Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Transformación Digital
de la Rama Judicial

INFORME EJECUTIVO

Protección de Datos Personales e Información Sensible en la Rama Judicial

Autodiagnóstico y Mesas Técnicas

Julio de 2025

Índice

Alcance

El Consejo Superior de la Judicatura, comprometido con el derecho a la protección de los datos personales de todos los actores que interactúan con la Rama Judicial, así como con otros derechos fundamentales como la intimidad, la imagen y la dignidad humana, llevó a cabo durante el primer semestre de 2025 dos ejercicios estratégicos, enfocados a identificar oportunidades de mejora en la gestión de datos personales e información sensible que circula tanto en el marco de los procesos judiciales como, en algunos casos, en el desarrollo de funciones administrativas. En este contexto, se desplegaron dos actividades clave:

- Un autodiagnóstico a nivel nacional en materia de protección de datos personales dirigido a jueces, magistrados, secretarios, relatores, oficiales mayores, auxiliares de justicia, personal administrativo, entre otros, con el objetivo de identificar las prácticas actuales, niveles de conocimiento, brechas operativas y necesidades institucionales relacionadas con el tratamiento de datos personales, incluyendo datos personales sensibles.

- Un ciclo de mesas técnicas dirigidas a las distintas jurisdicciones y especialidades, conformadas por servidores judiciales y administrativos, orientadas al fortalecimiento participativo del Protocolo para el Manejo del Material Probatorio con Información Sensible.

Ambas actividades, aunque distintas en su metodología y alcance, compartieron un propósito institucional común: ayudar a consolidar una política robusta, articulada, coherente y operativa de tratamiento de datos personales, que garantice un manejo ético, seguro y legal de la información personal, incluyendo la información sensible que se realiza su tratamiento en los despachos.

Este esfuerzo institucional se complementa con la formulación de un Protocolo para el Manejo del Material Probatorio con Información Sensible, así como con lineamientos para la publicación de contenidos web y procedimientos adicionales orientados a reforzar la protección de la información personal. Adicionalmente, estas acciones buscan avanzar en el cumplimiento a las órdenes impartidas por la Corte Constitucional, en particular en las sentencias **T-280 de 2022, SU-355 de 2022, T-398 de 2023 y T-203 de 2025.**

1 Resultado de la encuesta de autodiagnóstico sobre Protección de Datos Personales

1.1 Objetivo del autodiagnóstico

Identificar las prácticas actuales, niveles de conocimiento, medidas de protección implementadas y necesidades institucionales relacionadas con la protección de datos personales e información sensible en los despachos judiciales y en las funciones administrativas.

1.2 Ficha técnica

- **Título:** Diagnóstico inicial del tratamiento de datos personales y sensibles en la Rama Judicial
- **Instrumento de recolección:** Cuestionario estructurado aplicado digitalmente mediante Microsoft Forms.
- **Cobertura geográfica:** Nacional, en todas las jurisdicciones y especialidades de la Rama Judicial.
- **Población objetivo:** Servidores judiciales de diferentes niveles y roles (jueces, magistrados, secretarios, oficiales mayores, personal administrativo).
- **Tamaño de muestra:** 2.952 respuestas válidas (muestra voluntaria, de carácter no probabilístico).
- **Limitaciones del estudio:** La muestra no es estadísticamente representativa.
- **Periodo de aplicación:** Del 22 al 30 de mayo de 2025.

1.3 Perfil de los participantes

Jurisdicción o especialidad

- Del total de servidores judiciales que participaron en el autodiagnóstico, el 76,42 % pertenece a la jurisdicción ordinaria.
- En segundo lugar, se destaca la participación de la jurisdicción contenciosa administrativa (11,69%), seguida por otras jurisdicciones, así como dependencias administrativas que, aunque con menor representación porcentual, desempeñan un papel significativo en funciones transversales de gestión, apoyo y supervisión institucional.

1 Resultado de la encuesta de autodiagnóstico sobre Protección de Datos Personales

Especialidad

- La especialidad penal (35%) y la especialidad civil (29%) concentran la mayor proporción de respuestas, seguidas por despachos promiscuos (17 %), laboral (13 %) y de familia (7 %).
- Esta distribución refleja una amplia exposición a procesos con elevada carga probatoria, en los que es frecuente el tratamiento de información personal sensible, incluyendo historias clínicas, registros disciplinarios, testimonios de menores, imágenes, entre otros.

