Superintendencia de Notariado y Registro

Política específica de Tratamiento de Datos Personales

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: GIIAD-PI-001	**Versión: 1**	**Fecha: 29/May./2026**

EQUIPO DIRECTIVO:

Esther Cristina Gómez Melo
SECRETARÍA GENERAL
Alfonso Garcia Manasse
SUPERINTENDENTE DELEGADO PARA REGISTRO
Esther Cristina Gómez Melo
SUPERINTENDENTE DELEGADO PARA NOTARIADO (E)
Natalia Sanchez Martinez
SUPERINTENDENTE DELEGADO PARA PROTECCIÓN, RESTITUCIÓN Y FORMALIZACIÓN DE TIERRAS
Arcenio De Jesus Peralta Valbuena
DIRECCIÓN ADMINISTRATIVA Y FINANCIERA
Luis Yobany Robles Rubiano
DIRECTOR TÉCNICO DE REGISTRO
Mariana Isabel Arteaga Mejia
DIRECCIÓN DE TALENTO HUMANO
Luz Amparo Beltran Rojas
OFICINA ASESORA JURÍDICA
Jorge Arcecio Cañaveral Rojas
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
Fredy Alexander Martinez Garcia
OFICINA DE ATENCIÓN AL CIUDADANO
Nubia Patricia López Méndez
OFICINA ASESORA DE PLANEACIÓN

Mayo / 2026

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

Superintendencia de Notariado y Registro

Tabla de contenido

1. POLITICA 5
2. OBJETIVO 6
3. ALCANCE 6
4. MARCO LEGAL 6
5. GLOSARIO 8
6. PRINCIPIOS RECTORES 11
7. ARTICULACIÓN CON LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES (SIC) 13
8. RESPONSABLE Y/O ENCARGADO DEL TRATAMIENTO 14

8.1. ROLES PARA EL TRATAMIENTO DE DATOS PERSONALES 14

9. LIDERAZGO SOBRE PROTECCIÓN DE DATOS 16

9.1 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES (OPD) 16

9.2 FUNCIONES MINIMAS DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES (OPD) . 16

9.3 RUTA ÚNICA INSTITUCIONAL PARA LA ATENCIÓN DE SOLICITUDES DE INFORMACIÓN Y SOLICITUDES RELACIONADAS CON EL TRATAMIENTO DE DATOS PERSONALES 17

9.4 MECANISMO DE ESCALAMIENTO INTERNO 20

9.5 PUBLICIDAD REGISTRAL, ACCESO A INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES 24

10. DESTINATARIOS 24
11. AUTORIZACIONES 24
12. FINALIDADES 27

12.1 USUARIOS/CIUDADANIA EN GENERAL 28

12.2 ASPIRANTES A FUNCIONARIOS, FUNCIONARIOS Y EXFUNCIONARIOS 29

12.3 PROVEEDORES/CONTRATISTAS 31
12.4 ACCESO A SEDES, VIGILANCIA Y SEGURIDAD DE LAS INSTALACIONES 31
13. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES 33
13.1 INTEROPERABILIDAD E INTERCAMBIO INTERINSTITUCIONAL DE INFORMACIÓN 34
14. DERECHOS DEL TITULAR.....34
15. DEBERES DEL RESPONSABLE DEL TRATAMIENTO.....36
16. ATENCIÓN A CONSULTAS Y RECLAMOS.....39
16.1 CONSULTAS..... 39
16.2 RECLAMOS 40
17. CANALES DE ATENCIÓN.....45
18. INSTRUMENTOS COMPLEMENTARIOS DE LA POLÍTICA DE TRATAMIENTO DE DATOS.....46
19. BIBLIOGRAFÍA.....47

1. POLITICA

La Superintendencia de Notariado y Registro (SNR), como responsable del tratamiento, adopta la presente Política específica de Tratamiento de Datos Personales para garantizar el respeto del derecho fundamental de habeas data, definiendo directrices, roles, controles y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de datos personales, en cumplimiento de la normatividad vigente y bajo el principio de responsabilidad demostrada.

En Colombia, el derecho a la protección de datos personales está consagrado en el artículo 15 de la Constitución Política, el cual reconoce el derecho de todos los ciudadanos a conocer, actualizar, rectificar y/o cancelar sus datos personales recolectados en bases de datos tanto públicas como privadas. La Superintendencia de Notariado y Registro, reconociendo la importancia de su rol en el manejo de datos personales, se compromete a garantizar el derecho constitucional de los ciudadanos a acceder, corregir, eliminar y revocar la autorización de uso de sus datos personales recolectados en las bases de datos de la Entidad. Esto, en concordancia con los propósitos estipulados por la ley y las autorizaciones otorgadas, respetando fielmente el marco legal colombiano de protección de datos personales.

Con este propósito, se ha desarrollado la presente Política para el Tratamiento de Datos Personales, de obligatorio cumplimiento para todas las personas naturales o jurídicas que procesen datos personales contenidos en las bases de datos de la Entidad. Esta política establece las directrices necesarias para asegurar el cumplimiento de las obligaciones legales en materia de protección de datos, como lo dispone la Ley 1581 de 2012 que tiene por objeto desarrollar el derecho constitucional de todas las personas a conocer, actualizar y rectificar la información recolectada sobre ellas por las Instituciones en sus bases de datos o archivos; así como también los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Carta Política (intimidad personal y familiar y al buen nombre), y de igual manera el derecho a la información, consagrado en el artículo 20 de la Carta.

2. OBJETIVO

El propósito de esta Política es proporcionar información clara y completa a todos los grupos de interés, definiendo los principios y procedimientos que aseguren la protección de datos personales manejados por la **Superintendencia de Notariado y Registro**. Este compromiso incluye la observancia de la legislación vigente y la implementación de políticas y procedimientos adecuados para el ejercicio de los derechos de los titulares de los datos. Asimismo, establece las normas sobre la recolección, almacenamiento, uso, circulación y eliminación de los datos personales, garantizando así su tratamiento seguro y conforme a las disposiciones legales aplicables.

3. ALCANCE

- Dar cumplimiento a las exigencias de la normatividad vigente en materia de Protección de Datos Personales, así como a cualquier exigencia originada en el principio de responsabilidad demostrada.
- Brindar la debida protección a los intereses y necesidades de los titulares de la Información personal tratada por la SNR.
- Dar un trámite expedito y legal a las diferentes solicitudes y reclamaciones hechas por los Titulares de la Información, así como por sus causahabientes u otra persona que cuente con la debida autorización.

4. MARCO LEGAL

A continuación, se listan las principales normas vigentes en Colombia en materia de protección de datos personales, con cuyo cumplimiento la SNR está plenamente comprometida y que han sido tomadas en cuenta para efectos del desarrollo de la presente Política.

- Artículo 15 de la Constitución Política de Colombia.

- Ley 527 de 1999, “Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones”.
- Ley 1266 de 2008, “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países y se dictan otras disposiciones”.
- Ley 1273 de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.
- Decreto 886 de 2014 “por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.”
- Capítulo 25. Decreto 1074 de 2015 “reglamenta parcialmente la Ley 1581 de 2012”.
- Ley 1755 de 2015, "Por la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso administrativo.".
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.
- Título V de la Circular Única de la Superintendencia de Industria y Comercio
- Ley 594 de 2000, “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”, en materia de gestión documental, organización y conservación de archivos.

- Ley 1437 de 2011, “Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”, aplicable a las actuaciones administrativas y gestión de solicitudes de información.
- Ley 1579 de 2012, “Por la cual se expide el Estatuto de Registro de Instrumentos Públicos y se dictan otras disposiciones”.
- Ley 1448 de 2011, “Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones”.
- Decreto Ley 4633 de 2011, “Por medio del cual se dictan medidas de asistencia, atención, reparación integral y de restitución de derechos territoriales a las víctimas pertenecientes a los pueblos y comunidades indígenas”.
- Decreto Ley 4634 de 2011, “Por el cual se dictan medidas de atención, asistencia, reparación integral y restitución de tierras a las víctimas pertenecientes al pueblo Rrom o Gitano”.
- Decreto Ley 4635 de 2011, “Por el cual se dictan medidas de asistencia, atención, reparación integral y de restitución de tierras a las víctimas pertenecientes a comunidades negras, afrocolombianas, raizales y palenqueras”.
- Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

5. GLOSARIO

Se tendrán en cuenta las siguientes definiciones para efectos de la presente política:

AUTORIZACIÓN: Es el consentimiento previo, expreso e informado del titular de la información para llevar a cabo el tratamiento de datos personales.

AVISO DE PRIVACIDAD: Es la comunicación verbal o escrita que tiene como fin el informar al titular de los datos sobre la política de protección de datos de la Superintendencia de Notariado y Registro.

ACCESO RESTRINGIDO: Nivel de acceso a la información limitado a parámetros previamente definidos.

