciones aplicables, sino que consolida una cultura institucional basada en la protección de los datos personales, la mejora continua y el compromiso permanente con *la garantía de este derecho fundamental*.

4.2. Línea de acción B. Coordinación institucional entre los órganos y dependencias para la implementación de la PTDP y su articulación con los demás instrumentos relacionados con la protección de datos personales.

La implementación efectiva de la PTDP requiere mecanismos permanentes de articulación, seguimiento y mejora continua que permitan asegurar su aplicación uniforme en todos los procesos de la JEP. En este sentido, la PTDP debe entenderse como una responsabilidad transversal que involucra a las diferentes dependencias y procesos institucionales, en coordinación con las políticas y lineamientos institucionales y otros documentos.

La articulación entre la PTDP y estos instrumentos de gestión favorece un enfoque integral para la administración de los datos personales, evitando la implementación de acciones aisladas y promoviendo la coordinación institucional para la adopción de criterios, procedimientos y controles comunes. De esta manera, la protección de los datos personales se incorpora como un componente transversal de la gestión institucional y contribuye al cumplimiento de los principios de legalidad, responsabilidad, transparencia, seguridad y confidencialidad que orientan el tratamiento de la información.

A continuación, se relacionan algunas de las políticas, lineamientos y otros documentos establecidos por la JEP:

Tabla 5. Políticas o Lineamientos establecidos por la JEP A articular con la estrategia.

Tipo de Documento	Justificación para su articulación con la Política de Tratamiento de Datos Personales-PTDP
Política Institucional de Gestión Documental	Esta política define cómo la entidad gestiona sus documentos desde que se producen o reciben hasta su conservación permanente o eliminación. Esta política debe articularse con la PTDP porque ambas regulan aspectos relacionados con la gestión, administración y protección de la información institucional, dado que los documentos que se producen reciben, conservan y administran en la Jurisdicción contienen datos personales de diferentes categorías.

Tipo de Documento	Justificación para su articulación con la Política de Tratamiento de Datos Personales-PTDP
Índice de Información Clasificada y Reservada	Este instrumento define de acuerdo con el contenido de la documentación que tramita la JEP cuales requieren ser calificados como Reservados o Clasificados. Este debe articularse con la PTDP porque ambos instrumentos tienen como propósito común garantizar una gestión adecuada de la información institucional, estableciendo criterios para determinar su acceso, protección, uso y divulgación, especialmente cuando dicha información puede involucrar derechos fundamentales de las personas.
Registro de Activos de Información (RAI)	Es un inventario organizado y documentado de los activos de información que posee o administra la entidad, en el que se identifica qué información existe, quién es responsable de ella, dónde se encuentra, cómo se clasifica y qué medidas de protección requiere. El RAI hace parte de los instrumentos de gestión de la información previstos en la Ley 1712 de 2014 y su finalidad es facilitar la administración, disponibilidad, protección y acceso a la información pública, respetando las excepciones legales, entre ellas la protección de los datos personales. Su articulación es necesario porque constituye uno de los instrumentos fundamentales para identificar, caracterizar y gestionar adecuadamente la información institucional que contiene datos personales, permitiendo establecer controles acordes con la naturaleza, sensibilidad y riesgos asociados a dicha información.
Tablas de Control de Acceso-TCA	Son un instrumento archivístico y de gestión documental mediante el cual una entidad define y documenta quién puede acceder a la información que produce o administra, en qué condiciones y con qué nivel de autorización, de acuerdo con la naturaleza de la información, la normativa vigente y las funciones de los usuarios. Con este instrumento se realiza la restricción de acceso interna y externa a los expedientes desde el Sistema de Gestión Documental CONTI. Por tanto, las TCA deben articularse con la PTDP porque constituyen un mecanismo fundamental para garantizar que el acceso a la información personal se realice de acuerdo con los principios de seguridad, confidencialidad, necesidad, proporcionalidad y responsabilidad demostrada, evitando accesos, usos o divulgaciones no autorizadas.
Política de transparencia y rendición de cuentas a la ciudadanía de la JEP. Acuerdo AOG 031 de 2020 y las normas que lo modifiquen, sustituyan o deroguen.	Es el instrumento institucional que establece los lineamientos para garantizar el acceso a la información pública, promover la transparencia en la gestión institucional, fortalecer la participación ciudadana y asegurar la rendición de cuentas sobre el cumplimiento de la misión y los resultados de la Jurisdicción. Tiene como propósito establecer la transparencia como un marco jurídico, ético, organizacional y de gestión para todas las actuaciones de la JEP, facilitando a los titulares de derechos, grupos de interés y a la ciudadanía el ejercicio del derecho de acceso a la información pública y de participación en los asuntos de la entidad. Por tanto, se requiere su articulación con la PTDP toda vez que ambas buscan garantizar una gestión institucional responsable de la información, conciliando el deber de la entidad de proporcionar información pública con la obligación de proteger los derechos fundamentales de los titulares de datos personales. En ese sentido, la transparencia y la rendición de cuentas promueven el acceso de la ciudadanía a información relacionada con la gestión pública, sin embargo, el ejercicio de este derecho debe armonizarse con las restricciones legales relacionadas con la protección de la privacidad y los datos personales.
Política de Seguridad y Privacidad de la Información. Acuerdo AOG 045 de 2019 y las normas que lo modifiquen, sustituyan o deroguen.	Es el instrumento institucional mediante el cual la entidad establece los principios, lineamientos, responsabilidades y controles para proteger la información que administra, garantizando su confidencialidad, integridad, disponibilidad y privacidad, independientemente del medio en que se encuentre (físico o digital). En ese sentido, se requiere la articulación con la PTDP considerando que ambas tienen como propósito común garantizar la protección adecuada de la información institucional, estableciendo medidas orientadas a preservar su confidencialidad, integridad, disponibilidad y uso autorizado. Esta articulación permite que la PDP sea gestionada de manera integral, incorporando controles de seguridad durante todo el ciclo de vida de la información.

