Guía para la anonimización de datos personales y *compliance* en inteligencia artificial para el sistema Jurisemia

Anexo I del Acuerdo Reglamentario n.°1939 Serie "A" del 14/05/2026

Índice

Guía para la anonimización de datos personales y *compliance* en inteligencia artificial para el sistema Jurisemia

1. Introducción: objetivos y alcance

Imaginemos un caso judicial publicado en línea donde, sin intención, se menciona el nombre de una víctima menor de edad o se incluyen datos médicos de una persona. En segundos, esa información podría ser indexada por buscadores o utilizada por sistemas automáticos de inteligencia artificial, quedando fuera del control del Poder Judicial. Un simple descuido puede afectar derechos fundamentales y dañar la confianza ciudadana.

Ahora, supongamos una sentencia dictada en una causa de violencia doméstica. Aunque el expediente no se publica de manera completa, la resolución final se sube al buscador de jurisprudencia y aparece el nombre y apellido de la víctima, número de documento y dirección parcial. Un periodista o ciudadano la encuentra, reproduce esos datos y eso desencadena un problema institucional, pues no se respetó su privacidad, generando un daño irreparable para esa persona.

Para evitar estos riesgos y garantizar la protección de los datos personales -especialmente de las categorías especiales de datos personales (datos sensibles y datos de personas especialmente protegidas)-, el Poder Judicial de Córdoba, implementa un plan integral de protección de datos personales y *compliance* en inteligencia artificial (IA) para los documentos judiciales procesados mediante el sistema Jurisemia. La Guía para la anonimización de datos personales y *compliance* en inteligencia artificial para el sistema Jurisemia, en adelante la Guía, establece los lineamientos operativos y las buenas prácticas que aseguran que la carga, anonimización, revisión y control de calidad de los documentos se efectúen de manera segura, confiable y conforme a los principios de protección de datos personales. Asimismo, la Guía promueve la transparencia, la claridad y la responsabilidad proactiva en el uso de la IA.

La Guía está dirigida a agentes judiciales, equipos técnicos y operadores involucrados en la gestión, tratamiento y publicación de documentos judiciales. Su finalidad es orientar las tareas de anonimización de manera clara, homogénea y eficiente, combinando la protección de la privacidad con la transparencia y accesibilidad pública de la jurisprudencia. Este documento institucional se apoya en las normas nacionales e internacionales sobre protección de datos personales, en las recomendaciones de organismos especializados y en las mejores prácticas globales para la anonimización de información judicial.

La anonimización no es solo una obligación legal, es también una herramienta de confianza pública. Permite que la sociedad acceda a información valiosa y amplíe su conocimiento jurídico sin poner en riesgo la intimidad, la dignidad ni los derechos de las personas que intervienen en los procesos judiciales. En este sentido, la relevancia de proteger los datos personales en contextos de inteligencia artificial ha sido

reconocida a nivel internacional. La "Recomendación sobre la Ética de la Inteligencia Artificial" de la UNESCO (2021) insta a los Estados Miembros a:

"[...] establecer sus políticas de datos o marcos equivalentes, o reforzar las políticas y marcos existentes, para garantizar la seguridad total de los datos personales y los datos sensibles que, de ser divulgados, puedan causar daños, lesiones o dificultades excepcionales a las personas"[1].

El Estado argentino adoptó esta recomendación y, en 2023, la Subsecretaría de Tecnologías de la Información emitió la Disposición 2/23, que toma como base directa dicho instrumento. El presente documento se inscribe en esa misma línea, trasladando estos principios al ámbito concreto del tratamiento de documentos judiciales en el sistema Jurisemia.

2. Publicidad de las resoluciones judiciales

El deber de publicidad de resoluciones judiciales tiene base constitucional en la forma republicana de gobierno, de la que deriva el principio de publicidad de los actos de gobierno, y en tratados internacionales de derechos humanos con jerarquía constitucional, como en el derecho de acceso a la información pública. Asimismo, responde a la función pública de las decisiones judiciales, que deben ser accesibles para garantizar la transparencia, la rendición de cuentas y la difusión del derecho, lo que fortalece las capacidades estatales y la independencia del Poder Judicial. Así, el mayor conocimiento de la sociedad de las decisiones judiciales contribuye a la seguridad jurídica, la igualdad, el derecho de defensa y la transparencia de la Administración de justicia[2].

La publicación de resoluciones judiciales encuentra su fundamento primordial en el derecho de acceso a la información pública, consagrado en la Ley n.°27275. La normativa señalada establece una serie de principios rectores a fin de garantizar este derecho (art. 1, ib.), entre los que se destacan:

- Presunción de publicidad: toda la información en poder del Estado se presume pública, salvo las excepciones previstas por esta ley.
- Transparencia y máxima divulgación: toda la información en poder, custodia o bajo control del sujeto obligado debe ser accesible para todas las personas. El acceso a la información pública sólo puede ser limitado cuando concurra alguna de las excepciones previstas en esta ley, de acuerdo con las necesidades de la sociedad democrática y republicana, proporcionales al interés que las justifican.

[1] Organización de los Estados Americanos. (2021). Principios actualizados sobre la privacidad y la protección de datos personales.
[2] Podestá, F. (2010). Tratamiento de datos personales en la Justicia digital: Panorama argentino y otras referencias [Ponencia]. Seminario Regional de Protección de Datos, Montevideo, Uruguay, 1–4 de junio de 2010. Red Iberoamericana de Protección de Datos. Recuperado de https://www.redipd.org/sites/default/files/2020-01/Tratamiento_DP_en_PJ_F_Podesta.pdf

- Máximo acceso: la información debe publicarse de forma completa, con el mayor nivel de desagregación posible y por la mayor cantidad de medios disponibles.

- Apertura: la información debe ser accesible en formatos electrónicos abiertos, que faciliten su procesamiento por medios automáticos que permitan su reutilización o su redistribución por parte de terceros.

- Disociación: en aquel caso en el que parte de la información se encuadre dentro de las excepciones taxativamente establecidas por esta ley, la información no exceptuada debe ser publicada en una versión del documento que tache, oculte o disocie aquellas partes sujetas a la excepción.

- Responsabilidad: el incumplimiento de las obligaciones que esta ley impone originará responsabilidades y dará lugar a las sanciones que correspondan.

- Alcance limitado de las excepciones: los límites al derecho de acceso a la información pública deben ser excepcionales, establecidos previamente conforme a lo estipulado en esta ley, y formulados en términos claros y precisos, quedando la responsabilidad de demostrar la validez de cualquier restricción al acceso a la información a cargo del sujeto al que se le requiere la información.

- Buena fe: para garantizar el efectivo ejercicio del acceso a la información, resulta esencial que los sujetos obligados actúen de buena fe, es decir, que interpreten la ley de manera tal que sirva para cumplir los fines perseguidos por el derecho de acceso, que aseguren la estricta aplicación del derecho, brinden los medios de asistencia necesarios a los solicitantes, promuevan la cultura de transparencia y actúen con diligencia, profesionalidad y lealtad institucional.

Esta ley además de garantizar el efectivo ejercicio del derecho de acceso a la información pública, busca promover la participación ciudadana y la transparencia de la gestión pública, principios que se aplican plenamente al Poder Judicial como parte del Estado.

En este sentido, los propósitos y principios de la Carta de la OEA y sus instrumentos regionales de derechos humanos, señalan que en una “sociedad de la información” centrada en la persona y orientada al desarrollo, la protección del derecho de las personas a tener acceso a información y conocimientos, a usarlos y a difundirlos puede ayudar a las personas, a las comunidades y a los pueblos a alcanzar su pleno potencial, promover el desarrollo sostenible y mejorar la calidad de vida en general[3].