Cargos representados

- El cargo con mayor representación en la muestra es el de secretario (45,87%), seguido por jueces (23,38%) y otros actores relevantes como magistrados, oficiales mayores, auxiliares judiciales, escribientes, personal administrativo y de apoyo.
- Esta composición revela una estructura operativa piramidal en la que los niveles intermedios y de gestión documental asumen una gran parte de la responsabilidad en el manejo diario de datos personales.

1.4 Gestión de datos personales y sensibles

Tratamiento de datos personales

El 88% de los encuestados manifestó que en el desarrollo de sus funciones recolecta, administra o almacena datos personales, lo que evidencia el carácter masivo y transversal del tratamiento de información personal dentro de las funciones judiciales.

Tipos de datos más comunes tratados

Los encuestados indicaron que los datos más comúnmente tratados incluyen:

- **Datos identificativos y de contacto** (nombres, cédulas, teléfonos, correos electrónicos).
- **Datos sensibles** tales como historial médico, estado de salud, orientación sexual, étnica, así como fotografías.
- **Datos socioeconómicos y laborales**, ampliamente presentes en procesos civiles, laborales y de familia.

1 Resultado de la encuesta de autodiagnóstico sobre Protección de Datos personales

Manejo de información sensible

El 81% de los participantes indicó que gestiona regularmente información considerada sensible. Esta cifra refuerza la necesidad de contar con protocolos institucionales sólidos, medidas tecnológicas robustas, mecanismos de trazabilidad y programas de formación en protección de datos.

1.5 Determinación de la sensibilidad de la información

- Ante la consulta sobre quién determina el nivel de sensibilidad de la información en los despachos, el 37,47% indicó que esta función recae principalmente en jueces o magistrados.
- Sin embargo, un 16,57 % atribuye esta tarea a los secretarios, mientras que un 6,11 % reconoce que no existe una definición clara en su despacho.

Esta dispersión en los criterios y responsabilidades evidencia una brecha institucional, que puede generar inconsistencias en el tratamiento y protección de la información y pone de manifiesto la necesidad de estandarizar lineamientos operativos que delimiten funciones.

1.6 Riesgos identificados y casos reportados

Los servidores judiciales participantes señalaron ciertos riesgos operativos para la integridad y confidencialidad de los datos personales y sensibles. Entre los principales se destacan:

- **Pérdida o borrado de información**, derivada de fallas técnicas, almacenamiento inseguro o prácticas inadecuadas de gestión.
- **Accesos indebidos a carpetas compartidas** que exponen la información sin controles robustos de acceso.
- **Manipulación o alteración de documentos procesales** o grabaciones, intencionadas o accidentales.
- **Limitaciones de respaldo digital confiable** en la infraestructura tecnológica adecuada para soportar una gestión segura.

Estos hallazgos refuerzan la necesidad de implementar medidas estructurales preventivas y fortalecimiento institucional.

1 Resultado de la encuesta de autodiagnóstico sobre Protección de Datos Personales

1.7 Acciones prioritarias propuestas por los participantes

A partir de su experiencia práctica, los participantes propusieron un conjunto de medidas prioritarias para mejorar el tratamiento y la protección de datos personales y sensibles en la Rama Judicial:

- **Capacitación diferenciada por perfil funcional.** Diseñar e implementar programas de formación continua orientados por rol (jueces, secretarios, auxiliares, administrativos), con énfasis en:
  - Fundamentos normativos sobre protección de datos personales.
  - Técnicas de anonimización[1] y seudonimización[2].
  - Uso seguro y eficiente de las plataformas institucionales (SIUGJ, SGDE, OneDrive, etc.).
  - Identificación de riesgos asociados al ciclo de vida de los datos.
- **Protocolos institucionales claros, estandarizados y vinculantes.** Establecer lineamientos que definan, de manera uniforme y vinculante:
  - Los criterios de clasificación de información (pública, reservada, sensible).
  - Las condiciones de acceso por niveles de autorización.
  - Los procedimientos de conservación, traslado, consulta, custodia y eliminación de datos personales y sensibles.
- **Tecnología segura e interoperable.** Reforzar la infraestructura tecnológica mediante:
  - Autenticación multifactor[3]
  - Cifrado de extremo a extremo[4]
  - Trazabilidad integral de accesos y modificaciones.
  - Integración de sistemas judiciales con políticas activas de ciberseguridad.

