



JURISDICCIÓN ESPECIAL PARA LA PAZ

JEP-ES-12-01
Versión 0.0 / 2024-02-12

SECRETARÍA EJECUTIVA

Departamento de Atención al Ciudadano – Oficial de cumplimiento de la Política de
tratamiento de datos personales.

Estrategia tratamiento de datos personales

Bogotá, Febrero de 2024

Tabla de contenido

1. Introducción	3
2. Descripción de la estrategia	4
2.1. Marco de referencia.....	4
2.2. Marco Normativo.....	6
3. Diagnostico.....	7
A continuación, se presenta un diagnóstico orientado a identificar o establecer los parámetros para conocer el estado interno del tratamiento de los datos personales que la JEP recolecta..... 7	
3.1. Análisis DOFA del tratamiento de datos personales de la JEP.	7
3.1.1. Fortalezas.....	7
3.1.2. Oportunidades	9
3.1.3. Debilidades.....	9
3.1.4. Amenazas	10
4. Objetivo.....	11
4.1. Objetivo general	11
4.2. Objetivos específicos	11
5. Líneas de acción en cumplimiento de los objetivos.....	12
5.1. Implementar la metodología para la identificación, valoración y tratamiento de los riesgos de datos personales.	12
5.2. Promover el conocimiento y la formación en materia de tratamiento de datos personales entre funcionarios, funcionarias, contratistas, pasantes, practicantes y auxiliares judiciales AD Honorem de la JEP.	14
5.3. Articulación con las políticas internas de seguridad de la información y transparencia	16
5.4. Realizar las gestiones necesarias para salvaguardar la confidencialidad de la información personal y sensible, proteger la integridad de los datos personales y velar con la disponibilidad de estos.....	18
6. Desarrollo de las líneas de acción	19
7. Roles, responsables y función.....	21
8. Seguimiento y evaluación de la estrategia.....	21

1. Introducción



La Constitución Política de Colombia, consagra como derecho fundamental el derecho de toda persona de recibir información veraz e imparcial (Artículo 20) y que a su vez establece el derecho a su intimidad personal, familiar y a su buen nombre y el deber del Estado de respetarlos y hacerlos respetar (Artículo 15) y que en desarrollo de estos preceptos constitucionales, se sancionó la Ley Estatutaria 1581 del 17 de octubre de 2012, la cual establece los principios y disposiciones aplicables al tratamiento de datos personales que se encuentren registrados en cualquier base de datos de entidades tanto de carácter público como privado, reglamentada por los Decretos 1377 de 2013 y 886 de 2014 (hoy incorporados en el Decreto único 1074 de 2015) entre otros, normas en las que se establecen las Disposiciones Generales para la Protección de Datos Personales en Colombia.

De otra parte, la Ley 1712 de 2014 que desarrolla el derecho de acceso a la información pública nacional y, particularmente, en el artículo 2° dispone el principio de publicidad universal, según el cual toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no puede ser reservada o limitada sino por disposición constitucional o legal, de conformidad con lo dispuesto en esa misma ley.

Por otro lado, el Acto Legislativo 01 de 2017, incorporó al ordenamiento jurídico colombiano el Sistema Integral de Verdad, Justicia, Reparación y No Repetición – SIVJRNR, y en su artículo transitorio 5° creó la Jurisdicción Especial para la Paz (JEP) como el componente de justicia de este, con las funciones de administrar justicia de manera transitoria y autónoma, conocer de manera preferente y de forma exclusiva de las conductas cometidas con anterioridad al 10 de diciembre de 2016.

En atención a los preceptos normativos citados anteriormente, y con el fin de dar cumplimiento a los mismos, la Jurisdicción Especial para la Paz adopta la presente estrategia de cumplimiento de la Política de Tratamiento de Datos Personales, y que, como instrumento de la misma, tiene como objetivo garantizar los derechos de los titulares de datos y fomentar e incentivar la cultura de tratamiento de datos personales al interior de la entidad.

La estructura de la estrategia presentada en este documento se compone por un marco de referencia teórico y práctico, el correspondiente análisis normativo, un diagnóstico en materia de datos personales de la JEP, los objetivos generales y específicos, las líneas de acción y finalmente el desarrollo de la estrategia mediante un plan de acción.