La publicación de sentencias permite el conocimiento de los criterios jurisprudenciales vigentes, el debate público informado sobre la administración de justicia, el ejercicio efectivo de los derechos de defensa y el acceso igualitario a la información judicial. La disponibilidad de la jurisprudencia publicada genera mayor predictibilidad en las decisiones judiciales, coherencia en la aplicación del derecho,

[3] Organización de los Estados Americanos. (2021). Principios actualizados sobre la privacidad y la protección de datos personales.

posibilidad de identificar precedentes relevantes y el desarrollo progresivo de la doctrina jurídica.

En virtud de ello, el Tribunal Superior de Justicia (TSJ), a través del Boletín Judicial (cfr. arts. 99, 100, 101 y 102 de la Ley n.°8435 -Orgánica del Poder Judicial- y del Decreto Ley n.° 7212-A de fecha 22 de abril de 1957), y bajo un criterio orientado a la democratización de la información pública, procura garantizar estos principios. Para cumplir con este cometido, el TSJ -mediante el trabajo conjunto del Boletín Judicial (área de apoyo del TSJ), Data Center y el Área de Investigación, Desarrollo e Innovación Tecnológica- pone a disposición de la comunidad jurídica y judicial: Jurisemia. Un sistema que permite almacenar, sistematizar y consultar jurisprudencia, en tanto, ofrece a cada dependencia judicial la posibilidad de construir su propio repositorio jurisprudencial personalizado e incorpora un buscador semántico que, mediante técnicas de procesamiento del lenguaje natural, interpreta el lenguaje jurídico de las consultas y proporciona resultados más precisos y relevantes. Así, mediante el uso de inteligencia artificial, permite optimizar el acceso y la consulta de la jurisprudencia y los acuerdos del Poder Judicial de Córdoba, fortaleciendo la eficiencia y la transparencia institucional, y aportando transparencia algorítmica y rendición de cuentas, al facilitar que la ciudadanía comprenda cómo se administra justicia.

No obstante, en la medida en que las organizaciones públicas implementan innovaciones digitales basadas en procesamiento automatizado de datos e inteligencia artificial, la exigencia de responsabilidad y transparencia se agudiza. En este sentido, la teoría de las capacidades estatales autónomas sostiene que la fortaleza de las instituciones públicas depende de su capacidad de formular, ejecutar y controlar sus propias políticas con transparencia. La transparencia judicial fortalece la democracia, mejora la calidad institucional, permite el control ciudadano y garantiza la seguridad jurídica.

En este contexto, el Estado no es un actor más, tiene mayor responsabilidad y pone en juego su credibilidad y legitimidad. La falta de transparencia puede perjudicar a las personas, socavar la confianza del público y dificultar la rendición de cuentas. Es por ello, que esta Guía insiste sobre mejores prácticas de transparencia algorítmica en el Estado para dar garantías y seguridad a los ciudadanos.

2.1. El balance entre la publicidad de las resoluciones judiciales y la protección de datos personales

El acceso a la información pública y la protección de datos personales son indispensables para la democracia y el pleno ejercicio de los derechos humanos, la Organización de Estados Americanos (OEA) sostiene que ambos deben aplicarse complementariamente para hacer efectivas la participación ciudadana y la rendición de cuentas por parte de los Estados, contribuyendo al fortalecimiento de las instituciones públicas, a la igualdad, a la transparencia y a la plena vigencia del Estado de derecho[4].

[4] Organización de los Estados Americanos. (2017). Fortalecimiento de la democracia (AG/RES. 2905 [XLVII-O/17]).

Como se ha señalado, la publicación de resoluciones judiciales en la Provincia de Córdoba es una obligación que deriva del derecho de acceso a la información pública, del principio de transparencia estatal y de los estándares internacionales en materia de derechos humanos y democracia. No obstante, el cumplimiento de esta obligación no puede traducirse en un menoscabo de la protección de datos personales. Por el contrario, el acceso a la información pública y la protección de datos personales, deben entenderse como principios fundamentales que han de aplicarse en concordancia.

La publicidad de las resoluciones judiciales debe realizarse con pleno respeto a la protección de datos personales mediante técnicas de anonimización adecuadas. La divulgación de datos sensibles o de aquellos que puedan afectar derechos legítimos de su titular constituyen excepciones al acceso a la información pública. Sin embargo, ello no implica la no publicación de la resolución judicial que los contiene, sino la publicación tomando los debidos resguardos.

3. Conceptos fundamentales: identificación, anonimización y seudoanonimización

En el ámbito judicial, la protección de datos personales comienza por entender qué significa identificar a una persona. La **identificación** de una persona es posible a partir de un conjunto de datos -como nombre, domicilio, profesión, cargo o incluso detalles circunstanciales- que permiten reconocer directa o indirectamente a quién se refiere la información.

La **anonimización** refiere a la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados[5]. Una vez anonimizada correctamente, la información no se considera dato personal y, por lo tanto, queda fuera del ámbito de aplicación de la Ley n.° 25326 y demás normativa de protección de datos personales.

La Ley n.° 25326, en su artículo 2, define a la disociación de datos como "todo aquel tratamiento donde la información obtenida no pueda asociarse a persona determinada o determinable".

Por su parte, la Unión Europea, a través del Reglamento General de Protección de Datos (RGPD), en el Considerando 26, señala que los datos anónimos constituyen aquella información que *"no se refiere a una persona física identificada o identificable o a datos personales convertidos en anónimos de tal forma que el interesado no sea o ya no sea identificable"*.[6]

Por el contrario, la **seudo-anonimización** implica reemplazar los identificadores directos -como el nombre, documento, correo electrónico- por otros elementos -iniciales, códigos, seudónimos-, conservando así la posibilidad de revertir el proceso

[5] Organización de los Estados Americanos. (2021). Principios actualizados sobre la privacidad y la protección de datos personales.

[6] Unión Europea. (2016). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

bajo ciertas condiciones. A diferencia de la anonimización, la seudoanonimización no elimina el carácter de dato personal, por lo que el conjunto resultante sigue estando sujeto a la Ley n.° 25326 y requiere salvaguardas específicas. Por eso, es útil para trabajo interno o análisis técnico, pero no equivale a una anonimización completa y siempre está la posibilidad de reidentificar los datos personales.

3.1. Aplicación en el contexto judicial

Esta Guía se enfoca exclusivamente en la anonimización de los documentos judiciales que serán incorporados al sistema Jurisemia. No se trata de anonimizar el expediente completo, que debe conservarse íntegro en el juzgado correspondiente. El proceso de anonimización aplica únicamente a la versión pública de las resoluciones judiciales, es decir, aquella destinada a alimentar los sistemas de búsqueda y análisis de jurisprudencia.

La aplicación de este enfoque permite garantizar:

- La protección de datos que requieren protección de las personas involucradas;
- La preservación del valor jurídico y probatorio del expediente original;
- La confianza ciudadana en el uso ético y responsable de la inteligencia artificial en el Poder Judicial.

4. Protección de datos

4.1. Marco Normativo

La anonimización de los documentos judiciales que se publican en el sistema Jurisemia permite proteger la privacidad y los derechos de las personas involucradas y posibilita al Poder Judicial alinearse con los estándares internacionales más avanzados en protección de datos.

Este enfoque asegura que la publicación de las resoluciones cumpla con los más altos estándares de ética, legalidad y responsabilidad institucional, fortaleciendo la confianza de la ciudadanía en el uso de tecnologías como la inteligencia artificial para la búsqueda y análisis de jurisprudencia.

Por estas razones, el presente documento se basa en un conjunto de normativa y recomendaciones internacionales y nacionales, seleccionadas cuidadosamente para garantizar que los procedimientos de anonimización estén a la vanguardia y sean plenamente confiables.

4.1.1. A nivel internacional

- El Convenio 108 del Consejo de Europa y Protocolo modificatorio (Convenio 108+) (2018). Este protocolo establece medidas específicas para la protección de las personas frente al tratamiento automatizado de datos de carácter

personal[7]. En Argentina, el Convenio 108 fue incorporado a la legislación mediante la Ley n.° 27483 (2019), por lo que es jurídicamente aplicable y obligatorio en el país, asegurando que los procedimientos de anonimización cumplan con normas internacionales. Asimismo, el Protocolo modificatorio, Convenio 108+, fue ratificado por la Ley n.°27699 (2022).