Tipo de Documento	Justificación para su articulación con la Política de Tratamiento de Datos Personales-PTDP
	Adicionalmente, los datos personales hacen parte de los activos de información que deben ser protegidos, por lo tanto, su articulación con la PTDP permite garantizar que la información personal sea gestionada bajo medidas de seguridad adecuadas, considerando su naturaleza, sensibilidad y los riesgos asociados a su tratamiento. En el caso de la JEP, esta articulación adquiere especial relevancia debido a que la entidad administra información relacionada con víctimas, comparecientes, testigos, apoderados y otros grupos de interés, incluyendo datos sensibles y de especial protección constitucional que requieren medidas reforzadas de seguridad.
Documento de Relacionamento con la Ciudadanía y Demás Grupos de Interés	Es un documento que establece un marco conceptual de los diferentes lineamientos, mecanismos y herramientas que en la JEP se han definido e implementan, para la gestión de los escenarios de relacionamiento con la ciudadanía y demás grupos de interés en el marco del cumplimiento de las políticas asociadas a la relación Estado-ciudadanía. La articulación entre este documento y la PTDP es necesaria para garantizar que los mecanismos de atención, comunicación y participación ciudadana incorporen criterios adecuados para la recolección, uso, almacenamiento y protección de la información personal de los grupos de interés. Esta articulación permite asegurar que el relacionamiento institucional se desarrolle bajo los principios de legalidad, finalidad, confidencialidad y seguridad, fortaleciendo la protección de los derechos de los titulares y la confianza ciudadana en la gestión de la entidad.
Lineamientos de los enfoques diferenciales y la perspectiva de interseccionalidad Narrativa conjunta – Estrategia para su implementación en la JEP	Son un instrumento institucional de política interna que establece los criterios conceptuales y metodológicos para incorporar de manera transversal los enfoques diferenciales y la perspectiva interseccional en el cumplimiento de las funciones misionales y administrativas de la JEP. En especial, la presente estrategia se relaciona con este instrumento mediante la identificación de métodos diferenciados de recolección de datos, que permitan reconocer las características, necesidades y particularidades de los distintos grupos de interés de la entidad. La articulación entre ambos instrumentos resulta fundamental para garantizar que el tratamiento de datos personales incorpore criterios de enfoque diferencial e interseccional, especialmente frente a información asociada a grupos o personas que pueden encontrarse en condiciones de vulnerabilidad o requerir medidas reforzadas de protección. Esta articulación permite orientar la recolección, uso, análisis y gestión de la información bajo principios de pertinencia, proporcionalidad y respeto por la dignidad humana, evitando tratamientos que puedan generar discriminación, afectaciones a los derechos de los titulares o usos inadecuados de información sensible. Asimismo, permite fortalecer la definición de categorías de datos, variables e instrumentos de captura de información, asegurando que la gestión de datos personales responda a las necesidades institucionales sin desconocer las obligaciones derivadas del marco normativo de protección de datos personales.
Lineamientos de enfoque territorial en la Secretaría Ejecutiva de la JEP	La articulación entre los lineamientos de enfoque territorial en la Secretaría Ejecutiva de la JEP y la PTDP resulta necesaria para garantizar que la gestión y tratamiento de la información asociada a los territorios y comunidades atendidas por la Entidad incorpore criterios de protección de datos personales, confidencialidad y seguridad de la información. Esta articulación permite orientar la recolección, uso, análisis y gestión de datos conforme a las particularidades territoriales, garantizando la protección de los derechos de los titulares, especialmente cuando se trate de información sensible o relacionada con poblaciones en condiciones de vulnerabilidad. Especialmente, se fija la atención en a información recolectada en los listados de asistencia los cuales son manejados con estricta confidencialidad.