La presente estrategia tiene el propósito de definir los lineamientos para la implementación de la política de protección de datos personales al interior de la Jurisdicción Especial para la Paz, con el fin de asegurar el tratamiento de estos, en cuanto a su recolección, uso, circulación y disposición final. Con el propósito de dar un adecuado tratamiento a los datos personales, se ha identificado el siguiente marco de referencia y normativo que articula las disposiciones de protección de los datos personales.

2. Descripción de la estrategia

2.1. Marco de referencia

La Política de tratamiento de datos personales, tiene como su propósito garantizar los derechos de los titulares de datos personales, así: “La JEP recolecta, almacena, procesa, usa, circula y/o suprime datos personales públicos, semiprivados, privados y sensibles.”, de los grupos de interés y la ciudadanía en general que tiene o ha tenido alguna vinculación o participación en la entidad.





Así mismo la JEP estableció los principios generales para el tratamiento de datos personales, en el acuerdo AOG 030 de 2022¹, así, como los lineamientos de los funcionarios, contratistas, pasantes judicantes, etc. que manejan información personal y los derechos de las personas sobre sus datos personales, a continuación, se relacionan conceptos a tener en cuenta:

Ámbito de aplicación: Se aplica a todas las personas naturales o jurídicas que recolecten, almacenen, usen, circulen o supriman datos personales en el marco de su relacionamiento con la JEP.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables

Derechos de los titulares: Los Titulares de datos personales tienen derecho a conocer, actualizar y rectificar sus datos, solicitar la eliminación de sus datos, presentar quejas y reclamos, y conocer quiénes tienen acceso a sus datos entre otros².

En Colombia la autoridad encargada de velar por el cumplimiento de las normas de protección de datos personales es la Superintendencia de Industria y Comercio (SIC).

¹ Política de Tratamiento de Datos Personales

² Guía sobre el tratamiento de datos personales en las entidades estatales.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Obligaciones: La JEP maneja datos personales y es pertinente cumplir con ciertas obligaciones, tales como obtener el consentimiento informado de los titulares de los datos cuando se requiera, garantizar la seguridad y confidencialidad de los datos, informar a los titulares sobre el uso de sus datos y respetar los derechos de los titulares.

Principios: En la Política se establece los principios para el manejo de datos personales; finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Titular: persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales tales como la recolección almacenamiento, uso, circulación o supresión.

2.2. Marco Normativo

El marco normativo corresponde a lo señalado en la Política de Tratamiento de Datos Personales. Así mismo el marco normativo de la protección de datos personales en Colombia tiene su base



en la Constitución Política de Colombia estableció en el artículo 15 el derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas.

Mediante la Ley 1581 del 17 de octubre de 2012, reglamentada por los Decretos 1377 de 2013 y 886 de 2014 (hoy incorporados en el Decreto único 1074 de 2015), entre otros, se establecieron las Disposiciones Generales para la Protección de Datos Personales en Colombia. En cumplimiento de estas disposiciones la Jurisdicción Especial para la Paz expidió el Acuerdo AOG 030 de 2022 *“Por el cual se actualiza la Política de Tratamiento de Datos Personales de la JEP”*.

3. Diagnostico

A continuación, se presenta un diagnóstico orientado a identificar o establecer los parámetros para conocer el estado interno del tratamiento de los datos personales que la JEP recolecta.

3.1. Análisis DOFA del tratamiento de datos personales de la JEP.

3.1.1. Fortalezas

- La JEP cuenta con la Política de Tratamiento de Datos Personales, expedida en el Acuerdo de Órgano de Gobierno 030 de 2022.
- La JEP cuenta con la Política de Seguridad y Privacidad de la información que hace parte del Sistema de Gestión de Seguridad y Privacidad de la Información, expedida mediante Acuerdo de Órgano de Gobierno 045 de 2019, cuyo principal objetivo es proteger la confidencialidad, integridad y disponibilidad de la información de la

Entidad. Como apoyo al cumplimiento de esta política, se tienen implementados procedimientos complementarios basados en buenas prácticas de seguridad de la información, como lo son:

- Política de control de acceso
 - Política de teletrabajo
 - Política de seguridad en redes
 - Plan de sensibilización en seguridad de la información
 - Auditoría y monitoreo del cumplimiento de la Política de Seguridad y Privacidad de la Información.
 - Política de respaldo de información.
 - Evaluación de Riesgos de Seguridad de la Información.
 - Gestión de Incidentes de Seguridad de la Información.
 - Gestión de Vulnerabilidades.
- La JEP cuenta con la Política de transparencia y rendición de cuentas a la ciudadanía de la Jurisdicción Especial para la Paz, mediante acuerdo 031 de 2020, donde se designa el oficial de cumplimiento de la política de tratamiento de datos personales, en cabeza del Departamento de Atención al Ciudadano
 - La JEP cuenta con la Resolución 204 de 2022, por la cual se designa al Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales.
 - La entidad cuenta con una estrategia de adopción y transformación tecnológica que se denomina “justicia más digital”, la cual permite a la entidad contar con diferentes soluciones y aplicaciones tecnológicas que soportan la gestión de información, y en las que reposan diferentes tipos de datos.

3.1.2.Oportunidades



- Implementar integralmente la Política de Gobierno Digital Nacional la cual tiene como objetivo la transformación digital mejorando así la prestación de los servicios de la entidad, identificar los grupos poblacionales y evaluar la necesidad de la mejora en los canales de atención.
- Dar Cumplimiento a la regulación en la materia. Así como, mantenerse actualizado con las leyes y regulaciones relacionadas con el tratamiento de datos personales, puede identificar oportunidades para destacar en el cumplimiento y generar confianza con los grupos de interés.
- Realizar el análisis de datos personales puede proporcionar información valiosa para la gestión de la información y del conocimiento en la JEP. El análisis de datos personales puede desempeñar un papel fundamental en la investigación y el desarrollo de la JEP al proporcionar información valiosa para identificar víctimas y comparecientes, comprender los patrones del conflicto, construir casos sólidos y evaluar la magnitud de los delitos cometidos.

3.1.3.Debilidades

- Incumplimiento de las Políticas implementadas por la Entidad. Puede haber casos en los que no se sigan los procedimientos adecuados por parte de los funcionarios/as, contratistas, etc.
- Brechas de seguridad en las medidas de seguridad en cuanto al accesos no autorizados a los datos personales.
 - No contar con la debida clasificación de la información (Privada, semiprivada, pública, sensible).
 - No contar con copias de respaldo de la información.
 - Que la información sea de fácil acceso y manipulación.

- No contar con el inventario actualizado de las bases de datos de la Entidad.
- La falta de conciencia y capacitación de algunos funcionarios/as, contratistas, etc. que no sean conscientes de la importancia del tratamiento adecuado de los datos personales puede resultar en errores e incumplimientos involuntarios en materia de protección de datos personales.
- Desconocimiento del instrumento de recolección de bases de datos personales lo cual podría conllevaría a:
 - Clasificación inadecuada de la base de datos (dependerá de la clase de datos personales que se está recolectando).
 - Dificultad en el momento del registro y/o actualización ante la SIC1.
 - Identificación errónea de la finalidad principal
 - Solicitar autorización de protección de datos personales por parte del Titular cuando se requiera
 - No identificación del nivel de seguridad requerido
 - Conocer si la base se comparte
 - Ubicación de la base
 - Retención inadecuada de datos personales
 - Falta de evaluación y seguimiento a la Política de Tratamiento de datos personales de la JEP.

3.1.4. Amenazas

- Los ciberataques y la seguridad informática deficiente pueden representar una amenaza para la privacidad de los datos personales y la confianza de los grupos de interés y ciudadanía en general.
- Las filtraciones de datos pueden ocurrir debido a fallas en las medidas de seguridad,



errores humanos, brechas en las redes o sistemas de almacenamiento, entre otros factores.