ÁREA RESPONSABLE DE PROTECCIÓN DE DATOS: Es el área dentro de LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO, que tiene como función la vigilancia y control de la aplicación de la Política de Protección de Datos Personales y la implementación del Programa Integral de Protección de Datos Personales.

ÁREA RESPONSABLE DE LA ATENCIÓN A PETICIONES, QUEJAS, RECLAMOS Y CONSULTAS: Las peticiones, quejas, reclamos y consultas formuladas por los titulares de datos serán direccionadas por la Oficina de Atención al Ciudadano a la Oficina Asesora de Planeación.

BASE DE DATOS: Conjunto organizado de Datos Personales que sean objeto de tratamiento. Incluye archivos físicos y electrónicos.

CALIDAD DEL DATO: El dato personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible.

CAMBIO SUSTANCIAL: Modificación relevante que afecte finalidades del tratamiento, categorías de datos tratados, encargados/terceros, transferencias internacionales, canales de recolección, medidas de seguridad o cualquier otro elemento que implique variación material del riesgo o del tratamiento previamente informado.

CIRCULACIÓN RESTRINGIDA: Los datos personales sólo serán tratados por aquel personal de la SNR o quienes dentro de sus funciones tengan a cargo la realización de tales actividades.

CONFIDENCIALIDAD: Elemento de seguridad de la información que permite establecer quienes y bajo qué circunstancias se puede acceder a la misma.

DATO PERSONAL: Toda aquella información asociada a una persona y que permite su identificación.

DATO PÚBLICO: Dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.

DATO PRIVADO: Es aquel dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.

DATO SEMIPRIVADO: Es aquel dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

DATO SENSIBLE: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

DERECHO DE LOS NIÑOS, NIÑAS Y ADOLESCENTES: En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

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.

INCIDENTE DE SEGURIDAD: evento confirmado que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de datos personales, incluyendo accesos no autorizados, pérdida, fuga, alteración o divulgación indebida.

INFORMACIÓN DIGITAL: Toda aquella información que es almacenada o transmitida por medios electrónicos y digitales como el correo electrónico u otros sistemas de información.

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 son objeto de Tratamiento.

TRATAMIENTO: Es cualquier operación o conjunto de operaciones sobre Datos Personales que realice la SNR o los Encargados del Tratamiento, tales como la recolección, almacenamiento, uso, circulación o supresión.

TRANSFERENCIA DE DATOS: Tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

TRANSMISIÓN DE DATOS: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia, con el objeto de que un encargado realice tratamiento por cuenta del responsable.

RNBD (REGISTRO NACIONAL DE BASES DE DATOS): Registro administrado por la autoridad competente, que consolida información sobre bases de datos sujetas a registro, sus novedades y reportes, cuando aplique.

OPD (OFICIAL DE PROTECCIÓN DE DATOS PERSONALES): Rol funcional encargado de coordinar la implementación de la política, control de términos y trazabilidad de atención de titulares, y consolidación de evidencias de cumplimiento.

6. PRINCIPIOS RECTORES

La Superintendencia de Notariado y Registro se compromete con los titulares de la información a tratar sus datos personales, de conformidad con los siguientes principios:

- **LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS:** La SNR es consciente que el tratamiento al que se refiere la Ley 1581 de 2012 es una actividad reglada, que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
- **FINALIDAD:** La SNR tratara los datos con una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- **LIBERTAD**: La SNR tratará los datos sólo con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- **VERACIDAD O CALIDAD:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. En la SNR está prohibido el Tratamiento de Datos parciales, incompletos, fraccionados o que induzcan a error.
- **TRANSPARENCIA:** La SNR garantiza a los titulares de la información el derecho a obtener en cualquier momento y sin restricciones, información acerca de la existencia de los datos que le conciernan.
- **ACCESO Y CIRCULACIÓN RESTRINGIDA:** El tratamiento del dato está sujeto a los límites derivados de la naturaleza de los datos personales, de acuerdo con lo dispuesto en la Ley 1581 de 2012, la Constitución y demás normas concordantes. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley. Con excepción de la información pública, la SNR no pondrá a disposición los datos personales en Internet u otros medios de divulgación o comunicación masiva, salvo si el acceso es técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la Ley 1581 de 2012.
- **SEGURIDAD:** La SNR manejará la información sujeta a tratamiento a que se refiere la Ley 1581 de 2012 con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **CONFIDENCIALIDAD:** Todos los funcionarios y contratistas que intervengan en el Tratamiento de Datos Personales que no tengan la naturaleza de públicos están obligados a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de esta. La SNR se compromete a tratar los datos personales de los titulares de forma absolutamente confidencial, haciendo uso de estos, exclusivamente, para las finalidades indicadas en el apartado anterior, siempre que el titular no se haya opuesto a dicho tratamiento. Así mismo, la SNR informa que implementó las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de sus datos personales y evitar la alteración, pérdida, tratamiento y/o acceso no autorizado.
- **TEMPORALIDAD:** La SNR conserva los datos personales únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, de acuerdo con los lineamientos y tiempos establecidos en el Sistema de Gestión Documental, en lo relacionado con la conservación y preservación de la información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.
- **NECESIDAD:** Los datos personales tratados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos.

7. ARTICULACIÓN CON LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES (SIC)

La Superintendencia de Notariado y Registro (SNR) reconoce a la Superintendencia de Industria y Comercio (SIC) como autoridad nacional de protección de datos personales y, en consecuencia, atenderá de manera oportuna los requerimientos, instrucciones y medidas administrativas que esta imparta en ejercicio de sus

funciones de inspección, vigilancia y control. Asimismo, la SNR mantendrá disponibles las evidencias y soportes necesarios para la demostración del cumplimiento (principio de responsabilidad demostrada), incluyendo la atención de derechos de titulares, gestión de incidentes, y las actualizaciones que correspondan en el Registro Nacional de Bases de Datos (RNBD), cuando aplique.

8. RESPONSABLE Y/O ENCARGADO DEL TRATAMIENTO

a. Nombre o razón social: Superintendencia de Notariado y Registro

b. NIT: 899999007.

c. Domicilio: Bogotá D.C., Colombia.

d. Dirección: Calle 26 # 13-49 Interior 201

e. Correo electrónico: correspondenciasnr@supernotariado.gov.co

Correo electrónico protección de datos personales: protecciondatos.snr@Supernotariado.gov.co

f. https://www.supernotariado.gov.co/

g. Teléfonos:

- Conmutador: 57+(601) 514 0313
- Línea Atención al Ciudadano: 57+(601) 514 0313
- Línea anticorrupción: 01 8000 911 616
- Línea gratuita: 01 8000 911 616

8.1. ROLES PARA EL TRATAMIENTO DE DATOS PERSONALES

• Oficina Asesora de Planeación (OAP): lidera, coordina y controla la planeación, implementación, mantenimiento y mejora de la gestión de datos personales.

• Oficial de Protección de Datos Personales (OPD) - rol funcional: coordina la implementación de la política; punto focal para consultas y reclamos; control de términos, trazabilidad y evidencias; coordinación de incidentes y RNBD (cuando aplique); articulación con OAJ, OTI/SGSI, SG y OAC.

• Oficina de Atención al Ciudadano (OAC): realiza el seguimiento y articulación de la atención de las PQRSDF, en coordinación con las dependencias responsables de la respuesta y atención al ciudadano.

• Grupo de Gestión Documental / Correspondencia: responsable de la recepción y radicación de las PQRSDF a través del sistema institucional, así como de la gestión de los soportes de radicación y notificación. Toda solicitud debe surtir obligatoriamente el proceso de correspondencia para su respectiva radicación, de acuerdo con los lineamientos establecidos.

• Oficina de Tecnologías de la Información (OTI) / SGSI: controles técnicos de seguridad, control de acceso, protección de bases de datos, contención/análisis de incidentes y evidencias técnicas.

• Oficina Asesora Jurídica (OAJ): conceptos de reserva/clasificación, soporte jurídico en transferencias/transmisiones y contratos de encargo, y prevención de divulgación indebida.

• Secretaría General (SG) y áreas de apoyo: soporte administrativo y contractual; coordinación de supervisión y exigencia de cláusulas a encargados.

• Dueños del Proceso / Dueños de la Base de Datos: respuesta de fondo, inventario de BD, conservación conforme a TRD/PGD y aplicación de minimización en respuestas/publicaciones.

• Contratación y Supervisión: incorporación y verificación de cláusulas estandarizadas con encargados (seguridad, confidencialidad, reporte de incidentes, retorno/supresión).