---

1. Anonimización: es el proceso mediante el cual se condiciona un conjunto de datos de modo que no se pueda identificar a una persona, pero pueda ser utilizada para realizar análisis técnico y científico válido sobre ese conjunto de datos (MIT, 2007). Para el cumplimiento de los estándares de anonimización, los datos deben ser despojados de elementos suficientes para que el titular de los datos ya no pueda ser identificado, y por lo tanto estos datos deben procesarse para que no sea posible identificar a una persona mediante el uso de todos los medios razonables para ser utilizados por cualquier otra persona (Data Protection Commission, 2019). (Guía de Anonimización de Datos Estructurados, Archivo General de la Nación)

2. Seudonimización: consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. (...) La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización (Dictamen 05/2014 sobre técnicas de anonimización del Comité Europeo de Protección de Datos)

1 Resultado de la encuesta de autodiagnóstico sobre Protección de Datos Personales

- **Gestión documental centralizada y estandarizada:** Consolidar un modelo único de gestión documental que incluya:
  - Tablas de retención documental ajustadas al nivel de sensibilidad de la información.
  - Repositorios digitales institucionales con monitoreo permanente.
  - Responsables definidos para la administración de archivos.
- **Fortalecimiento organizacional:** Garantizar el cumplimiento y sostenibilidad de estas medidas mediante:
  - Designación de personal técnico especializado en protección de datos.
  - Implementación de auditorías internas periódicas.
  - Establecimiento de líneas de reporte y actuación frente a incidentes de seguridad de la información.

3. La autenticación multifactor es un mecanismo de seguridad que requiere más de un método de verificación para confirmar la identidad de un usuario al acceder a un sistema, aplicación o servicio.

4. El cifrado de extremo a extremo es un método de protección de datos que asegura que solo el emisor y el receptor de un mensaje pueden acceder a su contenido.

2 Mesas de trabajo sobre manejo de material probatorio con información sensible

2.1 Objetivo del ejercicio

Obtener insumos técnicos, operativos y normativos para el fortalecimiento de la propuesta de protocolo de manejo de material probatorio con información sensible en la Rama Judicial, a través del desarrollo de mesas técnicas con actores de la Rama Judicial, que permitan identificar buenas prácticas, retos de implementación y recomendaciones alineadas con el respeto a los derechos a la intimidad, a la imagen y a la protección de datos personales en la administración de justicia.

2.2 Metodología

El ejercicio se desarrolló de manera participativa, a través de cuatro mesas técnicas organizadas por jurisdicción o función transversal, con la participación activa de 61 personas entre jueces, magistrados, personal administrativo y técnico. Se llevaron a cabo, entre el 3 al 11 de julio de 2025. Las sesiones se distribuyeron de la siguiente forma

- **Sesión 1:** Penal y Familia
- **Sesión 2:** Civil y Laboral
- **Sesión 3:** Contencioso Administrativo, Disciplina Judicial.
- **Sesión 4:** Revisión tecnológica y gestión documental

Cada mesa trabajó con herramientas colaborativas, utilizando plantillas orientadoras que permitieron mapear problemas reales, priorizar riesgos y construir soluciones operativas desde la experiencia institucional.

2.3 Resultados por mesa temática

Los siguientes resultados corresponden al análisis de los aportes recopilados en las mesas temáticas desarrolladas. Esta etapa inicial buscaba organizar y sintetizar los principales puntos discutidos por los participantes en torno a los desafíos y propuestas relacionados con la protección de datos personales en el ámbito judicial. Si bien los resultados presentados permiten identificar tendencias y recomendaciones clave por cada área temática, se está realizando un análisis más profundo y detallado del insumo, con el fin de afinar las propuestas regulatorias, técnicas y operativas viables. A continuación, se presenta un resumen de los principales resultados por mesa:

2 Mesas de trabajo sobre manejo de material probatorio con información sensible

Mesa 1: Penal y Familia

- Se reiteró la aplicación del principio de reserva de información (art. 14 CPP) en audiencias preliminares, con reserva total del material sensible.
- En el juicio oral, el juez debe acceder íntegramente a las pruebas, pero su exhibición debe realizarse en audiencia de forma restringida, cuando se trate de información sensible.
- Se propuso reforzar las herramientas legales existentes, especialmente para audiencias con víctimas menores de edad o riesgo de revictimización.
- Se identificaron como medidas adicionales la seudonimización de víctimas, acuerdos de confidencialidad y restricciones de publicidad.
- La falta de un protocolo sobre la caducidad del dato negativo en sentencias fue señalada como un vacío que requiere regulación al interior de la Rama Judicial.