- El Reglamento General de Protección de Datos (RGPD) de la Unión Europea (2016). Representa el estándar más avanzado y reconocido internacionalmente en materia de protección de datos personales. Sus principios y obligaciones han servido de guía para adaptar prácticas de anonimización que minimicen riesgos de reidentificación[8].
- La Recomendación sobre la ética de la inteligencia artificial. Es el primer marco normativo universal sobre ética de la IA, remarca la importancia de proteger los datos personales en contextos de inteligencia artificial[9]. El Estado argentino adoptó esta recomendación y, en 2023, la Subsecretaría de Tecnologías de la Información emitió la Disposición 2/23, que toma como base directa dicho instrumento.
- El Kit de herramientas global sobre IA y el estado de derecho para el poder judicial (2023). Que subraya la importancia de la protección de datos y la ética en el uso de sistemas automatizados para el análisis de información judicial[10].

4.1.2. A nivel regional

- La Red Iberoamericana de Protección de Datos (RIPD) cuenta con los Estándares Iberoamericanos de Protección de Datos (2017). Sus recomendaciones facilitan la armonización de políticas y prácticas de anonimización entre países iberoamericanos, promoviendo buenas prácticas compartidas y consistentes con la normativa internacional. La Red prevé su actualización para 2026[11].
- Las “Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial” de la RIPD. Establecen orientaciones para que el desarrollo y uso de sistemas de inteligencia artificial se realice de manera respetuosa con los derechos fundamentales y la normativa de protección de datos personales[12].
- Las Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial. Ofrecen pautas concretas para garantizar que el desarrollo y uso de sistemas de inteligencia artificial respeten los principios fundamentales de protección de datos. Busca ayudar a responsables y encargados del tratamiento a aplicar, en la práctica, derechos como la licitud, transparencia, minimización, exactitud, limitación de finalidad y responsabilidad proactiva.

[7] Consejo de Europa (2018). Convenio 108+: Convenio para la protección de las personas con respecto al tratamiento de datos personales.
[8] Unión Europea. (2016). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
[9] UNESCO. (2021). Recomendación sobre la ética de la inteligencia artificial.
[10] UNESCO. (2023). Kit de herramientas global sobre IA y el estado de derecho para el poder judicial.
[11] Red Iberoamericana de Protección de Datos. (2017). Estándares iberoamericanos de protección de datos.
[12] Red Iberoamericana de Protección de Datos. (2019). Recomendaciones generales para el tratamiento de datos en la inteligencia artificial.

Asimismo, promueve la adopción de medidas éticas, técnicas y organizativas que aseguren que los proyectos de IA sean confiables, justos y centrados en las personas[13].

- Las Reglas de Heredia. Son un conjunto de recomendaciones aprobadas en el año 2003 por poderes judiciales latinoamericanos, organizaciones de la sociedad civil y especialistas, para orientar la publicación de información judicial en formatos digitales. Su objetivo es ofrecer un modelo común para garantizar la transparencia judicial sin vulnerar la privacidad de las personas involucradas en los procesos. Proponen criterios para el tratamiento y la disociación de datos personales en sentencias y expedientes difundidos en Internet. Se aplican únicamente a la divulgación electrónica de resoluciones y datos procesales. En Argentina fueron incorporadas al derecho interno mediante la Resolución 12/2010 de la Dirección Nacional de Protección de Datos Personales[14].
- Los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la OEA (2021). Establecen estándares regionales para garantizar un tratamiento legítimo, transparente y seguro de los datos personales. Refuerzan derechos como acceso, rectificación, supresión y portabilidad, y promueven obligaciones de responsabilidad proactiva para quienes tratan datos[15].

4.1.3. A nivel nacional

- La Ley n.° 25326 de Protección de Datos Personales (2000)[16]. Establece el marco general para el tratamiento de datos personales e impone obligaciones específicas cuando dicho tratamiento se lleva a cabo en el ámbito del sector público. En particular, el artículo 4 de la citada ley consagra los principios de legalidad, finalidad, pertinencia, proporcionalidad y exactitud que deben regir el tratamiento y el artículo 9 exige la adopción de medidas técnicas y organizativas adecuadas para garantizar la seguridad y confidencialidad de los datos.
- La Resolución 4/2019. Incluye criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley n.° 25326, referidos a sistemas de video vigilancia, tratamiento automatizado de datos, disociación de datos, consentimiento y otros[17].
- La Resolución 161/2023. Crea el “Programa de Transparencia y Protección de Datos Personales en el uso de la Inteligencia Artificial”, que impulsa procesos de análisis, regulación y fortalecimiento de capacidades estatales necesarias para acompañar el desarrollo y uso de la inteligencia artificial, tanto en el sector público como en el ámbito privado[18].

[13] Red Iberoamericana de Protección de Datos. (2019). Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de inteligencia artificial.
[14] Reglas de Heredia. (2003). Reglas de Heredia sobre difusión de información judicial en Internet
[15] Organización de los Estados Americanos. (2021). Principios actualizados sobre la privacidad y la protección de datos personales.
[16] Ley 25326. (2000). Protección de los datos personales. Argentina.
[17] Agencia de Acceso a la Información Pública. (2018). Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley n.° 25326 (Anexo I de la Disposición 60/2018).
[18] Agencia de Acceso a la Información Pública. (2023). Programa de transparencia y protección de datos personales en el uso de la inteligencia artificial (Resolución 161/2023).

- La Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable (2024). Proporciona lineamientos detallados sobre cómo las organizaciones pueden integrar la transparencia y la protección de datos personales en el ciclo de vida de los sistemas de IA[19].
- La Disposición 12/2010 de la Dirección Nacional de Protección de Datos Personales, emitida por la Agencia de Acceso a la Información Pública (AAIP). Establece criterios fundamentales para el tratamiento de datos personales en el ámbito judicial, especialmente relevante para la anonimización de documentos judiciales que serán incorporados a sistemas de jurisprudencia impulsados por inteligencia artificial, incorporando explícitamente las *Reglas de Heredia* como referencia para la difusión de información judicial en Internet[20].

4.1.4. Normativa interna del Poder Judicial

- Acuerdo n.° 7 (2010) del Tribunal Superior de Justicia (TSJ). Por intermedio de la Sala Penal, establece directrices para la protección de la identidad de Niños, Niñas y adolescentes que se mencionan en las resoluciones judiciales[21].
- Acuerdo Reglamentario n.°1850, Serie “A” (2024), del Tribunal Superior de Justicia (TSJ). Reconoce que la inicialización completa de los datos personales de los Niños, Niñas y Adolescentes y de sus familiares en las resoluciones judiciales podría generar dificultades en la legibilidad de las resoluciones y, a partir de ello, dispone la forma en que deberán inicializarse los datos personales de aquellos[22].

La lectura comprensiva de estos instrumentos permite que el Poder Judicial de Córdoba adopte estándares de protección de datos y anonimización alineados con la vanguardia internacional, asegurando la privacidad de las personas y la confianza pública en el uso de inteligencia artificial para la jurisprudencia.

4.2. Principios y obligaciones de la anonimización judicial

En el ámbito judicial, la anonimización consiste en el proceso técnico y normativo mediante el cual se eliminan o transforman los datos personales identificatorios de documentos judiciales, con el fin de garantizar la protección de la privacidad de las personas y el cumplimiento de las obligaciones en materia de protección de datos personales, sin afectar la transparencia, la publicidad y la coherencia de los actos judiciales. En el contexto del uso de inteligencia artificial (IA), la anonimización adquiere una relevancia particular al integrarse en sistemas automatizados de gestión, búsqueda y publicación de sentencias.