El incumplimiento de las disposiciones establecidas en la presente Política de Protección de Datos Personales, así como de los lineamientos, procedimientos, controles y obligaciones relacionadas con el tratamiento de la información, dará lugar a la activación de las acciones administrativas y de verificación

correspondientes por parte de la entidad. En caso de evidenciarse presuntas faltas asociadas al manejo inadecuado de datos personales, uso no autorizado de la información, incumplimiento de deberes de confidencialidad o vulneración de la normatividad aplicable, se adelantará el trámite correspondiente conforme a los procedimientos internos y al régimen disciplinario vigente, sin perjuicio de las acciones legales, civiles, penales o administrativas a que haya lugar.

9. LIDERAZGO SOBRE PROTECCIÓN DE DATOS

La Oficina Asesora de Planeación es la dependencia responsable de liderar, coordinar y controlar el avance en la planeación, implementación, mantenimiento y mejora de la gestión de Datos Personales. La Oficina de Atención al Ciudadano, la Oficina de Tecnologías de la Información y la Secretaría General y demás dependencias deberán apoyar la implementación, seguimiento y mejora continua de la Gestión de Datos Personales.

9.1 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES (OPD)

Para efectos de la presente política, la SNR contará con un Oficial de Protección de Datos Personales (OPD), como rol funcional responsable de coordinar la implementación de la política, consolidar evidencias de cumplimiento, y servir como punto focal institucional para la atención y control de términos de consultas y reclamos de titulares. El Oficial de Protección de Datos Personales de la SNR será el Jefe de la Oficina Asesora Planeación o a quien este designe.

El OPD operará en articulación con la Oficina de Atención al Ciudadano (OAC), la Oficina de Tecnologías de la Información (OTI), la Secretaría General (SG) y la Oficina Asesora Jurídica (OAJ).

Contacto funcional OPD: protecciondatos.snr@Supernotariado.gov.co

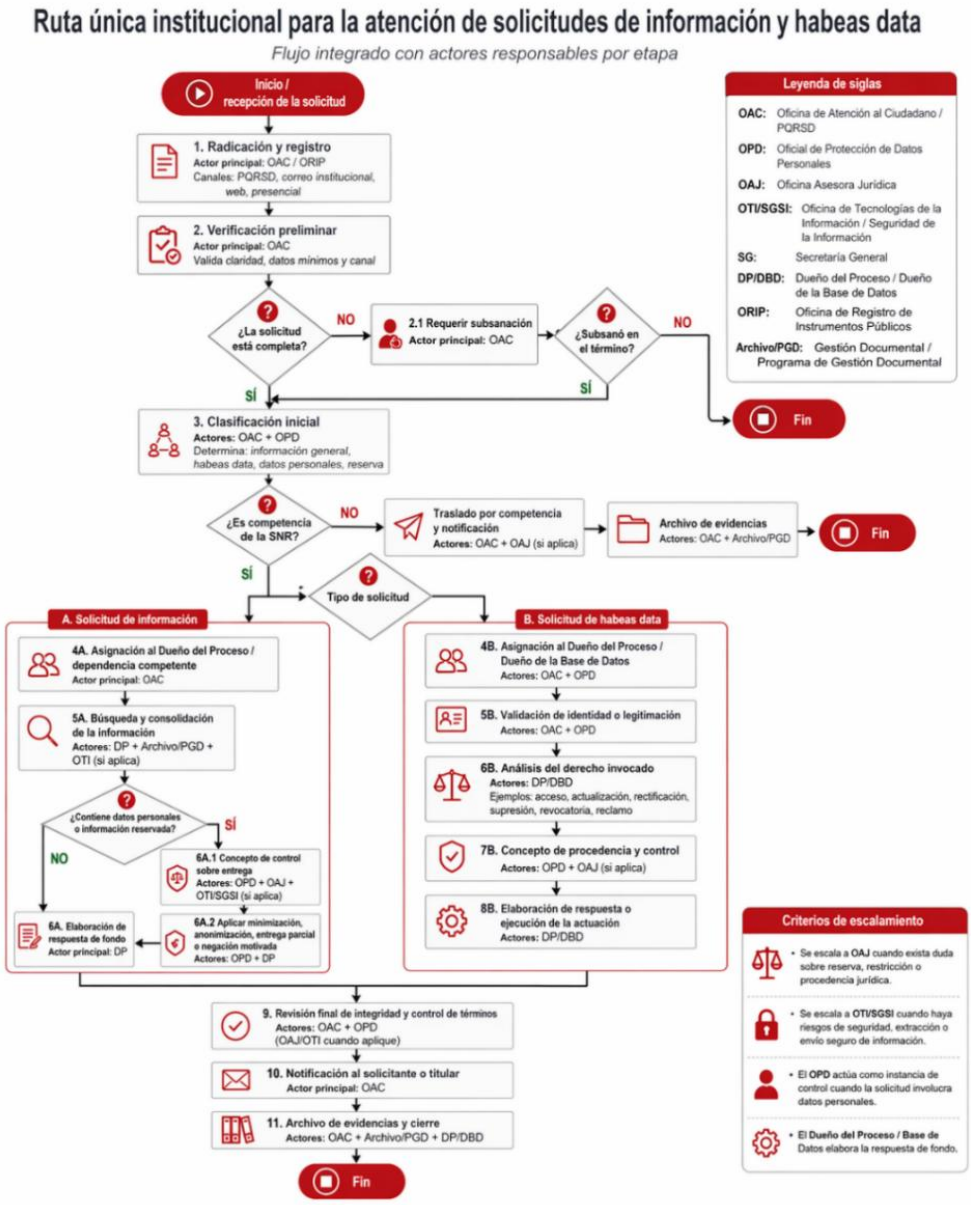
9.2 FUNCIONES MINIMAS DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES (OPD)

- ✓ Coordinar la implementación, actualización y divulgación de la política institucional de tratamiento de datos personales.
- ✓ Actuar como punto focal institucional para la atención de consultas y reclamos de titulares y para el control de términos y trazabilidad.
- ✓ Clasificar y direccionar solicitudes a los dueños del proceso/base de datos; consolidar evidencias de respuesta y cierre del caso.
- ✓ Administrar y mantener el inventario institucional de bases de datos con datos personales (dueño, finalidad, categorías, encargados, conservación).
- ✓ Coordinar el cumplimiento asociado al RNBD cuando aplique (actualizaciones, novedades, cambios sustanciales), conservando evidencias.
- ✓ Coordinar la gestión de incidentes de seguridad con OTI/SGSI, incluyendo análisis de impacto, decisiones de notificación y cierre con lecciones aprendidas.
- ✓ Articular con la OAJ la validación de reserva, clasificación y soporte jurídico en transferencias/transmisiones y contratos de encargo.
- ✓ Verificar, con Contratación/Supervisión, que los contratos con encargados incluyan cláusulas mínimas verificables de tratamiento (seguridad, confidencialidad, subencargados, retorno/supresión, reporte de incidentes).
- ✓ Ejecutar controles preventivos para evitar exposición indebida de datos personales en publicaciones institucionales e interoperabilidad, coordinando con el responsable de transparencia cuando exista.
- ✓ Impulsar formación y sensibilización anual en protección de datos para funcionarios/contratistas y emitir recomendaciones de mejora continua.

9.3 RUTA ÚNICA INSTITUCIONAL PARA LA ATENCIÓN DE SOLICITUDES DE INFORMACIÓN Y SOLICITUDES RELACIONADAS CON EL TRATAMIENTO DE DATOS PERSONALES

Con el fin de asegurar la trazabilidad, el control de términos, la uniformidad en la atención y la adecuada protección de la información y de los datos personales, la Superintendencia de Notariado y Registro adopta

la siguiente ruta única institucional para la atención de solicitudes radicadas por los canales oficiales de la entidad.



Fuente: Elaboración propia

Esta ruta aplicará tanto para:

a)Solicitudes de información, en el marco del derecho de petición y del acceso a la información. b) Solicitudes relacionadas con el tratamiento de datos personales o ejercicio del habeas data, tales como acceso, actualización, rectificación, supresión, revocatoria de autorización, consulta, reclamo o cualquier otra petición asociada al tratamiento de datos personales.

La ruta comprenderá las siguientes etapas:

1. Radicación de la solicitud por los canales oficiales habilitados por la entidad (GD/PQRSD, ORIP, correo institucional, página web u otros canales autorizados).
2. Verificación preliminar y clasificación inicial de la solicitud, con el fin de determinar si:
    - Corresponde a una solicitud de información general;
    - Involucra datos personales;
    - Constituye una solicitud de habeas data o;
    - Debe ser trasladada a otra entidad o dependencia competente.
3. Asignación al Dueño del Proceso y/o Dueño de la Base de Datos, según la naturaleza de la solicitud, para el análisis de fondo y consolidación de la respuesta.
4. Análisis de viabilidad jurídica, funcional y técnica, según el tipo de solicitud:
    - Cuando se trate de solicitud de información, se verificará la procedencia de la entrega, la existencia de información clasificada o reservada y la necesidad de aplicar criterios de minimización o protección de datos personales;
    - Cuando se trate de solicitud de habeas data, se verificará la identidad o legitimación del solicitante, la procedencia del derecho invocado y las condiciones para acceder, actualizar, rectificar, suprimir o limitar el tratamiento de los datos personales.
5. Concepto de control por parte del Oficial de Protección de Datos Personales (OPD), cuando la solicitud involucre datos personales, con el fin de evaluar la procedencia de la entrega, acceso, actualización,

rectificación, supresión, revocatoria o limitación del tratamiento, así como la necesidad de aplicar anonimización, minimización, entrega parcial o restricción.