- Uso indebido de datos, existe el riesgo de que los datos personales sean utilizados de manera incorrecta o no autorizada, ya sea por empleados internos, terceros o personas con acceso ilegítimo o ilegal.
- Fuga de Datos
- Acceso lógico no autorizado
- Malware (Virus)
- Phishing (Correos electrónicos fraudulentos)
- Ataques de negación de servicio
- Falta de cifrado de datos
- Acceso físico no autorizado
- Errores humanos
- Robo - pérdida de dispositivos
- Vulnerabilidades de Software (No actualizar)

4. Objetivo

4.1. Objetivo general

Propender el cumplimiento de las leyes y regulaciones en materia de tratamiento de datos personales, asegurando que los datos personales se recopilen, utilicen, almacenen, compartan, etc. de manera legal, ética y segura.

4.2. Objetivos específicos

- Identificar si se están tratando datos personales públicos, privados, semiprivados o

sensibles. (Cualquier información que permita la identificación de una persona debe considerarse datos personales).

- Emplear la metodología para la identificación, valoración y tratamiento de la JEP, para el levantamiento de los riesgos en el tratamiento de datos personales.
- Promover el conocimiento y la aplicación de la ley en materia de tratamiento de datos personales, enseñando a los funcionarios, funcionarias, contratistas, pasantes, practicantes y auxiliares judiciales AD Honorem de la JEP, sobre las leyes y regulaciones pertinentes.
- Gestionar la articulación con las políticas internas relacionadas con información.
- Realizar las gestiones necesarias para salvaguardar la confidencialidad de la información personal y sensible, proteger la integridad de los datos personales y velar con la disponibilidad de estos.

5. Líneas de acción en cumplimiento de los objetivos.

5.1. Implementar la metodología para la identificación, valoración y tratamiento de los riesgos de datos personales.

El tratamiento de datos personales conlleva una serie de riesgos que deben ser identificados y evaluados con el fin de desarrollar estrategias efectivas de protección y mitigación. Estos riesgos abarcan desde aspectos técnicos y de seguridad hasta cuestiones legales y de cumplimiento. Al considerarlos adecuadamente, se pueden establecer medidas sólidas para salvaguardar la privacidad y la integridad de los datos personales.

En primer lugar, es crucial identificar las posibles brechas de seguridad que podrían comprometer la confidencialidad y la integridad de los datos personales. Esto implica evaluar las vulnerabilidades en los sistemas y procesos utilizados para el manejo de datos personales, incluyendo redes, sistemas de almacenamiento y aplicaciones. También se deben tener en cuenta

los controles de acceso, las políticas de contraseñas y las medidas de protección contra ataques externos.



Además, el acceso no autorizado a los datos personales representa un riesgo significativo. Esto puede provenir tanto de funcionarios, funcionarias, contratistas, pasantes, practicantes y auxiliares judiciales AD Honorem de la JEP, como de terceros. Por lo tanto, es esencial evaluar y controlar los permisos de acceso, la gestión de usuarios y los protocolos de seguridad para evitar el acceso indebido a la información sensible.

La posibilidad de fugas de datos personales también debe ser considerada. Estas fugas pueden ser causadas por errores humanos, brechas de seguridad o acciones dolosas. La evaluación de las medidas de cifrado, los protocolos de transferencia segura de datos personales y las políticas de respuesta a incidentes son fundamentales para prevenir y mitigar este riesgo.

El uso indebido de los datos personales es otro aspecto crítico para considerar. Esto implica la posibilidad de que la información se utilice de manera no autorizada, como el acceso no autorizado, la divulgación no autorizada o el uso fraudulento. Para mitigar este riesgo, es necesario implementar políticas de privacidad claras, acuerdos de confidencialidad y establecer controles internos para detectar actividades sospechosas.

La falta de cumplimiento normativo es otro riesgo a tener en cuenta. Las leyes y regulaciones de protección de datos personales están en constante evolución, por lo que es necesario mantenerse actualizado y asegurarse de cumplir con los requisitos legales específicos. Esto incluye aspectos como el consentimiento adecuado, los períodos de retención de datos personales, las transferencias internacionales de datos personales y los derechos de los individuos.

El impacto en la reputación de la JEP también debe ser considerado al evaluar los riesgos del tratamiento de datos personales. Una violación de datos personales o un mal manejo de la información personal puede dañar la confianza de los grupos de interés y ciudadanía en general afectar negativamente la imagen de la JEP. Es esencial tomar medidas para evitar estos escenarios y establecer un plan de gestión de crisis en caso de que ocurran.