[19] Agencia de Acceso a la Información Pública. (2024). Guía para entidades públicas y privadas en materia de transparencia y protección de datos personales para una inteligencia artificial responsable.
[20] Dirección Nacional de Protección de Datos Personales. (2010). Disposición 12/2010.
[21] Tribunal Superior de Justicia de Córdoba. (2010). Acuerdo n.° 7. Poder Judicial de la Provincia de Córdoba.
[22] Tribunal Superior de Justicia de Córdoba. (2024). Acuerdo Reglamentario Serie “A” n.° 1850. Poder Judicial de la Provincia de Córdoba.

Los siguientes principios orientan la anonimización de los documentos a publicar en el sistema Jurisemia. Operan de manera integrada y complementaria en todo proceso de anonimización judicial. No constituyen compartimentos estancos, sino que deben aplicarse simultáneamente para garantizar un equilibrio entre transparencia y protección de datos personales.

4.2.1. Principio de legalidad

El tratamiento de los datos personales en el ámbito judicial debe realizarse conforme al marco legal dado por la Ley n.° 25326 y demás normas reglamentarias, basándose en una norma jurídica que lo autorice. El artículo 5, inciso b), de la Ley n.° 25326 establece que el tratamiento de datos personales puede realizarse sin el consentimiento del titular cuando resulte necesario para el ejercicio de las funciones propias de los poderes del Estado. Esta disposición constituye una base de legitimación sólida, que habilita a los organismos públicos -incluido el Poder Judicial de Córdoba- a intervenir sobre la información que gestionan siempre que ello responda a sus competencias legales.

La sistematización y publicación de sentencias, autos y demás resoluciones judiciales persigue fines constitucional y legalmente reconocidos: asegurar la transparencia, garantizar el acceso a la justicia y consolidar la seguridad jurídica. En virtud de ello, el Tribunal Superior de Justicia, a través del Boletín Judicial y con un criterio democrático, busca garantizar dichos principios mediante la implementación gradual del sistema Jurisemia. El tratamiento de estos datos por parte del Boletín Judicial se enmarcan dentro de las facultades y capacidades otorgadas a esta oficina por la normativa reglamentaria específica[23], que configura un entramado jurídico institucional que respalda el tratamiento y la difusión de jurisprudencia dentro del ámbito del Poder Judicial de Córdoba, en cumplimiento de sus funciones.

4.2.2. Principio de finalidad y de minimización

El artículo 4, inciso 3), de la Ley n.° 25326, dispone que el tratamiento de datos anonimizados debe regirse, en primer lugar, por el principio de *finalidad*: la información solo puede utilizarse para fines compatibles con los objetivos originales que justificaron su recopilación. Por supuesto, una vez anonimizado, el dato personal deja de estar sujeto a la legislación sobre protección de datos. Sin embargo, la anonimización no convierte la información en un recurso libre de responsabilidades; su propósito es reducir riesgos y proteger derechos, manteniendo la coherencia con la finalidad que motivó su tratamiento.

[23] Ley n.° 8435 Orgánica del Poder Judicial; Decreto Ley n.° 7212-A del Tribunal Superior de Justicia (TSJ); Acuerdo Reglamentario n.° 608, Serie “A”, del 12/6/2001; Acuerdo Reglamentario n.° 95, Serie “B”, del 28/8/2012; que crea el Consejo Consultivo del Boletín Judicial. El Acuerdo Reglamentario 1673, Serie A, que modifica el AR n.° 95. La resolución sobre el Redactor Jurisprudencial *ad honorem* del Boletín Judicial (AR 95, Serie B, 28/8/2012). La resolución sobre el Supervisor de Redactores Jurisprudenciales ad honorem (Acuerdo N.º 1, Serie B del 11/2/2014). El Acuerdo N.° 577, Serie A del 26/7/2019, que establece la dependencia orgánica directa del Boletín Judicial del TSJ como Área de Apoyo. El Acuerdo Reglamentario 608, Serie A del 12/6/2001, sobre la remisión de jurisprudencia al Boletín Judicial.

En este contexto, la finalidad del tratamiento de los documentos judiciales que contienen los datos anonimizados se limita estrictamente al desarrollo, funcionamiento y mejora del sistema de búsqueda de Jurisemia, en armonía con la misión institucional del Boletín Judicial de garantizar la publicidad y la transparencia de las decisiones judiciales. Ello, teniendo en cuenta que la finalidad de la difusión en internet de las resoluciones judiciales es el conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley para procurar alcanzar la transparencia en la administración de justicia[24].

A su vez, el proceso de anonimización debe ajustarse al principio de *minimización*, lo que implica recolectar, conservar y tratar únicamente los datos estrictamente necesarios para cumplir la finalidad definida. Este principio debe aplicarse de manera uniforme tanto antes de la anonimización como después de ella, evitando incorporar o retener información que exceda el propósito del tratamiento.

Finalmente, la aplicación conjunta de estos principios exige que la protección de datos en las resoluciones judiciales no se realice de manera indiscriminada. Solo se deben anonimizar aquellos datos que revelen información especialmente sensible o de especial protección cuya divulgación pueda generar riesgos concretos. En todos los casos, la anonimización debe realizarse mediante una evaluación cuidadosa que asegure que el precedente judicial conserve la claridad de sus fundamentos y la inteligibilidad del resultado alcanzado.

4.2.3. Principio de transparencia

Los proyectos de anonimización inteligente se inscriben en una visión de justicia abierta, centrada en la gestión responsable de los datos, la transparencia activa y la promoción de políticas judiciales orientadas al ciudadano. La transparencia en los portales de publicación de jurisprudencia, como Jurisemia, alude a la posibilidad de que los usuarios accedan a información judicial de manera clara, confiable y verificable. Esto supone no solo que las resoluciones estén disponibles públicamente, sino también que cada fallo incluya los datos necesarios para asegurar su correcta trazabilidad y citación -tribunal interviniente, tipo y n.° de resolución y fecha de su dictado- permitiendo así reconstruir su origen y seguir la evolución jurisprudencial de un tema determinado. Este estándar se garantiza obteniendo las resoluciones oficiales provenientes del Sistema de Administración de Causas (SAC), asegurando la integridad del flujo entre la fuente institucional y el documento publicado.

Asimismo, la transparencia abarca la claridad en los criterios de publicación, lo que implica no solo detallar la fuente oficial de la que emana cada resolución, sino también explicar qué tipo de jurisprudencia se difunde y por qué, evitando decisiones arbitrarias en la selección de casos y permitiendo que los usuarios comprendan el alcance y la representatividad de la información disponible. Estos criterios de publicación se vinculan con la difusión de resoluciones novedosas, relevantes o de interés general, especialmente aquellas que involucran interés público, incorporan

[24] Podestá, F. (2010). Tratamiento de datos personales en la Justicia digital: Panorama argentino y otras referencias [Ponencia]. Seminario Regional de Protección de Datos, Montevideo, Uruguay, 1-4 de junio de 2010. Red Iberoamericana de Protección de Datos. Recuperado de https://www.redipd.org/sites/default/files/2020-01/Tratamiento_DP_en_PJ_F_Podesta.pdf

nueva doctrina judicial o reflejan una modificación en la línea jurisprudencial sobre una cuestión determinada.

4.2.4. Principio de proporcionalidad

La publicidad de las decisiones judiciales garantiza el control ciudadano, la rendición de cuentas y la confianza en la justicia; sin embargo, esta apertura no puede vulnerar los derechos de las personas involucradas en los fallos judiciales. Para lograr ese equilibrio, es necesario que las medidas de anonimización apliquen el criterio de proporcionalidad, de modo que se difunda la información necesaria para garantizar la transparencia institucional sin exponer información personal sensible.