6. Elaboración de la respuesta de fondo por el Dueño del Proceso y/o Dueño de la Base de Datos, con el apoyo de las dependencias competentes cuando aplique.
7. Revisión de integridad, legalidad y control de términos, a cargo del OPD cuando la solicitud involucre datos personales, y de la OAC respecto de la trazabilidad y gestión de la respuesta.
8. Notificación al solicitante o titular a través del canal institucional correspondiente.
9. Archivo de evidencias y cierre del caso en el repositorio institucional, garantizando la trazabilidad de la actuación surtida.

Nota. Para solicitudes relacionadas con la supresión o eliminación de datos personales, además de las etapas anteriores, se aplicará el procedimiento específico de supresión descrito en el apartado de Reclamos, el cual incorpora análisis de impacto en procesos y sistemas, validación de obligaciones de conservación (TRD/PGD y normas aplicables), evaluación de riesgos y ejecución técnica controlada.

Parágrafo 1. Cuando la solicitud requiera análisis especializado, exista duda sobre la procedencia de la entrega de información o se identifiquen riesgos asociados a reserva, clasificación, seguridad de la información o protección de datos personales, se activará el escalamiento a las dependencias competentes, tales como la Oficina Asesora Jurídica, la Oficina de Tecnologías de la Información, la Secretaría General u otras que correspondan.

Parágrafo 2. El Oficial de Protección de Datos Personales no sustituye al Dueño del Proceso ni al Dueño de la Base de Datos en la elaboración de la respuesta de fondo, sino que actúa como instancia de control, orientación y validación cuando la solicitud involucre datos personales o riesgos asociados a su tratamiento.

9.4 MECANISMO DE ESCALAMIENTO INTERNO

Cuando una solicitud requiera análisis especializado, implique riesgos jurídicos, técnicos, de seguridad o de protección de datos personales, o suponga decisiones que excedan la gestión ordinaria del proceso, la SNR

aplicará el siguiente **mecanismo de escalamiento interno**, con el fin de garantizar una respuesta integral, jurídicamente sustentada, segura y trazable.

Nivel 1: OPD (clasificación, control de términos, articulación).

Nivel 2: OAJ (concepto jurídico / reserva), OTI/SGSI (concepto técnico / seguridad), SG (gestión administrativa), según corresponda.

Nivel 3: Instancia directiva competente (decisiones institucionales o de alto impacto, incluyendo cambios sustanciales).

ARTICULACIÓN CON LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Con el fin de asegurar coherencia institucional, la gestión de riesgos asociada al tratamiento de datos personales se desarrolla y se integra conforme a la Política General para la Administración de Riesgos de la SNR vigente.

Los Dueños del Proceso/Dueños de la Base de Datos (primera línea) identificarán eventos de riesgo de privacidad y definirán controles y planes de tratamiento en sus procesos y sistemas (por ejemplo: acceso no autorizado, divulgación indebida, pérdida, alteración, tratamiento sin base legal, retención excesiva o supresión no controlada).

La OAP y el OPD (segunda línea) consolidarán y darán seguimiento al registro de riesgos de privacidad, verificando la aplicación de controles y asegurando que las solicitudes complejas (por ejemplo, supresión) incorporen análisis de impacto y de riesgos antes de ejecutar acciones irreversibles.

La Oficina de Control Interno de Gestión (tercera línea) realizará seguimiento y auditoría a la efectividad de controles, evidencias y planes de tratamiento, en articulación con las instancias de gobierno que correspondan.

ARTICULACIÓN CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

La presente política se articula con el Manual de Políticas del Sistema de Gestión de Seguridad de la Información (SGSI) de la SNR vigente, garantizando que el tratamiento de datos personales opere bajo los principios de confidencialidad, integridad y disponibilidad.

En particular, la atención de solicitudes que involucren datos personales aplicará los lineamientos del SGSI relacionados con: gestión de activos, control de acceso, seguridad de comunicaciones, criptografía cuando aplique, seguridad en la relación con proveedores/encargados y gestión de incidentes de seguridad de la información.

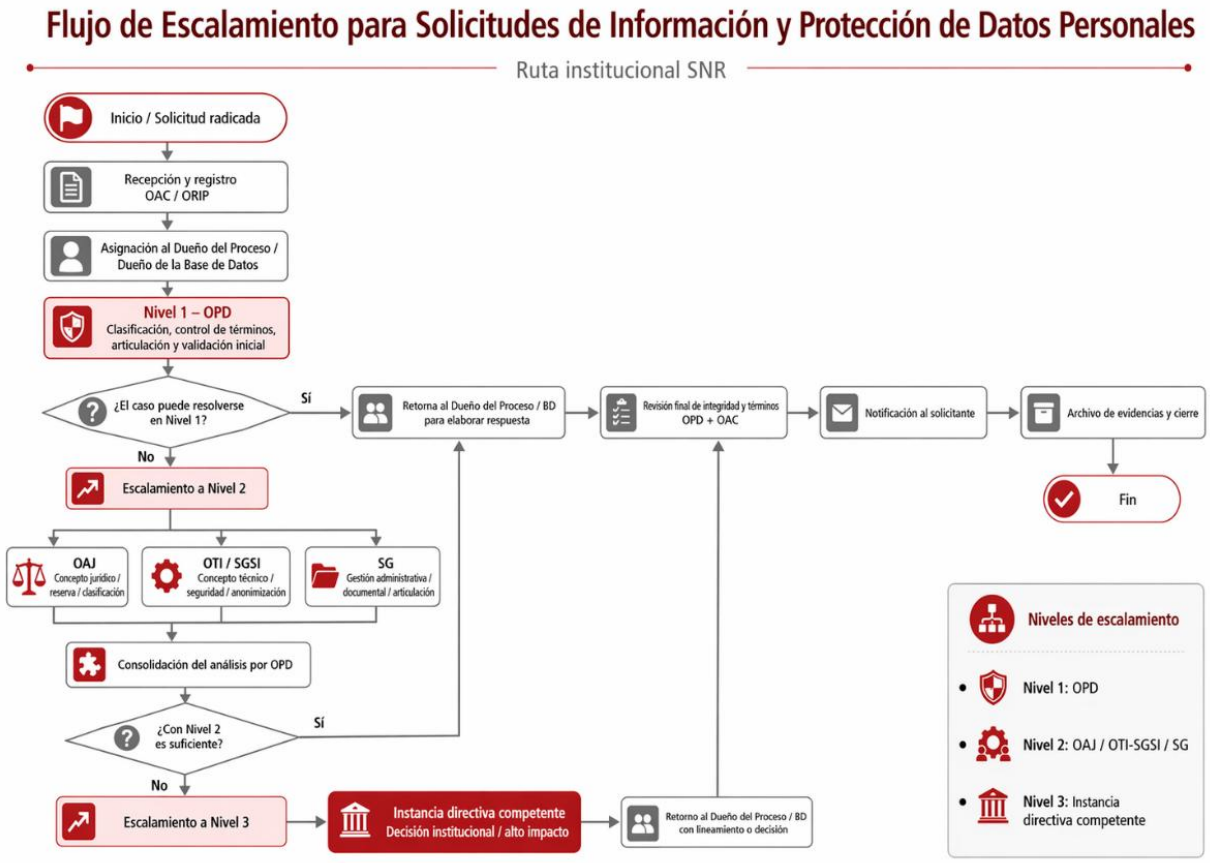
Los incidentes que comprometan o puedan comprometer datos personales se gestionarán como incidentes de seguridad de la información bajo liderazgo de OTI/SGSI y coordinación del OPD para análisis de impacto, evidencias, decisiones de notificación y acciones correctivas y preventivas.

ARQUITECTURA DE INFORMACIÓN, TRAZABILIDAD Y CADENA DE VALOR DEL DATO

Para asegurar consistencia y cumplimiento normativo en toda la cadena de valor del dato, la SNR mantendrá un inventario institucional de bases de datos y activos de información con datos personales, enlazando: proceso origen, sistema de información, repositorios, responsables, finalidades, categorías de datos, encargados, transferencias/transmisiones, controles aplicables y tiempos de conservación (TRD/PGD).