Tipo de Documento	Justificación para su articulación con la Política de Tratamiento de Datos Personales-PTDP
Lineamientos para la implementación del enfoque de niños, niñas y adolescentes en la JEP.	Es un instrumento institucional que orienta a los órganos y las dependencias de la JEP para incorporar, de manera transversal, el enfoque de derechos de la niñez y la adolescencia en el desarrollo de sus funciones judiciales y administrativas. Su finalidad es garantizar que todas las actuaciones de la JEP que involucren a niños, niñas y adolescentes —como víctimas, comparecientes, testigos o cualquier otra calidad procesal o administrativa— se desarrollen bajo el principio del interés superior del niño, con un enfoque de protección integral y de garantía reforzada de sus derechos. En especial, la presente estrategia se relaciona con el Anexo N°6. La articulación resulta necesaria para garantizar que la recolección, uso, almacenamiento y gestión de información relacionada con niños, niñas y adolescentes se realice bajo criterios reforzados de protección, atendiendo su condición de sujetos de especial protección constitucional. Esta articulación permite asegurar el tratamiento adecuado de sus datos personales, especialmente aquellos de carácter sensible, mediante la aplicación de principios de seguridad, confidencialidad, finalidad y protección integral de sus derechos.

Por su parte, el seguimiento constituye un mecanismo indispensable para verificar el grado de implementación de la Política, evaluar la eficacia de las acciones desarrolladas e identificar oportunamente oportunidades de mejora. Para ello, resulta necesario establecer instrumentos que permitan monitorear el cumplimiento de las obligaciones institucionales, medir el avance de la estrategia mediante indicadores y realizar evaluaciones periódicas que faciliten la toma de decisiones y el fortalecimiento de los controles.

En este contexto, la mejora continua representa un principio orientador para consolidar la madurez institucional en materia de protección de datos personales. La revisión periódica de procedimientos, la actualización de controles, el análisis de incidentes, la incorporación de lecciones aprendidas y la adaptación a los cambios normativos, tecnológicos y organizacionales permiten fortalecer progresivamente la capacidad institucional para garantizar la protección de los derechos de los titulares de la información.

En consecuencia, esta línea de acción busca consolidar un modelo de gobernanza para la protección de los datos personales, basado en la coordinación interinstitucional, el seguimiento sistemático y la mejora continua, que permita demostrar el cumplimiento de la PTDP y fortalecer el principio de responsabilidad demostrada (*accountability*), generando mayor confianza en la gestión que la JEP realiza sobre la información personal bajo su responsabilidad.