A efectos de evaluar si las medidas de anonimización de los datos personales son adecuadas y proporcionales al fin perseguido, deben considerarse diversos criterios jurídicos, contextuales y técnicos que se abordan en los distintos apartados de la presente Guía. En la publicación de las resoluciones judiciales, el principio de proporcionalidad implica anonimizar únicamente aquellos datos cuya supresión resulte estrictamente necesaria para resguardar la identidad o la intimidad de las personas, sin menoscabar el contenido jurídico o el valor informativo del fallo. Las técnicas empleadas no deben ser tan restrictivas que vuelvan inservible la información ni tan laxas que comprometan la privacidad; por el contrario, deben asegurar un equilibrio que preserve simultáneamente la protección de datos y la publicidad de la decisión judicial.

Ejemplo de incumplimiento del principio de proporcionalidad

Un tribunal dicta sentencia sobre un conflicto entre una empresa y un trabajador que sufrió incapacidad por un accidente laboral. Para “proteger los datos personales” del trabajador, se decide eliminar no solo los nombres de las partes, sino también el monto del reclamo, el porcentaje de incapacidad, las dolencias padecidas, la fecha de los hechos y toda referencia contextual, dejando un texto casi imposible de interpretar:

“La parte actora (*dato suprimido*) demandó a su empleadora (*dato suprimido*) reclamando la suma (*dato suprimido*) en concepto de indemnización por incapacidad laboral (*dato suprimido*) con motivo del accidente de trabajo ocurrido el día (*dato suprimido*), conforme a la normativa prevista (*dato suprimido*)”

En este caso la anonimización resulta excesiva: se eliminaron datos que no permiten identificar directamente a las personas, pero que sí son necesarios para comprender el contenido de la sentencia, evaluar el criterio del tribunal y permitir su estudio. El exceso de supresiones puede romper el equilibrio entre protección de datos y acceso a información pública de calidad.

Propuesta superadora que respeta el principio de proporcionalidad

“La parte actora (identificada como “trabajador”) demandó a su empleadora Talar SRL, reclamando la suma de ocho millones de pesos en concepto de indemnización por incapacidad laboral del 23% por las secuelas sufridas con motivo del accidente de trabajo ocurrido el día 25/4/2020, conforme a la normativa prevista en la Ley de Contrato de Trabajo”.

4.2.5. Rendición de cuentas

El principio de rendición de cuentas implica que los responsables no solo deben cumplir las normas de protección de datos, sino poder demostrar activamente que las cumplen. En la publicación de resoluciones judiciales, ello supone que se debe poder acreditar que: i) se aplicaron medidas de anonimización adecuadas, ii) se realizó una evaluación de adecuación y proporcionalidad, iii) se conserva un registro del proceso que garantice su trazabilidad, y iv) se adoptaron todas las medidas necesarias para que el personal interviniente (especialmente, los gestores de carga y los supervisores) reciba capacitación en buenas prácticas de protección de datos.

Esta obligación se encuentra presente en la normativa, las legislaciones modernas y los estándares internacionales referidos en esta Guía, siendo clave para garantizar que quienes tratan información personal asuman una responsabilidad activa en el cumplimiento de las normas y buenas prácticas en materia de privacidad. Estas medidas, que permiten la rendición de cuentas, no se limitan a cumplir formalmente con la ley, sino que demuestran de manera transparente las acciones adoptadas para proteger los datos, prevenir riesgos y responder ante eventuales incidentes.

Este enfoque refuerza la confianza de los titulares de los datos y de la sociedad en general, al evidenciar que la organización no solo actúa conforme a las obligaciones legales, sino que también promueve una cultura de respeto, transparencia y mejora continua en la gestión de la información personal.

4.2.6. Seguridad y confidencialidad

Las medidas de seguridad y confidencialidad en la protección de datos personales comprenden el conjunto de acciones técnicas, organizativas y administrativas destinadas a preservar la integridad, disponibilidad y privacidad de la información. Estas medidas buscan evitar accesos no autorizados, alteraciones, pérdidas o tratamientos indebidos de los datos, e incluyen desde controles de acceso, cifrado y copias de respaldo, hasta políticas internas de gestión, capacitación del personal y cláusulas de confidencialidad. Su aplicación debe ser proporcional al tipo de datos tratados y al nivel de riesgo asociado, asegurando que toda persona o entidad que intervenga en el tratamiento actúe bajo estrictas obligaciones de reserva y responsabilidad. De este modo, se garantiza que la información personal se maneje de forma segura y conforme a los principios fundamentales de la protección de datos.

Este principio refuerza la necesidad de que cuando la anonimización se practique mediante sistemas de inteligencia artificial, estos operen sobre infraestructuras seguras y aisladas, aplicando medidas como el uso de conexiones cifradas y entornos protegidos, garantizando la imposibilidad de lectura o acceso indebido a los datos.

4.2.7. Supervisión humana

Las nuevas tecnologías han permitido la incorporación de componentes automatizados en la tarea de anonimización de las resoluciones judiciales, lo que permite acelerar las cargas, aumentar la eficiencia, reducir los errores manuales y escalar las operaciones de forma más eficaz. No obstante, la anonimización automatizada no debe reemplazar la intervención humana, sino complementarla.

El control humano en la validación y entrenamiento de los modelos es un requisito esencial para asegurar el criterio contextual y evitar errores o sesgos en el proceso. Un programa automatizado de anonimización puede equivocarse al no identificar ciertos datos sensibles (por ejemplo, referencias indirectas que permitan reconocer a una persona) o al eliminar información relevante para la comprensión jurídica de un fallo. Por ese motivo, la revisión humana resulta indispensable para verificar los resultados del proceso automatizado, corregir errores, evaluar el riesgo de reidentificación y asegurar que la anonimización mantenga el equilibrio entre la protección de la privacidad y la publicidad de la información judicial.

5. Roles y responsabilidades en el proceso de anonimización

El adecuado cumplimiento de la normativa aplicable en materia de protección de datos requiere el compromiso activo de todo el personal involucrado, trabajando de manera coordinada para alcanzar el estándar deseable de protección de datos. El tratamiento de datos personales en Jurisemia es llevado a cabo por agentes del Poder Judicial de la Provincia de Córdoba, a quienes esta Guía les asigna roles claramente definidos y responsabilidades específicas, especialmente quienes desempeñan los roles asociados a la plataforma Nexo[25] (administradores, supervisores y gestores de carga y testeo).

Es importante que los actores involucrados entiendan que trabajan con activos valiosos que la Ley de Protección de Datos Personales exige sean resguardados, para garantizar la confidencialidad, disponibilidad, seguridad y preservar el derecho a la intimidad y protección de datos de las personas.

Este capítulo expone las buenas prácticas que deben observar los agentes judiciales en el proceso de anonimización. Ello comprende: (i) a los gestores de carga y testeo de las distintas dependencias; (ii) a quiénes desempeñan funciones de supervisión y auditoría en el Boletín Judicial; y (iii) a quienes integran las áreas técnicas del Poder Judicial y son responsables de garantizar la seguridad del sistema, bajo la supervisión del Boletín Judicial.

Para estos actores se establecen pautas de registro de actividad, capacitación continua y protocolos de auditoría, subrayando la existencia de una responsabilidad compartida, aunque diferenciada, a fin de evitar la dilución de obligaciones.

[25] Nexo es la plataforma de gestión documental (interfaz privada de carga) que actúa como puerta de ingreso y control de todo documento que se incorpora a Jurisemia. Permite subir, revisar y publicar resoluciones judiciales mediante un sistema de control diferenciado por roles que garantiza: la trazabilidad de las resoluciones judiciales, la aplicación de criterios institucionales de publicación previamente definidos, la protección de datos personales dentro del sistema, y que solo documentos oficiales, correctamente revisados y anonimizados, puedan ser consultados a través de la interfaz pública de Jurisemia. De este modo, Nexo facilita la auditoría de todo el proceso y asegura que el contenido expuesto al público sea confiable, consistente y respetuoso de la normativa de protección de datos.