Las solicitudes de titulares, especialmente las relacionadas con supresión/eliminación, deberán analizar su impacto sobre procesos y sistemas de información (fuentes, integraciones, copias de trabajo, repositorios documentales, interoperabilidad y publicaciones), garantizando trazabilidad de decisiones, controles aplicados y evidencias de ejecución.

Toda actuación (por ejemplo, supresión, restricción o anonimización) debe reflejarse en el inventario de datos, en los metadatos operativos y, cuando aplique, en los instrumentos de arquitectura de información establecidos por la entidad.



Fuente: Elaboración propia

1.1 ARTICULACIÓN CON TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

La gestión de transparencia y acceso a información pública se articulará con la gestión de protección de datos personales, con el fin de prevenir la exposición indebida de datos personales en publicaciones, interoperabilidad y respuestas. El Oficial de Protección de Datos (OPD) coordinará y articulará con el

responsable o enlace de transparencia y con la Oficina Asesora Jurídica (OAJ) las validaciones necesarias de clasificación, reserva y minimización de datos antes de divulgar información.

9.5 PUBLICIDAD REGISTRAL, ACCESO A INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

La publicidad registral y el derecho de acceso a la información pública no habilitan la publicación masiva, abierta, indiscriminada o no controlada de datos personales. Antes de entregar, interoperar, publicar o divulgar información que contenga datos personales, el OPD y la dependencia responsable deberá verificar competencia legal, finalidad, necesidad, proporcionalidad, reserva o clasificación, minimización de datos y riesgo para los titulares.

En publicaciones institucionales, informes, tableros, respuestas y bases compartidas, la SNR privilegiará datos agregados, anonimizados o seudonimizados. La inclusión de nombres, números de identificación, direcciones, o información que permita inferir calidad de víctima, pertenencia étnica, situación jurídica del predio o condición de sujeto de especial protección deberá justificarse expresamente.

10. DESTINATARIOS

La presente política está dirigida a nuestros clientes/usuarios, funcionarios y contratistas, proveedores, aliados y en general nuestros grupos de interés sobre los cuales la Superintendencia realiza tratamiento de información personal.

11. AUTORIZACIONES

Salvo en los casos que por Ley para el tratamiento de datos personales no sea requerida autorización del titular del dato, la SNR solicitará al titular de la información el consentimiento previo, expreso e informado para el tratamiento de sus datos personales. La autorización también podrá obtenerse a partir de conductas inequívocas del titular del dato, las cuales permitan concluir de manera razonable que éste otorgó su

consentimiento para el tratamiento de su información. Dichas conductas deben exteriorizar de manera clara la voluntad de autorizar el tratamiento.

El consentimiento del titular se podrá obtener por cualquier medio que pueda ser objeto de consulta posterior, tales como, comunicación escrita, verbal, virtual o por conductas inequívocas.

La SNR como responsable del Tratamiento, deberá conservar prueba del cumplimiento de lo previsto en el presente numeral y, cuando el Titular lo solicite, entregarle copia de esta.

Así mismo, cuando se trate de información que se relacione con los siguientes tipos de datos, se deberán tener en cuenta las siguientes consideraciones especiales respecto de las autorizaciones:

Datos sensibles: Para el tratamiento de datos sensibles, la SNR informará al titular de los datos lo siguiente:

- Para el tratamiento de este tipo de información el titular no está obligado a dar su autorización o consentimiento.
- Se informará de forma explícita y previa qué tipo de datos sensibles serán solicitados.
- Se comunicará el tratamiento y la finalidad que se le dará a los datos sensibles.
- La autorización de los datos sensibles será previa, expresa y clara.

En caso de tratamiento de datos relativos a la salud, **la SNR,** implementará las medidas necesarias para proteger la confidencialidad de la información. Los datos sensibles biométricos tratados tienen como finalidad la identificación de las personas, la seguridad, el cumplimiento de obligaciones legales y la adecuada prestación de los productos.

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

- El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Datos de niños, niñas y adolescentes: La **SNR** se asegurará que el tratamiento de este tipo de datos se realice de conformidad con los derechos de los niños, niñas y adolescentes. En este sentido, se protegerá su carácter especial y velará por el respeto de sus derechos fundamentales, de acuerdo con lo dispuesto en los artículos 5, 6 y 7 de la Ley 1581 de 2012, en los artículos 6 y 12 del Decreto 1377 de 2013, y demás normas que los modifiquen o adicionen. Para efectos de cumplir lo anterior, la SNR actuará de conformidad con lo siguiente:

- Se solicitará autorización del representante legal del niño, niña o adolescente, previo ejercicio del derecho a ser escuchado del menor de edad. Opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto, a efectos de realizar el tratamiento de sus datos personales.
- Se informará el carácter facultativo de responder preguntas acerca de los datos de los niños, niñas o adolescentes.
- Se informará de forma explícita y previa cuáles son los datos objeto de tratamiento y la finalidad de este.

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

Información requerida por la Entidad, en ejercicio de sus funciones legales o por orden judicial.

a) Datos de naturaleza pública.

b) Casos de urgencia médica o sanitaria.

c) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

d) Datos relacionados con el Registro Civil de las Personas.

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

La SNR, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad de este.

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

c) Los derechos que le asisten como Titular.

d) La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.

La SNR como responsable del Tratamiento, deberá conservar prueba del cumplimiento de lo previsto en el presente numeral y, cuando el Titular lo solicite, entregarle copia de esta.

12. FINALIDADES

Las siguientes son las principales finalidades con las que la SNR realiza el tratamiento de la información personal:

12.1 USUARIOS/CIUDADANIA EN GENERAL

a) Controlar las solicitudes relacionadas con los servicios prestados por la Entidad.

b) Emitir las respuestas de las consultas y derechos de petición a los peticionarios.

c) Adelantar los trámites, servicios y otros procedimientos administrativos que sean solicitados a la Entidad

d) Adelantar el cobro coactivo de las sanciones impuesta por la Entidad y para el control de asignación y términos legales dentro de la dependencia.

e) Enviar comunicaciones y notificaciones de actos administrativos emitidos por las Delegaturas y demás áreas misionales y de apoyo de la Entidad.

f) Realizar campañas, actividades de divulgación y capacitaciones como cursos y oferta educativa presencial y virtual.

g) Desarrollar e implementar programas sectoriales.

h) Actualizar bases de bases de datos, incluyendo los casos en que se requiera transmitir o transferir a un tercero, la información para la validación, depuración, enriquecimiento y homogenización de datos, previo cumplimiento de las exigencias legales.

i) Manejo de la información por parte de proveedores y/o contratistas para las gestiones relacionadas con tramites y servicios definidos en sus respectivos vínculos con la Entidad y siempre que ello sea estrictamente necesario.

j) Elaborar estudios, estadísticas, encuestas, análisis de tendencias, relacionados con los servicios que presta la Entidad.

k) Presentar informes a entidades externas, tales como, el Ministerio de Justicia y el Derecho, Contraloría General de la República, Procuraduría General de la Nación, Fiscalía General de la Nación, entre otras, que permitan dar cumplimiento a las exigencias legales y a análisis estadísticos requeridos a la Entidad.

l) Gestionar la información necesaria para el cumplimiento de las obligaciones tributarias, contractuales, comerciales y de registros comerciales, corporativos y contables.

m) Transmitir la información a encargados nacionales o internacionales con los que se tenga una relación operativa que provean los servicios necesarios para la debida operación de la Entidad.

n) Prestar los servicios de información a través de los diferentes medios de contacto.

o) Evaluar la calidad de los servicios prestados.

p) Grabación de imágenes o cualquier otro registro que sirva de soporte y evidencia de los eventos y audiencias realizadas.

q) Mejorar las iniciativas promocionales de la oferta de prestación de servicios y actualización de productos de la Entidad.

r) Las demás finalidades que se determinen en procesos de obtención de Datos Personales para su tratamiento, y en todo caso de acuerdo con la Ley y en el marco de las funciones que lo son atribuibles a la SNR.

s) Realizar el tratamiento de datos a nivel de interoperabilidad con otras entidades del Estado, con el fin de cumplir sus obligaciones misionales utilizando los datos suministrados por los titulares de los datos personales.