Mesa 2: Civil y Laboral

- Se recomendó diseñar un protocolo basado en el principio de **"**privacidad por diseño**"**, que incorpore:
  - Etiquetado desde el origen (al radicar la demanda) de cada prueba: pública, reservada o sensible.
  - Repositorios judiciales con cifrado, autenticación multifactor y prohibición de almacenamiento de información personal en equipos institucionales**.**
  - Control de acceso exclusivo a partes y apoderados, con anonimización previa de datos sensibles.
  - Canales oficiales únicos de circulación con trazabilidad completa.
  - Un sistema de descatalogación y conservación segura al cierre del proceso.
- La propuesta enfatiza el ciclo de vida completo del dato: desde su ingreso hasta su eliminación o archivo.

---

5. Seudonimización: consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. (…) La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización (Dictamen 05/2014 sobre técnicas de anonimización del Comité Europeo de Protección de Datos)

6. La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva [9] para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso) Definición de la Agencia Española de Protección de Datos

7.Se refiere a un procedimiento o mecanismo mediante el cual se retiran ciertos elementos de un catálogo, base de datos o inventario. Es decir, se marca que ya no están activos, disponibles o vigentes.

2 Mesas de trabajo sobre manejo de material probatorio con información sensible

Mesa 3: Contencioso Administrativo y Disciplinario

- Se resaltó la sobrecarga judicial como un factor que dificulta una adecuada protección de datos sensibles.
- Se propuso fortalecer la planta judicial y aplicar principios de oportunidad para descongestionar casos.
- En materia tecnológica, se sugirió reemplazar OneDrive y SharePoint por un sistema documental judicial especializado**,** con administrador de seguridad de la información que controle permisos, cifrado y trazabilidad.
- Para evitar fugas o dispersión, se recomendó eliminar el uso de carpetas compartidas, correos personales o accesos sin roles definidos.
- Se insistió en la necesidad de contar con un compendio normativo único**,** que unifique criterios sobre qué información se reserva, por cuánto tiempo y bajo qué condiciones.

Mesa 4: Gestión Documental y Tecnología

- Se planteó como prioridad la parametrización de las tablas de retención en los sistemas judiciales, de modo que todo expediente tenga una etiqueta visible de su nivel de sensibilidad.
- Se recomendó establecer un sistema automatizado de anonimización (con enmascaramiento[8] y seudonimización), que proteja la integridad del expediente sin alterar su estructura visual o jurídica.
- Se propuso incorporar metadatos controlados que generen alertas ante exportación o publicación de información sensible.
- En cuanto al ciclo de vida digital, se sugirió implementar:
  - Reglas temporales de **desindexación**[9] o baja automática de visibilidad**.**
  - Flujos internos claros para solicitudes de desindexación y anonimización.
- Finalmente, se reiteró la necesidad de capacitación permanente sobre ciberseguridad, anonimización, normativa de protección de datos y manejo de plataformas institucionales (Ley 1581 de 2012, Ley 1712 de 2014, Sentencia T729 de 2015).

8. Es una técnica que oculta parcial o totalmente la información sensible o confidencial, de forma que solo se muestre lo estrictamente necesario, sin revelar los datos reales.
9. Desindexación: es el proceso mediante el cual se retira un contenido de los resultados de los buscadores de internet (como Google) para que no aparezca fácilmente al buscar ciertos datos, como el nombre de una persona. La información no se elimina del sitio web original, simplemente deja de ser visible a través de los motores de búsqueda cuando se utiliza un criterio específico (como el nombre del titular de los datos).

2 Mesas de trabajo sobre manejo de material probatorio con información sensible

2.4 Recomendaciones generales

Con base en los aportes recogidos en las mesas, se plantean las siguientes acciones estratégicas:

- **Adopción de un protocolo transversal de manejo de material probatorio con información sensible,** el cual de manera progresiva se adaptará según jurisdicción y especialidad.
- **Revisión y fortalecimiento normativo**, con enfoque unificado en criterios de clasificación, acceso, circulación y caducidad de información.
- **Fortalecimiento tecnológico**, con sistemas de gestión documental seguros, trazables y accesibles sólo por roles autorizados.
- **Implementación de medidas preventivas**, como anonimización[10], seudonimización[11] y caducidad del dato negativo[12] de manera controlada.
- **Formación continua y especializada**, diferenciada por rol, y con énfasis en el uso correcto de plataformas institucionales.
- **Seguimiento y evaluación periódica**, con auditorías internas y responsables designados por área para verificar el cumplimiento del protocolo.