Es importante estar al tanto de los cambios tecnológicos y las amenazas emergentes en el ámbito de la protección de datos personales. Las nuevas tecnologías y técnicas utilizadas por los ciberdelincuentes pueden representar riesgos adicionales para la seguridad de los datos personales. Mantenerse actualizado y adaptar continuamente las medidas de seguridad es esencial para proteger eficazmente la privacidad de los datos personales.

5.2. Promover el conocimiento y la formación en materia de tratamiento de datos personales entre funcionarios, funcionarias, contratistas, pasantes, practicantes y auxiliares judiciales AD Honorem de la JEP.

La importancia de promover el conocimiento y la formación en materia de tratamiento de datos personales destaca la responsabilidad y confianza que la JEP debe tener al manejar datos sensibles de la ciudadanía. Además, se resalta la necesidad de cumplir con las regulaciones legales y normativas en protección de datos personales.

Asimismo, la importancia de promover la transparencia y la participación ciudadana en el manejo de los datos personales, informando a la ciudadanía sobre cómo se utilizan y protegen sus datos y permitiendo su participación en las decisiones relacionadas con el tratamiento de los mismos. Se ha subrayado la importancia de prevenir riesgos y proteger los derechos fundamentales de la ciudadanía a través del conocimiento y la formación en protección de datos personales.





Promover el conocimiento y la formación en el tratamiento de datos personales en la entidad contribuye a una buena gestión y a la eficiencia en la gestión de la información. Al contar con personal capacitado en tratamiento de datos personales, se establecen procedimientos claros y eficientes para la recolección, almacenamiento, procesamiento, uso, circulación y/o supresión de datos personales.

Cumplir con las regulaciones y leyes en materia de protección de datos personales es esencial para garantizar la privacidad y seguridad de la información de los individuos. Estas regulaciones establecen obligaciones legales y principios fundamentales de privacidad que deben ser respetados por la JEP.

De acuerdo con la ley 1581 de 2012, donde se establecen los principios en protección de datos personales, dentro de este se encuentran el consentimiento informado, la minimización de datos, la seguridad de la información y la respuesta adecuada a los derechos de los individuos. Cumplir con estas regulaciones no solo evita sanciones legales, sino que también fortalece la confianza de la ciudadanía, promueve buenas prácticas en el tratamiento de datos y establece una relación de transparencia y responsabilidad entre la JEP y la ciudadanía.

Además, el cumplimiento de las regulaciones y leyes en datos personales implica implementar medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados o violaciones de seguridad. Esto ayuda a prevenir la divulgación, alteración o destrucción no autorizada de la información personal. Al cumplir con estas medidas de seguridad, la entidad demuestra su compromiso con la protección de la privacidad de los individuos y refuerza la confidencialidad e integridad de los datos que manejan.

5.3. Articulación con las políticas internas de seguridad de la información y transparencia.

La articulación entre las políticas internas de seguridad de la información, la transparencia en el tratamiento de datos personales es esencial para garantizar una protección sólida de la privacidad y seguridad de la información. Al alinear estas políticas, se establecen directrices claras para proteger la confidencialidad, integridad y disponibilidad de los datos personales, al tiempo que se cumple con las regulaciones y leyes aplicables.

Esta sinergia fomenta la confianza de la ciudadanía al garantizar que sus datos se tratan de manera segura y transparente, y proporciona una base sólida para una respuesta efectiva ante posibles incidentes de seguridad. Al trabajar en conjunto, estas políticas y prácticas aseguran una protección integral de los datos personales, reforzando así la salvaguardia de la privacidad y la confianza entre la entidad y la ciudadanía.

A continuación, se relacionan algunas de las Políticas o Lineamientos establecidos por la JEP

Tipo de Documento	Nombre	Ítem
Política	Política de Tratamiento de Datos Personales	
Política	Política Institucional de Gestión Documental	Seguir las políticas y procedimientos de seguridad de la información de la JEP para proteger los archivos que contienen datos personales y otra información confidencial de acceso no autorizado.