En cuanto a las obligaciones legales y responsabilidades a su cargo, los agentes que, por razón de sus tareas, tengan o puedan tener acceso a datos personales deberán observar las siguientes **funciones y deberes**:

- Cumplir con lo dispuesto en la presente Guía, las cláusulas de protección de datos personales y de confidencialidad dispuestas y las restantes medidas organizativas y de seguridad sean de aplicación a Jurisemia.
- Tratar los datos personales a los que tenga acceso, directa o indirectamente, de acuerdo a las instrucciones impartidas.
- Utilizar los datos personales a los que tienen acceso exclusivamente para las tareas que se le hubieren asignado, de acuerdo a su perfil, rol y cargo.
- Guardar el deber de secreto y confidencialidad, respecto a la información que conozca o pueda conocer, con motivo del desempeño de su función, incluso luego de concluida la relación laboral.
- Usar de forma personal e intransferible los mecanismos de identificación y autenticación ante los sistemas de información y permisos de acceso físico y lógico otorgados.
- Notificar a su superior jerárquico inmediato y al Boletín Judicial de todas las incidencias que tenga conocimiento y afecten a datos personales dentro del área de su injerencia.
- Informar si advierte posibles debilidades en las medidas de seguridad de protección de datos implementadas y que estime que ponen en peligro la disponibilidad de los datos, la confidencialidad o integridad de los mismos.
- Remitir inmediatamente al Boletín Judicial cualquier solicitud de ejercicio de derechos conforme lo normado en la Ley n.° 25326 de la que hubiese tomado conocimiento.
- Realizar las capacitaciones previstas para el uso del sistema Jurisemia y demás herramientas creadas para la gestión de su implementación, desarrollo y mejora continua del sistema.

Lo anterior implica que se encuentra **prohibido**:

- Abrir o de cualquier forma acceder a perfiles de otros usuarios y a cualquier soporte que contenga datos personales, cuando no se encuentre autorizado de acuerdo al cargo y el perfil de acceso físico y lógico asignado.
- Intentar saltar los mecanismos y dispositivos de seguridad establecidos para la custodia y protección de la información.
- Intentar acceder a datos, recursos o zonas a los que no se le ha autorizado acceso.
- Utilizar datos personales con fines fraudulentos, desleales o ilícitos.
- Utilizar o tratar los datos personales para otras finalidades que no se ajusten a las tareas y funciones de acuerdo a su cargo.

No obstante, lo expuesto en este capítulo no excluye la obligación que pesa sobre magistrados, funcionarios y demás empleados judiciales de velar, en el ejercicio de sus funciones, por el cumplimiento de la normativa aplicable en materia de protección de datos.

Asimismo, en tanto la interacción en el sistema Jurisemia implica la utilización de la plataforma Nexo los agentes deben observar -además de las medidas señaladas

anteriormente- los lineamientos que se dispongan en los manuales específicos para dicha plataforma.

6. Criterios de protección de datos en resoluciones judiciales

A los efectos de garantizar una aplicación coherente y uniforme de la anonimización en la publicación de resoluciones judiciales, la Guía establece los lineamientos para distinguir la información que requiere un nivel reforzado de protección. Si bien ciertos datos personales pueden publicarse sin anonimización cuando su tratamiento se vincula al ejercicio de funciones estatales (art. 5 inc. b, Ley n.° 25326), este documento delimita expresamente los supuestos en los que corresponde aplicar medidas de protección reforzada. Esto se debe a que la publicidad judicial no autoriza la exposición innecesaria de aspectos íntimos o vulnerables, ni la difusión de información que pueda generar un daño desproporcionado a las personas involucradas.

En este apartado se presentan los lineamientos generales que orientan el tratamiento de los datos presentes en las resoluciones judiciales y se establecen las categorías cuya divulgación exige medidas específicas de resguardo.

6.1. ¿Qué son los datos personales?

Los **datos personales** comprenden toda información que identifique o pueda identificar razonablemente a una persona física de manera directa o indirecta. Esto incluye datos como números de identificación, localización, identificadores en línea o cualquier información vinculada a aspectos físicos, fisiológicos, genéticos, mentales, económicos, culturales o sociales. Puede expresarse en formatos numéricos, alfabéticos, gráficos, fotográficos, acústicos, electrónicos o de cualquier otro tipo. Esta noción excluye la información que no permite, de manera razonable, identificar a una persona en particular [26].

De ahí que, para asegurar la protección de la privacidad sin menoscabar el principio de publicidad judicial, previo a realizar el proceso de anonimización, al gestor de carga y testeo le corresponde evaluar el contenido de la resolución judicial a fin de determinar la presencia de datos que requieran de protección reforzada.

6.2. Categorías especiales de datos personales

La necesidad de proteger una resolución judicial surge cuando su contenido incluye datos personales que, por su carácter, pueden suponer un riesgo para sus titulares. Estas resoluciones requieren un tratamiento especial para evitar la

[26] Organización de los Estados Americanos. (2021). Principios actualizados sobre la privacidad y la protección de datos personales.

identificación o exposición indebida de los interesados y, por consiguiente, la vulneración de sus derechos.

Esta Guía prevé medidas de anonimización obligatoria para las resoluciones que exigen un mayor nivel de resguardo, por contener al menos una de las categorías especiales de datos personales -datos sensibles o datos de personas especialmente protegidas-. La intensidad de las medidas a aplicar se determinará en función del riesgo de identificación, el potencial daño para los titulares de los datos y el impacto que su divulgación puede generar en su vida privada.

Los **datos sensibles** refieren a una categoría que abarca los aspectos más íntimos de las personas físicas. Son aquellos que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información sobre salud personal, vida sexual, orientación sexual, datos genéticos o biométricos y asuntos familiares. Su divulgación no autorizada puede generar discriminación, estigmatización o afectar derechos fundamentales, por lo que requieren medidas reforzadas de protección. La sensibilidad de un dato, no obstante, puede variar según el contexto cultural o temporal, y los riesgos pueden ser insignificantes en algunos casos y críticos en otros.

Los **datos de personas especialmente protegidas** son aquellos que, aun cuando no encuadren formalmente como datos sensibles, requieren protección reforzada en atención a la situación de vulnerabilidad de sus titulares. Esta vulnerabilidad puede fundarse en múltiples factores tales como la edad, condición de salud, situación de exclusión social, entre otros que colocan a la persona en posición de riesgo o desventaja estructural. La revelación de estos datos puede generar daños adicionales, revictimización, estigmatización o discriminación. Su tratamiento exige las mismas medidas reforzadas de resguardo aplicables a los datos sensibles, junto con una mayor diligencia proactiva por parte de quienes intervienen en su identificación y manejo, a fin de garantizar una protección efectiva que prevenga cualquier exposición indebida.

Estas categorías constituyen el marco conceptual utilizado para definir qué información se debe anonimizar en la publicación de resoluciones judiciales, privilegiando siempre la protección de las personas frente al riesgo de identificación y de exposición abusiva.

6.2.1. Identificación precisa de las categorías especiales de datos personales

Sin dejar de considerar las recomendaciones que deben tenerse en cuenta en cada fuero en particular, las categorías obligatorias de anonimización (datos sensibles y datos de personas especialmente protegidas) deben ser aplicadas en todos los fueros judiciales.

Los listados que se presentan a continuación no son excluyentes, sino complementarios con el modelo de matriz de riesgos que se desarrollará más adelante, el cual orientará la evaluación contextual y proporcional que se debe realizar en cada caso en concreto.

Sin perjuicio del marco conceptual descrito, quedan exceptuados aquellos casos en los cuales el interesado expresamente solicite que se consignen sus datos personales, de conformidad a la normativa vigente.[27]

6.2.1.1. Por el tratamiento de datos sensibles

Como se explicó anteriormente, esta categoría de datos abarca supuestos que involucran los aspectos más íntimos de las personas humanas, la asociación de estos datos con su titular concreto y posterior divulgación no autorizada, puede generar discriminación, estigmatización o afectar derechos fundamentales de las personas involucradas. La protección reforzada de los documentos judiciales debe aplicarse cuando se revele información sobre:

- **Origen racial o étnico:** refiere a cualquier dato que permita identificar o inferir la pertenencia de una persona a un grupo racial, étnico, pueblo originario o comunidad indígena. Incluye menciones directas, referencias culturales o lingüísticas, adscripciones comunitarias o cualquier información que pueda revelar dicha pertenencia.