De manera complementaria, esta línea de acción busca fortalecer la articulación con las entidades con las cuales la JEP mantiene convenios vigentes para el intercambio de información, promoviendo la definición y adopción de mecanismos de coordinación, control y verificación que permitan identificar y gestionar riesgos asociados al tratamiento y transferencia de datos personales. Lo anterior, con el propósito de establecer responsabilidades claras entre las partes, fortalecer la trazabilidad de las operaciones de tratamiento y contar con evidencia sobre las medidas implementadas para garantizar

el cumplimiento de la PTDP, en aplicación del principio de responsabilidad demostrada (*accountability*) y bajo un enfoque de corresponsabilidad en la protección de los datos personales.

4.3. Línea de acción C. Implementar la metodología para la identificación, valoración y tratamiento de los riesgos de datos personales.

La gestión del riesgo constituye un componente fundamental para la implementación efectiva de la PTDP de la JEP, en la medida en que permite identificar, analizar, valorar y tratar los riesgos asociados al ciclo de vida de los datos personales, con el propósito de prevenir afectaciones a los derechos de los titulares y garantizar el cumplimiento del marco normativo aplicable.

En el desarrollo de sus funciones, la JEP realiza el tratamiento de información personal de diversos grupos de interés, incluyendo datos de carácter sensible y de especial protección constitucional. Esta realidad exige la adopción de un enfoque preventivo que permita identificar oportunamente las amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad, disponibilidad y uso adecuado de la información, así como establecer controles administrativos, técnicos y organizacionales que reduzcan la probabilidad de materialización de dichos riesgos.

En este contexto, la gestión del riesgo comprende la evaluación permanente de aspectos como los accesos no autorizados, las vulnerabilidades tecnológicas, la pérdida o divulgación indebida de información, los errores en el tratamiento de los datos personales, el incumplimiento de las obligaciones legales y los riesgos derivados de cambios tecnológicos o nuevas amenazas en materia de seguridad de la información. La identificación y tratamiento oportuno de estos riesgos fortalece la capacidad institucional para prevenir incidentes que puedan afectar los derechos de los titulares o comprometer el cumplimiento de las funciones de la entidad.

Esta línea de acción promueve la incorporación de la gestión del riesgo como un proceso transversal en la administración de los datos personales, articulado con los sistemas de control interno, seguridad de la información y gestión institucional. Lo anterior permite orientar la toma de decisiones hacia la prevención, fortalecer los mecanismos de control y consolidar una cultura organizacional basada en la mejora continua y la responsabilidad demostrada (*accountability*), de manera que la protección de los datos personales haga parte integral de la gestión institucional y contribuya a preservar la confianza de la ciudadanía en la JEP.

La implementación efectiva de la PTDP requiere contar con mecanismos de gobernanza que permitan articular las responsabilidades de las diferentes dependencias y actores que intervienen en el tratamiento de información personal, garantizando una aplicación coordinada, uniforme y permanente de los lineamientos institucionales. En este sentido, fortalecer la coordinación institucional constituye

un elemento fundamental para asegurar que los principios, obligaciones y controles establecidos en la Política sean incorporados de manera transversal en los procesos y actividades de la entidad.

Como se indicó en párrafos anteriores, en el marco de sus funciones constitucionales y legales, la JEP gestiona información personal de diversos grupos de interés, incluyendo datos sensibles y de especial protección constitucional, cuyo tratamiento involucra la participación de diferentes áreas responsables de la recolección, almacenamiento, uso, custodia, actualización y disposición de la información. Esta diversidad de actores y escenarios de tratamiento requiere establecer mecanismos claros de articulación, comunicación y coordinación que permitan orientar la implementación de la Política bajo criterios homogéneos y conforme con el marco normativo vigente.