	 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.
	Registro de Activos de Información	
	Esquema de Publicaciones	
	Tablas de Control de Acceso	Con este instrumento se realiza la restricción de acceso interna y externa a los expedientes desde el Sistema de Gestión Documental CONTI
Política	Política de transparencia y rendición de cuentas a la ciudadanía de la Jurisdicción Especial para la Paz	
Política	Política de Seguridad y Privacidad de la Información	
Lineamiento	Lineamientos de los enfoques diferenciales y la perspectiva de interseccionalidad Narrativa conjunta – Estrategia para su implementación en la JEP-	Identificación de métodos diferenciados de recolección de datos
Lineamiento	Lineamientos de enfoque territorial en	Se presta atención a la

	la Secretaría Ejecutiva de la JEP	información recolectada en los listados de asistencia y los datos tomados son manejados con estricta confidencialidad.
Lineamiento	Lineamientos para la implementación del enfoque de niños, niñas adolescentes en la jurisdicción especial para la paz	Anexo N°6

5.4. Realizar las gestiones necesarias para salvaguardar la confidencialidad de la información personal y sensible, proteger la integridad de los datos personales y velar con la disponibilidad de estos.

La importancia de salvaguardar la información y cuidar su confidencialidad radica en proteger los datos personales y sensibles de posibles accesos no autorizados. Al hacerlo, se evitan riesgos como el robo de identidad, el uso indebido de la información o la divulgación no autorizada.

Además, al mantener la confidencialidad de la información, se genera confianza entre la JEP y la ciudadanía, lo que fortalece la imagen institucional. Así como implementar medidas de seguridad adecuadas.

La integridad de los datos personales es un aspecto fundamental en cualquier estrategia de protección de la información. Al garantizar la integridad de los datos personales, se busca preservar su exactitud y confiabilidad, evitando modificaciones no autorizadas o errores que

puedan comprometer su validez. Para lograrlo, es esencial implementar una serie de medidas y prácticas.



Se deben establecer controles de calidad en los procesos de ingreso y almacenamiento de datos, verificando su validez y precisión. Además, es importante mantener copias de seguridad periódicas para poder restaurar los datos personales en caso de pérdida o corrupción. Asimismo, es necesario implementar medidas de seguridad para proteger los datos de ataques maliciosos, como el uso de herramientas de detección de intrusiones y sistemas actualizados de protección.

La disponibilidad de los datos personales es un aspecto clave en la gestión de la información. Verificar la disponibilidad implica asegurarse de que los datos estén accesibles cuando se necesiten.

Esto requiere contar con una infraestructura tecnológica confiable, implementar sistemas de respaldo el monitoreo y mantenimiento de los sistemas de almacenamiento.

Además, es importante considerar aspectos como la escalabilidad, los tiempos de respuesta y la seguridad de los datos. Al verificar la disponibilidad de los datos, se garantiza su accesibilidad, se mejora la eficiencia operativa y se asegura la continuidad de las actividades de la entidad.

6. Desarrollo de las líneas de acción

- Identificación, valoración y gestión de los riesgos en datos personales
- Implementar planes de tratamiento de los riesgos y controles con oportunidad de mejora, asociados a la estrategia y cumplimiento de la ley 1581 y sus decretos.
- Determinar el tiempo que deben conservarse los datos personales de acuerdo con su finalidad, obligaciones legales y contractuales.
- Obtener las autorizaciones de los titulares para la recolección y/o tratamiento de datos

personales y enviarlo a custodia.

- Custodiar las autorizaciones para el tratamiento de los datos personales dadas por los titulares.
- Identificar y/o actualizar el inventario de activos de información de las Bases de Datos de datos personales.
- Reportar y actualizar las Bases de Datos a la Registro Nacional de Bases de Datos
- Gestionar habilidades en los funcionarios, funcionarias, contratistas, pasantes, practicantes y auxiliares judiciales AD Honorem de la JEP en tratamiento de datos personales
- Promover el conocimiento y la aplicación de la ley en materia de tratamiento de datos personales dentro de las personas naturales o jurídicas que recolecten, almacenen, usen, circulen o supriman datos personales en el marco de su relacionamiento con la JEP.
- Disponer los canales y procedimientos de consulta y reclamos, cuando se requiera
- Articulación de las Políticas y/o lineamientos establecidos por la JEP.
- Asegurar que los encargados implementen condiciones de seguridad y privacidad de la información del Titular alineadas con las políticas.
- Actualización de la documentación del proceso
- Implementar planes de remediación/acciones correctivas y preventivas
- Implementar estrategia de seguridad de la información y privacidad de datos personales (Brindar condiciones de seguridad y privacidad)
- Asegurar el uso responsable de las bases de datos personales de acuerdo con su finalidad
- Ejecutar una evaluación de protección de datos personales, en cumplimiento de la normatividad interna o externa.