12.2 ASPIRANTES A FUNCIONARIOS, FUNCIONARIOS Y EXFUNCIONARIOS

a) Realizar las actividades necesarias para dar cumplimiento a las obligaciones legales en relación con los

aspirantes a funcionarios, funcionarios y exfuncionarios de la Entidad.

b) Controlar el cumplimiento de requisitos relacionados con el Sistema General de Seguridad Social.

c) Publicar los directorios instruccionales.

d) En caso de datos biométricos capturados a través de sistemas de videovigilancia o grabación su tratamiento tendrá como finalidad la identificación, seguridad y la prevención de fraude interno y externo.

e) Para el caso de los participantes en convocatorias de selección, los datos personales tratados tendrán como finalidad adelantar las gestiones de los procesos de selección; las hojas de vida se gestionarán garantizando el principio de acceso restringido.

f) Informar y comunicar las generalidades de los eventos desarrollados por la Entidad por los medios y en las formas que se consideren convenientes.

g) Gestionar la cadena presupuestal de la Entidad: pagos de la Entidad, emisión de certificados de ingresos y retenciones y relaciones de pagos.

h) Gestionar el proceso Contable de la Entidad.

i) Compartir sus datos personales con las autoridades (judiciales o administrativas) nacionales o extranjeras cuando la solicitud se base en razones legales, procesales, y/o tributarias.

j) Consulta de sus datos en las listas restrictivas y vinculantes, en cumplimiento del Programa de Transparencia y Ética Pública en lo referente al Lavado de Activos y Financiación del Terrorismo, así como el cumplimiento con estándares de ética e integridad establecidos por la SNR. Tratándose de exfuncionarios, la SNR almacenará, aún después de finalizado el vínculo laboral, la información necesaria para cumplir con las obligaciones que puedan derivarse en virtud de la relación que existió conforme a la legislación

colombiana, entre otras, la de proporcionar las certificaciones laborales que sean solicitadas y/o aquellas solicitadas por terceros frente a quienes es te adelante un proceso de selección.

12.3 PROVEEDORES/CONTRATISTAS

- Contar con información de cada uno de los contratistas y visitantes que ingresen a las instalaciones de la SNR.
- Controlar e identificar el acceso a las sedes administrativas del Nivel Central.
- Mantener la seguridad y control de accesos a los edificios, sucursales y otras instalaciones en donde desarrolle actividades la SNR.

12.4 ACCESO A SEDES, VIGILANCIA Y SEGURIDAD DE LAS INSTALACIONES

La SNR informa a todos los titulares que los datos recolectados directamente en los puntos de seguridad de las sedes administrativas, edificios, sucursales y otras instalaciones, obtenidos de los documentos de identidad presentados al personal de seguridad, las videograbaciones, que se realizan dentro o fuera de las instalaciones de la SNR, entre otros, se utilizan con fines de seguridad de las personas, los bienes e instalaciones.

CONTROL ACCESO: A efectos de garantizar la confidencialidad o reserva de la información, en aquellas áreas donde se ejecuten procesos relacionados con dicha información se deberán implementar controles de acceso y avisos de privacidad, que restrinjan el ingreso a las instalaciones del personal no autorizado. Así mismo, se debe contar con un registro de ingresos y salidas, que deberá estar documentado a efectos de guardar la trazabilidad correspondiente.

VIDEO VIGILANCIA: La Entidad cuenta con cámaras de videovigilancia instaladas en sus sedes y demás espacios donde se desarrollan sus funciones, con el fin de garantizar la seguridad de las instalaciones, los servidores y los usuarios, por lo anterior y con la finalidad dar cumplimiento a las políticas de seguridad física; las imágenes son conservadas por un tiempo prudencial. En caso de que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea

resuelto. Las Bases de Datos de la SNR tendrán el periodo de vigencia que corresponda a la finalidad para el cual se autorizó su tratamiento y de las normas especiales que regulen la materia, así como aquellas normas que establezcan el ejercicio de las funciones legales asignadas a la Entidad. Las imágenes de las cámaras de seguridad deben conservarse en un sistema o soporte al que solo pueda acceder el personal autorizado y que cuente con las medidas de seguridad técnicas y organizativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de las imágenes.

• Contar con información de cada uno de los funcionarios, contratistas y visitantes que ingresen a las instalaciones de la SNR incluyendo sus sedes.

• Controlar e identificar el acceso a las sedes administrativas del Nivel Central.

• Mantener la seguridad y control de accesos a los edificios, sucursales y otras instalaciones.

La SNR informa a todos los titulares que los datos recolectados directamente en los puntos de seguridad de las sedes administrativas, edificios, sucursales y otras instalaciones, que sean suministrados en documentos del personal de seguridad, y los datos obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de la SNR, se utilizan con fines de seguridad de las personas, los bienes e instalaciones.

NOTA DE CLARIDAD (FINALIDADES – PROVEEDORES/CONTRATISTAS): Sin perjuicio de las finalidades asociadas al control de accesos y seguridad de instalaciones, la SNR podrá tratar datos personales de proveedores/contratistas para: adelantar procesos de selección, contratación, ejecución, supervisión, pagos, control de obligaciones legales/contractuales, verificación de inhabilidades, y gestión de accesos estrictamente necesarios para la ejecución contractual, conforme a los principios de necesidad y acceso restringido.

NOTA DE CLARIDAD (VIDEOVIGILANCIA – CONSERVACIÓN): El término de conservación de registros de videovigilancia, controles de acceso e ingresos/salidas se definirá conforme a la Tabla de Retención Documental (TRD), el Plan de Conservación Documental y/o los instrumentos institucionales aplicables.

Cuando exista requerimiento judicial o administrativo, las imágenes podrán conservarse como evidencia por el tiempo necesario para la atención del proceso correspondiente.

13. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

La SNR podrá transferir y transmitir los datos personales a terceros con quienes tenga relación operativa que le provean de servicios necesarios para la debida operación, o de conformidad con las funciones establecidas en la normatividad vigente. En dichos supuestos, se adoptarán las medidas necesarias para que las personas que tengan acceso a los datos personales cumplan con la presente Política y con los principios de protección de datos personales y obligaciones establecidas en la Ley. La SNR está comprometida con verificar el nivel de los estándares de protección y seguridad del país receptor de la información personal, realizar la declaración de conformidad (cuando aplique) y suscribir contrato de transferencia u otro instrumento jurídico que garantice la protección de los datos personales objeto de transferencia.

En todo caso, cuando la SNR requiera transmitir los datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, establecerá cláusulas contractuales o celebrará el documento idóneo de transmisión de datos personales en el que indicará el alcance del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales, las obligaciones del encargado para con el titular y el responsable y el termino. Mediante dicho instrumento, el encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables vigentes. Además de las obligaciones que impongan normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado:

- Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.

- Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- Guardar confidencialidad respecto del tratamiento de los datos personales.
- En caso de transferencia se dará cumplimiento a las obligaciones estipuladas en la Ley 1581 de 2012 y demás normas concordantes.

13.1 INTEROPERABILIDAD E INTERCAMBIO INTERINSTITUCIONAL DE INFORMACIÓN

Todo intercambio de información con entidades públicas o privadas, en particular con quienes actúa la SNR, deberá contar con fundamento legal, convencional o requerimiento formal que habilite el tratamiento.

El instrumento de intercambio deberá identificar finalidad específica, categorías de datos, campos estrictamente necesarios, responsable o encargado, medidas de seguridad, restricciones de uso posterior, mecanismos de trazabilidad, plazo de conservación, procedimiento de incidentes y obligaciones de confidencialidad. La entrega masiva de información deberá ser excepcional, justificada y sometida a evaluación de riesgo por la dependencia dueña de la información, con apoyo del OPD, OAJ y OTI/SGSI cuando corresponda.

14. DERECHOS DEL TITULAR

Los titulares de los datos que son objeto de tratamiento por la SNR podrán:

a) Conocer, actualizar y rectificar los Datos frente a él o los Encargados del Tratamiento de datos.

b) Solicitar prueba de la autorización otorgada, o cualquier otra que suscriba el titular de los Datos Personales para el efecto, salvo cuando expresamente se exceptúe como requisito para el Tratamiento de datos de conformidad con la ley.

c) Ser informado por la Entidad o el Encargado del Tratamiento, previa solicitud, respecto del uso que se les ha dado a los datos.

d) Presentar ante la autoridad competente quejas o reclamos por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, sustituyan o adicionen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Autoridad Competente haya determinado que, en el Tratamiento la SNR o Encargados del Tratamiento de Datos Personales, han incurrido en conductas contrarias a la ley y a la Constitución. La revocatoria procederá siempre y cuando no exista la obligación legal o contractual de conservar el dato personal.

f) Acceder en forma gratuita a los Datos Personales que hayan sido objeto de Tratamiento.

En concordancia con lo dispuesto en el artículo 20 del Decreto 1377 de 2013, el ejercicio de los derechos anteriormente mencionados podrá ejercerse por las siguientes personas:

• Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

• Por sus causahabientes, quienes deberán acreditar tal calidad.

• Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

• Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

15. DEBERES DEL RESPONSABLE DEL TRATAMIENTO

La SNR como responsable del Tratamiento, deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan la actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la ley.

k) Adoptar procedimientos específicos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso de sus datos.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de

seguridad y existan riesgos en la administración de la información de los Titulares.

o) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

p) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Los encargados deberán cumplir las condiciones mínimas de seguridad definidas en el Registro Nacional de Bases de datos las cuales se pueden consultar en: https://www.supernotariado.gov.co/

q) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley 1581 de 2012 y demás normas concordantes y vigentes.

r) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

s) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente política.

t) Adoptar un Manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

u) Registrar en las bases de datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley.

v) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte

de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

w) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.

x) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

y) Informar a LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO cuando se presenten violaciones

a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

z) Cumplir las instrucciones y requerimientos que imparta LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.

aa) Verificar que el responsable del Tratamiento tiene la autorización para el tratamiento de datos personales del Titular.

ab) Mantener y actualizar el inventario institucional de bases de datos con datos personales, incluyendo como mínimo: dueño, finalidad, categorías de datos, encargados, transferencias/transmisiones y términos de conservación.

ac) Formalizar y ejecutar el proceso institucional de cumplimiento asociado al RNBD (cuando aplique), incluyendo calendario, responsables y evidencias de actualización y reporte de novedades.

ad) Adoptar y mantener un protocolo operativo de gestión de incidentes de seguridad relacionados con datos personales, que incluya detección, contención, análisis, decisiones de notificación, remediación y cierre con lecciones aprendidas.

ae) Mantener una matriz institucional de encargados del tratamiento y cláusulas contractuales estandarizadas verificables para transmisión/encargo, incluyendo obligaciones de seguridad, confidencialidad, subencargados, retorno/supresión y reporte de incidentes.

af) Implementar un control preventivo para evitar exposición de datos personales en publicaciones institucionales, interoperabilidad y respuestas a solicitudes, articulando transparencia, jurídica, seguridad de la información y protección de datos.

16. ATENCIÓN A CONSULTAS Y RECLAMOS

Los titulares de la información cuando requieran realizar alguna consulta, queja o reclamo podrán hacer uso de:

16.1 CONSULTAS.

Los titulares, sus causahabientes o cualquier otra persona que pueda tener un interés legítimo, podrán solicitar que se les informe sobre los datos personales del titular que se encuentren almacenados en cualquier base de datos de la SNR.

De acuerdo con lo anterior, la Entidad garantizará el derecho de consulta, dándole a conocer la información personal vinculada al titular.

Las peticiones presentadas por el titular del dato, relacionadas con consultas que versen sobre temas de acceso a la información, constancias de la autorización otorgada por el titular, usos y finalidades de la información personal, o cualquier otra consulta relacionada con la información personal entregada por parte

del titular, y otros deberán presentarse por medio de los canales habilitados por la Entidad, esto es, envío al correo electrónico, radicación de PQR y/o comunicación telefónica.

La petición deberá ser atendida dentro un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no sea posible atender la consulta dentro del término previsto, se informará al interesado, señalando los motivos de la demora y la fecha en que se atenderá la consulta, la cual no superará los cinco (5) días hábiles siguientes al vencimiento del primer término, de conformidad con lo establecido en el artículo 14 de la Ley 1581 de 2012.

Responsable de atención de consultas: El Oficial de Protección de Datos Personales de la SNR, será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en las presentes políticas.

16.2 RECLAMOS

Derechos garantizados mediante el procedimiento de reclamos:

a) Corrección o Actualización: La SNR, garantizará a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de corregir o actualizar los datos personales que reposen en sus bases de datos, mediante presentación de reclamación, cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política de Tratamiento de Datos Personales para que sea procedente la solicitud de Corrección o Actualización.

b) Revocatoria de la autorización o Supresión de los datos Personales: La SNR, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de solicitar la revocatoria de la autorización o solicitar la supresión de la información contenida en su registro individual o toda aquella que esté vinculada con su identificación cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política de Tratamiento de Datos Personales. Así mismo se garantiza el derecho de presentar reclamos cuando adviertan el presunto incumplimiento de la Ley

1581 de 2012 o de la presente Política de tratamiento de datos personales. Responsable de atención de Reclamos: El Oficial de Protección de Datos Personales de SNR, será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en las presentes políticas. Las reclamaciones presentadas deberán contener como mínimo la siguiente información:

- Nombres y apellidos del Titular y/o su representante y/o causahabientes;
- Describir el motivo del reclamo de forma clara y expresa, donde se establezcan los hechos que originaron el mismo, presentando los documentos que pretenda hacer valer.
- Acreditar el interés legítimo con el que actúa quien presenta el reclamo y adjuntar, en caso de ser necesarios, los soportes correspondientes.
- Señalar la dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
- Firma, número de identificación o procedimiento de validación correspondiente.

Una vez sea recibida la solicitud de ACTUALIZACIÓN o de RECTIFICACIÓN de información por parte del Titular de los datos o su representante o tercero debidamente autorizado, a través de los canales de atención establecidos por la Entidad, la Oficina de Atención al Ciudadano remitirá la solicitud al Oficial de Protección de Datos Personales, quien procederá a verificar que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho se ejerza por un interesado o por un representante de éste, acreditando con ello, que se cuenta con la legitimidad legal para hacerlo.

Reclamaciones sin cumplimiento de Requisitos legales: En caso de que el reclamo resulte incompleto, se requerirá al reclamante dentro de los cinco (5) días hábiles siguientes a su recepción para que subsane las fallas y aporte la información o documentación faltante. El reclamante contará con un término máximo de dos (2) meses, contados a partir del día siguiente al requerimiento, para dar respuesta.

Desistimiento del Reclamo: Transcurridos el término mencionado en el parágrafo anterior dos (2) meses, desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. Los peticionarios y/o interesados podrán desistir en cualquier tiempo de sus peticiones, sin perjuicio de que la respectiva solicitud pueda ser nuevamente presentada con el lleno de los requisitos legales, pero las autoridades podrán continuar de oficio la actuación si la consideran necesaria por razones de interés público; en tal caso expedirán resolución motivada.

Recepción de reclamos que no correspondan a la Entidad: En caso de que la SNR reciba un reclamo dirigido a otra organización, dará traslado a quien corresponda en un término máximo de cinco (5) días hábiles e informará de la situación al reclamante.

Inclusión de leyenda en la base de datos: Recibida la reclamación de forma completa, en un término máximo de dos (2) días hábiles contados desde la recepción, la SNR Incluirán en la base de datos donde se encuentren los datos personales del Titular, una leyenda que diga "reclamo en trámite" y el motivo de este. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

Plazos de Respuesta a los Reclamos: El término máximo para atender el reclamo será lo establecido por la Ley 1755 del 2015 y las demás normas concordantes.

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

Procedimiento de Supresión o Eliminación de Datos Personales: En caso de resultar procedente la supresión/eliminación solicitada por el titular en el marco de un reclamo, la SNR ejecutará la actuación garantizando que la eliminación no permita la recuperación de la información en los repositorios objeto de tratamiento. Previo a la ejecución, se realizará un análisis de impacto para identificar los procesos, sistemas de información, integraciones y repositorios documentales donde se encuentren los datos, así como las

obligaciones legales, contractuales o archivísticas que impidan la supresión total (TRD/PGD). En esos casos, se aplicará la alternativa procedente (restricción del tratamiento, anonimización o conservación por obligación), dejando trazabilidad y evidencias de decisión y ejecución.

Etapas mínimas y responsables:

1) Recepción y radicación del reclamo y remisión al OPD para control de términos.

2) Verificación de identidad o legitimación del solicitante (OAC + OPD).

3) Identificación de la(s) base(s) de datos, proceso(s), sistema(s) de información y repositorios donde se encuentren los datos a suprimir (Dueño del Proceso/DBD + OTI + Archivo/PGD, según aplique).

4) Evaluación de obligaciones de conservación y restricciones de supresión (TRD/PGD, normas especiales, obligaciones contractuales o judiciales), definiendo si procede supresión total o una alternativa (Dueño del Proceso/DBD + Archivo/PGD + OAJ).

5) Evaluación de impacto y riesgos asociados a la supresión (integridad de registros, interoperabilidad, auditoría, disponibilidad) y definición de controles de seguridad para la ejecución (OPD + OTI/SGSI).

6) Decisión de procedencia y forma de atención: supresión, anonimización, restricción del tratamiento o negativa motivada cuando exista obligación de conservar (OPD + Dueño del Proceso/DBD + OAJ, cuando aplique).

7) Ejecución técnica controlada en los sistemas y repositorios aplicables, asegurando trazabilidad (bitácora), control de accesos y eliminación segura cuando proceda (OTI/SGSI + Dueño del Proceso/DBD).