- **Opiniones políticas:** comprende toda manifestación, expresa o implícita, de convicciones políticas de una persona, como, afiliación partidaria, participación en actividades políticas, adhesión a ideologías o a movimientos.

- **Convicciones religiosas, filosóficas o morales:** refiere a las creencias religiosas, prácticas espirituales, así como convicciones de naturaleza filosófica, ética o moral que formen parte de la identidad personal o del modo de vida de una persona.

- **Afiliación sindical:** abarca la pertenencia o vinculación de una persona a sindicatos, asociaciones gremiales o cualquier forma de organización representativa de trabajadores.

- **Información referente a la salud personal:** indica cualquier dato que permita conocer, inferir o revelar el estado de salud físico o mental de una persona, como diagnósticos médicos, resultados de estudios, historias clínicas, tratamientos farmacológicos, internaciones, pericias psiquiátricas o psicológicas, certificaciones de discapacidad, porcentaje de capacidad laboral o cualquier otra información que describa condiciones de salud.

- **Información referente a vida sexual, orientación sexual e identidad de género:** abarca cualquier dato que revele prácticas sexuales, historial o vida sexual de una persona; su orientación sexual (heterosexual, homosexual, bisexual u otra); o su identidad y expresión de género, incluyendo información relativa a procesos de afirmación o adecuación de género.

- **Datos genéticos y biométricos que identifiquen de manera unívoca a una persona:** comprende la información de carácter técnico que permite la

[27] En este sentido, consultar precedente del Tribunal Superior de Justicia de la Provincia de Córdoba, Sala Penal, en autos: “Soria, Jorge Javier psa abuso sexual gravemente ultrajante y abuso sexual con acceso carnal - Recurso de casación”, expediente n.° 10268780, sentencia n.° 362 del 25 de septiembre de 2025.

identificación única de un individuo, ya que se basa en características biológicas inmutables y medibles. Abarca, por una parte, los *datos genéticos*, que son la información hereditaria o adquirida que revela características biológicas únicas, como el ADN y los perfiles genéticos. Por otra parte, incluye los *datos biométricos*, que son la información resultante de un tratamiento técnico específico, relacionada con características físicas, fisiológicas o de comportamiento, que posibilita la identificación unívoca. Esto incluye las huellas dactilares, los patrones de iris, las imágenes faciales procesadas para reconocimiento y la voz sometida a tratamiento técnico con fines de identificación.

- **Asuntos familiares**[28]: abarca todos los datos que revelan información sobre el entorno familiar, sus vínculos relacionales o la situación personal íntima de sus integrantes. Incluye datos sobre: dinámicas familiares internos (relaciones de afecto, desafecto, dependencia o conflicto); vínculos de parentesco, filiación, matrimonios, divorcios y uniones convivenciales; problemas privados o la reserva espiritual de los integrantes del grupo familiar; y/o cualquier otra información que, por su naturaleza, se encuentre ligada a la intimidad y dignidad de las personas en el contexto de la vida familiar.

6.2.1.2. Por el tratamiento de datos de personas especialmente protegidas

En estos casos, los documentos judiciales deben someterse a las mismas medidas reforzadas de resguardo aplicables a los casos que contienen datos sensibles, debido a que sus titulares son personas que merecen una especial protección dada la vulnerabilidad que revisten. Esta categoría incluye, de forma no exhaustiva, a personas que requieren una tutela reforzada de sus derechos fundamentales.

La protección reforzada se aplica a datos que identifiquen o que permitan identificar a:

- **Niños, Niñas y Adolescentes** (NNyA) que sean menores de 18 años, aun cuando no adquieran el carácter de parte en el proceso principal.
- **Personas víctimas de violencia de género**: involucra toda información que identifique a personas que han sufrido violencia de género en cualquiera de sus modalidades, para evitar su revictimización.
- **Adultos mayores que requieren especial protección** debido a su dependencia, fragilidad o especiales dificultades que limitan su autonomía o capacidad de defensa de sus derechos.
- **Testigos, denunciantes o terceros** intervinientes en el proceso, cuya divulgación pueda comprometer su seguridad física o psíquica o exponerlos a situaciones de estigmatización, discriminación o exclusión social.
- **Personas con discapacidad** física, sensorial, intelectual o mental.

[28] Este supuesto de protección como dato sensible, se encuentra previsto en la Regla de Heredia para la Difusión de Información Judicial en Internet, Regla n.° 5.

- **Personas afectadas por enfermedades graves o terminales** (incluye condiciones crónicas que impliquen dependencia o riesgo de exclusión social o laboral).
- **Personas pertenecientes a pueblos indígenas, comunidades originarias o minorías étnicas y culturales.**
- **Personas discriminadas por orientación sexual, identidad o expresión de género u otras características que las coloquen en situación de vulnerabilidad.**
- **Personas en situación de extrema pobreza o exclusión social** cuya desventaja económica y social limita su acceso a derechos y aumenta el riesgo ante el mal uso de sus datos.
- **Personas afectadas por barreras de comunicación** (incluye el analfabetismo, baja escolaridad o la existencia de barreras lingüísticas o comunicacionales que dificultan la comprensión de sus derechos y el ejercicio de su consentimiento).
- **Personas cuya situación de vulnerabilidad se revele tras la aplicación de la perspectiva de género** en la resolución judicial, evidenciando dinámicas de desigualdad, asimetría y/o abuso de poder, discriminación o violencia.

6.3. Datos que requieren anonimización

Cuando se verifica alguna de las causales de protección -presencia de datos sensibles y/o datos de personas especialmente protegidas-, corresponde aplicar medidas de anonimización orientadas a impedir la vinculación de esa información con una persona determinada. En el ámbito de las resoluciones judiciales, esto no implica suprimir el dato sensible ni el contenido relevante del fallo -que en la mayoría de los casos forma parte del razonamiento jurídico-, sino anonimizar al titular de los datos y los indicadores directos e indirectos que permitan su identificación.

Para determinar qué información se debe anonimizar en un documento judicial, resulta esencial identificar y evaluar en cada caso los indicadores que permitan reconocer, directa o indirectamente, a los sujetos de protección. Estos datos se clasifican en dos categorías: a) **Indicadores directos**: son atributos exclusivos y se pueden usar como datos clave para volver a identificar a un individuo, es decir, permiten vincular inmediatamente la información con una persona determinada (como el nombre, apellido, número de DNI, etc.); y b) **Indicadores indirectos**: son atributos que no individualizan por sí solos, ya que no son exclusivos de un individuo, pero pueden identificarlo cuando se combinan con otra información u elementos que surgen del contexto del caso (por ejemplo: una combinación de la edad, género y código postal)[29].

Detectar y evaluar ambos tipos de identificadores resulta esencial para aplicar el proceso de anonimización adecuado que preserve la inteligibilidad jurídica del

[29] Agencia Española de Protección de Datos. (2022). Guía básica de anonimización.

precedente sin comprometer la identidad ni la privacidad de quienes intervienen. Para ello, deben considerarse también los criterios y particularidades propios de cada fuero.