7. Roles, responsables y función

Los roles, responsables y funciones desempeñan un papel esencial en la adecuada gestión y protección de la información personal. Así mismo estos elementos son fundamentales para asegurar el cumplimiento de las leyes y regulaciones, así como para salvaguardar los derechos y privacidad de los Titulares.

Los roles se refieren a las funciones designadas dentro de la estrategia para gestionar y proteger los datos personales. Cada uno de estos roles tiene responsabilidades y funciones específicas en relación con el tratamiento de datos personales.

L = Líder de la función

R = Responsable operativo

A = Aprueba

C = Consulta

I = Informa del resultado de la actividad

Los responsables son áreas designadas que asumen la responsabilidad de cumplir con las actividades relacionados con el tratamiento de datos personales y las funciones se refieren a las actividades específicas que los responsables deben llevar a cabo para cumplir con sus responsabilidades en materia de tratamiento de datos personales. *(Anexa matriz con relación de roles, responsables y funciones en la JEP)*

8. Seguimiento y evaluación de la estrategia

Seguimiento: a cargo del Departamento de Atención al Ciudadano, toda vez que es el Oficial de cumplimiento de la Política de Tratamiento de Datos Personales.

Evaluación: A cargo de la Subdirección de Control Interno a través de los procesos de auditoría

que adelanta.

Es responsabilidad de todas las servidoras y servidores públicos, contratistas, pasantes, practicantes y auxiliares judiciales AD Honorem de la JEP, el cumplir con lo establecido en la presente estrategia de tratamiento de datos personales y contribuir a la plena observancia de la normatividad vigente en materia de tratamiento de datos personales.

9. Referencias

Constitución Política de Colombia (1991). Artículo 15 y 17. Disponible en: [Constitución Política de Colombia](#).

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Disponible en: [Por el cual se reglamenta parcialmente la Ley 1581 de 2012](#).

Superintendencia de Industria y Comercio (2021). Guía sobre el tratamiento de datos personales en las entidades estatales. Disponible en: [Guía sobre tratamiento de datos personales](#).

Jurisdicción Especial para la Paz (2019). Acuerdo AOG 045. Por el cual se adopta la Política de Seguridad y Privacidad de la Información. Disponible en: [Política de Seguridad y Privacidad de la Información](#).

Jurisdicción Especial para la Paz (2020). Acuerdo AOG 031. Por el cual se adopta la Política de transparencia y rendición de cuentas a la ciudadanía de la Jurisdicción Especial para la Paz. Disponible en: [Política de transparencia y rendición de cuentas a la ciudadanía de la JEP](#)

Jurisdicción Especial para la Paz (2022). Acuerdo AOG 030. Por el cual se actualiza la Política de Tratamiento de Datos Personales de la JEP. Disponible en: [Política de Tratamiento de Datos Personales de la JEP](#)



Jurisdicción Especial para la Paz (2022). Resolución No. 204. [Por la cual se designa el Oficial de Cumplimiento de la Política de Tratamiento de Datos Personales de la Jurisdicción Especial para la Paz.](#) Disponible en: [Oficial de Cumplimiento de la Política de Tratamiento de datos personales JEP.](#)

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en: [Disposiciones generales para la protección de datos personales.](#)

Elaboró:

Sandra Marcela Parra Castillo – Técnico I

Revisó:Constanza Cañon Charry – Jefe Departamento de Atención a la Ciudadanía
José Luis Noguera Pérez – Contratista**Aprobó:**Claudia Liliana Erazo Maldonado– Subsecretaria Ejecutiva
Harvey Danilo Suarez Morales– Secretario Ejecutivo**CONTROL DE CAMBIOS:**

Fecha Actualización	Número de Versión	Descripción del Cambio
2023-12-02	0.0	Elaboración de la estrategia