10. Anonimización: es el proceso mediante el cual se condiciona un conjunto de datos de modo que no se pueda identificar a una persona, pero pueda ser utilizada para realizar análisis técnico y científico válido sobre ese conjunto de datos (MIT, 2007). Para el cumplimiento de los estándares de anonimización, los datos deben ser despojados de elementos suficientes para que el titular de los datos ya no pueda ser identificado, y por lo tanto estos datos deben procesarse para que no sea posible identificar a una persona mediante el uso de todos los medios razonables para ser utilizados por cualquier otra persona (Data Protection Commission, 2019). (Guía de Anonimización de Datos Estructurados, Archivo General de la Nación)

11. Seudonimización: consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. (...) La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización (Dictamen 05/2014 sobre técnicas de anonimización del Comité Europeo de Protección de Datos)

12. Caducidad del Dato Negativo: la información que resulte desfavorable al titular debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad, de forma que queda prohibida la conservación indefinida de los datos después que han desaparecido las causas que justificaron su acopio y administración (párrafo 69, Sentencia T-398 de 2023)

3 Conclusiones del autodiagnóstico y el desarrollo de las mesas técnicas

El trabajo articulado entre las distintas jurisdicciones, especialidades y equipos técnicos permitió identificar tanto los desafíos operativos como las oportunidades de mejora en el tratamiento de datos personales, incluyendo información sensible.

El protocolo que surja de estas mesas debe reflejar un enfoque preventivo, práctico y adaptable, que respalde el deber institucional de proteger los datos personales y sensibles, sin obstaculizar el acceso a la justicia ni el principio de contradicción. Consolidar esta herramienta permitirá avanzar hacia una administración de justicia más segura, confiable y respetuosa de los derechos fundamentales.

El análisis conjunto del autodiagnóstico y de las mesas técnicas confirma que el tratamiento de datos personales y la gestión del material probatorio sensible son funciones transversales, de alto impacto y riesgo institucional para la Rama Judicial. Su adecuado manejo incide directamente en la garantía de los derechos fundamentales, la legitimidad de las actuaciones judiciales y la confianza de la ciudadanía en el sistema de justicia.
Ambos ejercicios permitieron:

- **Visibilizar las prácticas actuales**, las brechas tecnológicas, normativas y operativas en la gestión de información sensible.
- **Recoger propuestas concretas**, viables y contextualizadas desde la experiencia directa de los operadores judiciales.
- **Generar insumos técnicos y estratégicos** para estructurar la propuesta de un protocolo institucional robusto, preventivo y operativo.

4 Siguientes pasos

A partir de las actividades ejecutadas, las próximas acciones se enfocarán en culminar las etapas pendientes con el objetivo de lograr la implementación integral de la Política de Tratamiento de Datos Personales. En este sentido, se procederá a:

1. **Finalizar las etapas de revisión, ajustes, socialización y comentarios**, del documento de **Política de Tratamiento de Datos**, asegurando su adopción, difusión y apropiación por parte de todos los actores involucrados.

2. En cuanto al **Protocolo de Manejo de Material Probatorio con Información Sensible**, se adaptarán las recomendaciones y buenas prácticas obtenidas a partir de las mesas técnicas, seguido de su análisis, ajustes al documento, socialización, adopción, difusión y apropiación.

3. Para los **Lineamientos de Publicaciones Web**, se fortalecerá la versión actual, realizar los ajustes necesarios y socializar el documento resultante.

4. En el caso del **Manual Interno de Políticas y Procedimientos en Protección de Datos Personales**, se desarrollarán las propuestas y actualizaciones correspondientes en cuanto a procedimientos, roles, obligaciones y controles, consolidando posteriormente el manual unificado, su revisión y socialización.

Estas acciones garantizarán la consolidación de un marco normativo interno robusto y alineado con la normativa vigente en protección de datos personales, transparencia y acceso a la información pública fortaleciendo las capacidades institucionales en esta materia.