En este sentido, esta línea de acción promueve una gestión integral de la protección de datos personales, articulada con los sistemas institucionales de gestión, control interno y seguridad de la información, así como los mecanismos institucionales para la identificación, valoración y tratamiento de riesgos, fortaleciendo la capacidad de la JEP para prevenir posibles afectaciones a los derechos de los titulares y consolidar una cultura organizacional orientada a la protección de la información, la transparencia institucional y la confianza de la ciudadanía.

4.4. Línea de acción D. Fortalecer la gobernanza institucional para la implementación, seguimiento, evaluación y mejora continua de la Política de Tratamiento de Datos Personales.

La implementación efectiva de la PTDP requiere contar con mecanismos de gobernanza que permitan la identificación clara de las responsabilidades de las diferentes dependencias y actores que intervienen en el tratamiento de información personal, garantizando una aplicación coordinada, uniforme y permanente de los lineamientos institucionales. En este sentido, fortalecer la coordinación institucional constituye un elemento fundamental para asegurar que los principios, obligaciones y controles establecidos en la Política sean incorporados de manera transversal en los procesos y actividades de la entidad.

Como se ha indicado a lo largo de este documento, en el marco de sus funciones constitucionales y legales, la JEP gestiona información personal de diversos grupos de interés, incluyendo datos sensibles y de especial protección constitucional, cuyo tratamiento involucra la participación de diferentes áreas responsables de la recolección, almacenamiento, uso, custodia, actualización y disposición de la información. Esta diversidad de actores y escenarios de tratamiento requiere establecer mecanismos claros de articulación, comunicación y coordinación que permitan orientar la implementación de la Política bajo criterios homogéneos y conforme con el marco normativo vigente.

Esta línea de acción busca consolidar espacios e instrumentos institucionales que faciliten la coordinación, el seguimiento, monitoreo y evaluación de la implementación de la PTDP, permitiendo

identificar avances, brechas, dificultades y oportunidades de mejora. Para ello, resulta necesario fortalecer herramientas de medición, reporte y análisis que proporcionen información objetiva para la toma de decisiones y la definición de acciones preventivas y correctivas orientadas al cumplimiento de los lineamientos institucionales.

De igual manera, el fortalecimiento de los mecanismos de coordinación y seguimiento contribuye al cumplimiento del principio de responsabilidad demostrada (*accountability*), en la medida en que permite evidenciar la adopción de medidas organizacionales, técnicas y administrativas encaminadas a garantizar la protección efectiva de los datos personales. Así, la entidad podrá contar con elementos que demuestren no solo la existencia de la Política, sino también su aplicación efectiva, evaluación periódica y mejora continua.

En este sentido, esta línea de acción promueve una gestión integral y transversal de la PTDP, articulada con las dependencias misionales de la JEP que, en el desarrollo de sus funciones, realizan actividades de tratamiento de datos personales, particularmente aquellos de carácter sensible y de especial protección constitucional, fortaleciendo la adopción coordinada de medidas de prevención, control y gestión de riesgos, orientadas a evitar posibles afectaciones a los derechos de los titulares. De esta manera, se busca consolidar una cultura organizacional basada en la protección de la información, el cumplimiento y la responsabilidad demostrada (*accountability*), la gestión preventiva de riesgos asociados al tratamiento de información de víctimas y comparecientes, así como contribuir al fortalecimiento de la transparencia institucional y de la confianza de la ciudadanía en la gestión que realiza la JEP sobre los datos personales bajo su responsabilidad.

5. Implementación de la Estrategia

- Plan específico por líneas de acción.

Con base en la definición de las cuatro líneas de acción que conforman esta estrategia, se ha establecido un plan denominado “**plan para la implementación de la estrategia de gestión de protección de datos personales en la JEP**”, orientado a desarrollar de manera organizada y progresiva las acciones requeridas para su ejecución. Este plan contempla, para cada una de las líneas de acción definidas, la identificación de actividades específicas, responsables institucionales, productos o resultados esperados y los tiempos previstos para su desarrollo, con el propósito de facilitar su seguimiento, monitoreo y evaluación.