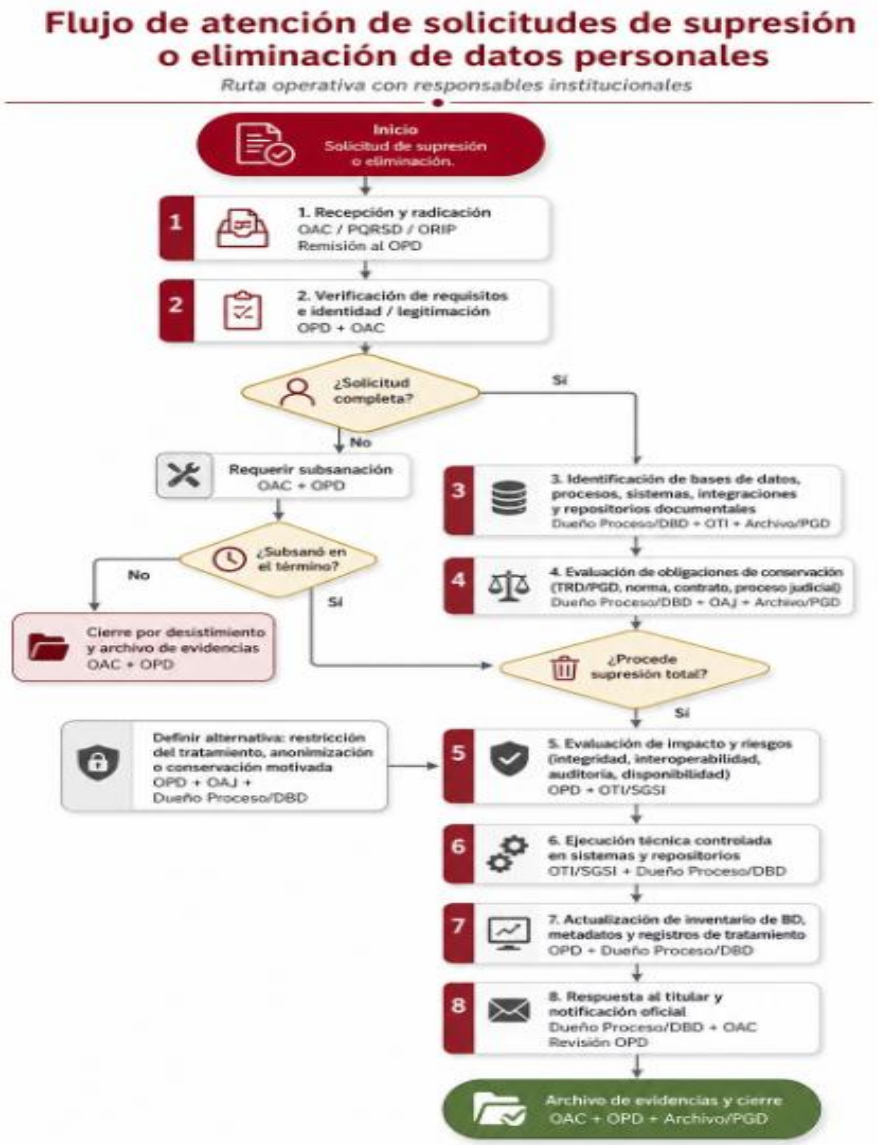
8) Actualización de instrumentos de gestión de datos: inventario de bases de datos, metadatos operativos y registros de tratamiento asociados, incluyendo el estado de la solicitud (OPD + Dueño del Proceso/DBD).

9) Elaboración y notificación de la respuesta al titular, incluyendo la actuación realizada o la motivación de la decisión (Dueño del Proceso/DBD + OAC; revisión OPD).

10) Archivo de evidencias del caso (radicado, análisis de impacto, conceptos, soportes de ejecución, respuesta y notificación) en el repositorio institucional (OAC + OPD + Archivo/PGD).

Flujograma específico del procedimiento de supresión o eliminación de datos personales

El siguiente flujograma resume las etapas mínimas, puntos de decisión y responsables institucionales para atender solicitudes de supresión o eliminación de datos personales



Fuente: Elaboración propia

17. CANALES DE ATENCIÓN

La SNR tiene habilitado para los titulares de los datos personales los siguientes canales de atención para el ejercicio de sus derechos a conocer, actualizar, rectificar y/o suprimir, su información personal.

- **Oficinas de Registro de Instrumentos Públicos:** Los titulares de la información pueden acercarse a cualquier ORIP y presentar su solicitud dentro de los términos establecidos por la ley.
- **Líneas telefónicas:** Para realizar una reclamación acerca del manejo de datos personales los titulares de la información pueden comunicarse a los siguientes teléfonos: o Conmutador: 57+(601) 514 0313

  o Línea Atención al Ciudadano: 57+(601) 514 0313

  o Línea anticorrupción: 01 8000 911 616 o Línea gratuita: 01 8000 911 616
- **Correo Institucional:** correspondenciasnr@supernotariado.gov.co
- **Página web:** En la página web oficial https://servicios.supernotariado.gov.co/login/ el titular de la información puede conectarse con la SNR e instaurar el requerimiento.

18. INSTRUMENTOS COMPLEMENTARIOS DE LA POLÍTICA DE TRATAMIENTO DE DATOS

Son instrumentos complementarios de la presente política los manuales, guías, procedimientos, instructivos, formatos, avisos de privacidad entre otros documentos aprobados y/o divulgados por el Sistema Integrado de Gestión o el Comité Institucional de Gestión y Desempeño que sean necesarios para una implementación y mantenimiento adecuados de los lineamientos establecidos en esta política, así como las normativas vigentes relacionadas con la protección de datos personales.

Adicionalmente, para la implementación y mantenimiento de esta política, la SNR adoptará y mantendrá actualizados, entre otros, los siguientes instrumentos complementarios:

- Inventario institucional de bases de datos con datos personales (con dueño, finalidad, categorías, encargados y conservación).
- Procedimiento institucional RNBD (cuando aplique): calendario de actualización, gestión de cambios sustanciales y reporte de novedades.
- Protocolo institucional de gestión de incidentes de seguridad de datos personales.

- Matriz institucional de encargados del tratamiento y modelo de cláusulas de transmisión/encargo.
- Se debe incorporar el tratamiento de datos personales en los procedimientos relacionados a la gestión del datos y divulgación (publicaciones, interoperabilidad y respuestas).
- Avisos de privacidad estandarizados por canal (web, presencial, videovigilancia e interoperabilidad), que se publicarán o exhibirán en cada punto de recolección o intercambio de información, informando qué datos se tratan, para qué se usan, cómo ejercer derechos y dónde consultar la política.
- Política General para la Administración de Riesgos de la SNR vigente y los instrumentos de identificación, valoración, tratamiento y seguimiento de riesgos institucionales, incluyendo riesgos de privacidad.
- Manual de Políticas del Sistema de Gestión de Seguridad de la Información (SGSI) de la SNR y los procedimientos del SGSI asociados a control de acceso, incidentes, continuidad, proveedores y cumplimiento.
- Registro y matriz de riesgos de privacidad (tratamiento de datos personales) integrada al modelo institucional de gestión de riesgos, con sus controles y planes de tratamiento.
- Instrumentos de arquitectura de información y gestión de datos que aseguren trazabilidad (catálogo/registro de activos de información, matriz proceso-sistema-dato y mecanismos de linaje cuando aplique).
- Procedimiento operativo de supresión/eliminación, anonimización y restricción del tratamiento, con evidencias de impacto, ejecución técnica y cierre.

19. BIBLIOGRAFÍA

- Ley 1581 de 2012 - https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
- Manual de Responsabilidad Demostrada Superintendencia de Industria y Comercio – https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
GIIAD-PI-001	1	28/05/2026	Actualización integral: incorporación de OPD, funciones mínimas, ruta única y escalamiento; ajuste del procedimiento de supresión/eliminación con análisis de impacto en procesos y sistemas; alineación con la Política General de Administración de Riesgos y con el Manual del SGSI; y fortalecimiento de trazabilidad en la arquitectura de información.
GTI - PI - 001	1	3/Oct./2025	Se determina el cambio de estado a obsoleto del presente documento, teniendo en cuenta que, a partir del 27 de mayo de 2026, la función de Oficial de Protección de Datos fue asignada a la Oficina Asesora de Planeación, de conformidad con el memorando SNR2026IE-015872-3. En consecuencia, la responsabilidad del documento cambia de proceso y pasa de su ubicación actual, es decir **Gestión de Tecnologias de la Información** al proceso de Gestión de la Innovación, Investigación y Analítica de Datos. Por lo anterior, no es procedente mantener la trazabilidad de versionamiento del documento existente, razón por la cual se gestiona como un nuevo documento dentro del proceso responsable.

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	**APROBÓ**	**REVISIÓN METODOLÓGICA**	**Vo. Bo. Oficina Asesora de Planeación**
Rafael Ramos Ballesteros, Diego Alejandro Peñalosa Cubillos	Nubia Patricia Lopez Mendez	Laura Nathalia Cardenas Jimenez	Nubia Patricia Lopez Mendez
Contratista - Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación **Comité de Gestión Institucional de Gestión y Desempeño II Sesión Extraordinaria**	Funcionaria - Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación
Fecha: 15/04/2026	Fecha: 15/05/2026	Fecha: 27/05/2026	Fecha de Aprobación: 29/05/2026