De esta manera, el plan para la implementación de la estrategia de gestión de protección de datos personales en la JEP se constituye como una herramienta de gestión que permite orientar la ejecución de la estrategia, promover la articulación entre las dependencias involucradas y facilitar el

cumplimiento de los objetivos propuestos, mediante la definición clara de actividades, responsabilidades y cronogramas, contribuyendo así a la consolidación de una gestión institucional orientada a la protección efectiva de los datos personales, la mejora continua y el principio de responsabilidad demostrada (*accountability*).

Dado el carácter dinámico de la gestión de la PTDP y la evolución permanente del contexto normativo, tecnológico e institucional, el plan para la implementación de la estrategia de gestión de protección de datos personales es objeto de revisión, ajuste, actualización y complementación de manera anual o cuando las necesidades institucionales lo requieran. Esto permitirá incorporar nuevas acciones, redefinir prioridades y fortalecer los mecanismos de implementación, manteniendo la alineación entre la PTDP de la JEP y los demás instrumentos institucionales relacionados con la protección de datos personales.

- **Instrumento y Mecanismos de Seguimiento**

El plan para la implementación de la estrategia de gestión de protección de datos personales en la JEP mencionado, se constituye como el principal instrumento para el seguimiento del desarrollo de la estrategia, permitiendo verificar el avance en la ejecución de las acciones programadas, evaluar el cumplimiento de los objetivos específicos e identificar oportunidades de mejora. Para ello, se realiza seguimiento mensual por parte de la OAAC, mediante el cual se realiza el monitoreo de los productos esperados y el seguimiento del estado de cumplimiento de las actividades, información que sirve de insumo para la toma de decisiones y la actualización continua de la estrategia.

Así mismo, como mecanismo de fortalecimiento de la gobernanza de la protección de datos personales y con el fin de asegurar la implementación transversal de la PTDP y de esta estrategia se conformó un equipo colaborativo institucional integrado por enlaces designados por cada dependencia de la entidad. Este esquema de articulación permite coordinar el seguimiento a la ejecución de las acciones definidas en el citado plan, facilitar el flujo de información entre las áreas, promover la apropiación de las responsabilidades asociadas al tratamiento de datos personales y fortalecer la cultura de protección de datos en todos los niveles organizacionales.

Los enlaces actúan como puntos focales, articulados desde la OAAC para la identificación de necesidades, la gestión de riesgos, el seguimiento a las bases de datos bajo su responsabilidad, la implementación de controles, la atención de requerimientos relacionados con el ejercicio de los derechos de los titulares y el monitoreo del cumplimiento de las disposiciones normativas e institucionales.

Elaboró:

Nelly Quintana Jerez –Oficina Asesora de Atención a la Ciudadanía

Revisó:

Constanza Cañon Charry – Asesor III Oficina Asesora de Atención a la Ciudadanía
Yomar Angelica Muñoz – Profesional Especializada I (Subsecretaria Ejecutiva)
Diana Alexandra González Nieto - Contratista (Subsecretaria Ejecutiva)

Aprobó:

Claudia Liliana Erazo Maldonado– Subsecretaria Ejecutiva

Revisión metodológica:

Adela del Pilar Parra González - Subdirectora de Planeación
Julieth Paulin Fragozo Serpa -Profesional de Gestión I (SP)
Catalina Santamaría- Contratista (SP)

Revisión metodológica SGC:

Maria Luisa Rodriguez Moreno – Subdirectora de Fortalecimiento Institucional
Oscar Javier Pedroza Mogollón – Profesional Especializado II (SFI)
Oscar Javier Rodriguez Machado – Contratista (SFI)

CONTROL DE CAMBIOS

Fecha Actualización	Número de Versión	Descripción del Cambio
2024-12-02	0.0	Elaboración de la Estrategia
2026-09-01	1.0	Actualización del marco de referencia, marco normativo, objetivo general, objetivos específicos y se precisaron las líneas de acción, con el fin de brindar mayor claridad, coherencia y alineación con las necesidades identificadas y el plan de trabajo definido para la vigencia 2026. Asimismo, se fortaleció el diagnóstico conforme a la estructura definida en el formato actualizado. Se ajusta el nombre del documento normalizándolo como estrategia de implementación.