A continuación, se expone una lista ejemplificativa de indicadores directos e indirectos detectados en el ámbito judicial:

- Nombres, apellidos y apodos de personas sujetas a protección.
- Números de DNI, pasaporte, LE, CUIT, CUIL.
- Datos de identificación digital: correos electrónicos, usuarios de redes sociales, direcciones IP, URL de perfiles, números de teléfono.
- Número o código de cuenta bancaria (alias, CBU, CVU).
- Número de legajo laboral.
- Carátula y número del expediente.
- Edad.
- Género.
- Carrera, profesión, posición laboral (ej. gerente).
- Fecha de nacimiento, tomo, año de inscripción, número de certificado de nacimiento.
- Direcciones. Domicilios que requieran protección especial, por ejemplo, los relacionados con testigos o víctimas cuando su difusión pueda exponerlos a represalias, acoso o revictimización. Incluyendo calles, numeración, pisos, departamentos o nombres de edificios o complejos habitacionales pequeños.
- Código postal.
- Nombre de la empresa, nombres de escuelas, hospitales u otros establecimientos, cuando su mención pueda permitir la identificación de la persona protegida.
- Números de historias clínicas.
- Estado civil.
- Descripciones físicas (ej. cicatrices, tatuajes, altura, peso) y rasgos distintivos que permitan individualizar a la persona protegida.
- Identificadores de bienes registrables. Números de matrículas de vehículos, patentes, dominios o matrículas de bienes muebles e inmuebles cuando se vinculen directamente con personas cuya identidad se protege. En casos específicos (por ejemplo, en un abuso sexual cometido dentro de un vehículo), también será necesario anonimizar elementos como marca, modelo o color si ello contribuye a la identificación.
- Localización (coordenadas) del Sistema de Posicionamiento Global (GPS).

- Localidades, ciudades, municipios, provincias, barrios que por su baja población o por la notoriedad del caso permitan individualizar a la persona protegida.

- Datos de personas jurídicas cuando, por sí solos o en combinación con otros elementos, permitan identificar a personas humanas especialmente protegidas o cuyos datos sensibles se ventilen en la causa. Por ejemplo: “Fernando Gómez y Hnos. SRL”.

**Aclaración importante*: Este listado de indicadores directos e indirectos de identificación dependerá del fuero específico en el que se apliquen y del contexto del caso. Corresponde aplicar el principio de proporcionalidad a fin de armonizar la protección y evitar la identificación del sujeto a proteger.

6.4. Datos de las resoluciones judiciales que no requieren anonimización

La publicación de resoluciones judiciales requiere un equilibrio entre la protección de datos personales y la preservación del valor público, jurídico e institucional del fallo. En este sentido, existen categorías de información que, por su naturaleza, no identifican a personas físicas protegidas o bien constituyen datos públicos necesarios para comprender la decisión judicial y por lo tanto no deben ser anonimizadas.

El listado que se presenta a continuación es enunciativo y no taxativo. Se trata de elementos estructurales propios de las resoluciones, imprescindibles para garantizar la transparencia del sistema de justicia, la publicidad de los actos judiciales, el control ciudadano y el valor jurisprudencial de las decisiones. Estos datos mantienen su carácter público siempre que no permitan, por sí solos o en combinación con otros elementos, identificar a personas vulnerables o revelar información sensible (es decir, que no exista riesgo de identificación).

A continuación, se detallan los **datos que deben mantenerse visibles** en la publicación de resoluciones:

- Nombres de tribunales, juzgados o cámaras: por ejemplo: “Cámara de Apelaciones en lo Civil y Comercial Segunda Nominación, de la ciudad de Córdoba”; Juzgado de Control, Niñez, Adolescencia, Penal Juvenil, Violencia Familiar, de Género y Faltas de la ciudad de Deán Funes.

- Fecha de la sentencia, número y lugar donde se dictó la resolución.

- Datos de protocolización.

- Cargos públicos o funciones oficiales, cuando el dato es de interés público o se refiere al ejercicio de la función. Por ejemplo: “El Ministro de Salud, Sr. Juan Paz, dictó la resolución…”.

- Fundamentos jurídicos, citas legales, doctrina y jurisprudencia[30]: deben mantenerse intactos para asegurar el valor pedagógico, científico y normativo de la sentencia.
- Datos de personas jurídicas. Tales como la razón social de empresas, asociaciones u organismos públicos, n.° de inscripción en IPJ, fecha de constitución, etc. Por ejemplo: “Banco de la Nación Argentina”.
- Datos de personas que han alcanzado voluntariamente el carácter de pública y el proceso está relacionado con las razones de su notoriedad[31].
- Datos de profesionales intervinientes en función pública o profesional: Por ejemplo: nombres de jueces, fiscales, camaristas, defensores, secretarios o abogados, cuando su actuación es parte del proceso judicial.
- Montos económicos mencionados en la resolución: costas, indemnizaciones, regulaciones, cuotas, intereses, multas y formas de pago.
- Identificación de profesionales auxiliares (peritos, traductores, licenciados/as, jurados populares, etc.), cuando actúan en carácter público o institucional.

6.5. Anonimización en supuestos no previstos

Existen documentos judiciales que refieren a situaciones que no encuadran en las categorías especiales de datos personales previstas en esta Guía, pero que, por sus particularidades, pueden requerir un tratamiento de protección. En estos casos, al gestor de carga y testeo le corresponde evaluar, aplicando el principio de proporcionalidad, si la difusión del contenido podría causar exposición indebida o daño a los involucrados, aun cuando el supuesto no se encuentre expresamente contemplado en las reglas anteriores. Se trata, por ejemplo, de casos de alto interés público, mediático o situaciones que afecten de modo significativo la vida privada de las personas.

En tales casos, el principio de proporcionalidad cumple un rol central: permite determinar si la anonimización es necesaria y, en su caso, definir el alcance y el modo adecuado de implementarla para asegurar una protección suficiente de la privacidad.

[30] Salvo cuando de la cita jurisprudencial se pueda determinar que se trata de una causa que pueda contener información sensible o se traten personas especialmente protegidas (ej. “Juan Pérez - Denuncia por Violencia familiar”, etc.), se deberá anonimizar la carátula del expediente, dejando solo tribunal, tipo y n.° de resolución y fecha de su dictado.

[31] Las Reglas de Heredia para la Difusión de Información Judicial en Internet, en su Regla n.° 6, que refiere a la transparencia y el acceso a la información pública en el ámbito judicial, dispone que prevalece el interés público si la persona involucrada ha alcanzado voluntariamente un carácter público, siempre que el proceso esté relacionado con las razones de su notoriedad. El concepto de *personas voluntariamente públicas* refiere a funcionarios públicos (cargos electivos o jerárquicos) o particulares que se hayan involucrado voluntariamente en asuntos de interés público (en este caso se estima necesaria una manifestación clara de renuncia a un área determinada de su intimidad). Sin embargo, se encuentran excluidas las cuestiones de familia o aquellas en las que exista una protección legal específica.

6.6. Procedimiento para la detección de categorías especiales de datos personales

Para iniciar el proceso de anonimización, al gestor de carga y testeo le corresponde efectuar una serie de pasos secuenciales orientados a la detección de las categorías especiales de datos personales que requieren protección reforzada. Este procedimiento constituye el primer nivel de revisión dentro del control escalonado por roles que implementa Nexo (punto 8 de esta Guía). Su correcta ejecución resulta indispensable para que, en la instancia posterior, el supervisor pueda ejercer una revisión efectiva de las decisiones de anonimización adoptadas. En cada paso, al gestor le corresponde adoptar las medidas de protección que se ajusten al caso bajo análisis, respetando el principio de proporcionalidad.

6.6.1. Primer paso. Control de la necesidad de anonimización

El proceso se inicia con la evaluación del contenido de la resolución, la cual permite identificar y clasificar qué fallos se encuadran dentro de las categorías especiales de datos personales y, por ende, requieren anonimización. En esta instancia, se deben distinguir las resoluciones que no requieren protección, por no encuadrarse en las categorías previstas en esta Guía, de aquellas que sí la requieren por implicar riesgos significativos para los derechos de las personas involucradas.[32]

6.6.2. Segundo paso. Control de proporcionalidad

En los casos donde la resolución requiere protección, el segundo paso consiste en clasificar la información que aquella contiene para determinar qué datos específicos deben ser anonimizados. En este punto, el gestor de carga y testeo, aplicando el principio de proporcionalidad, le corresponde distinguir entre los *datos a anonimizar*[33] (por tratarse de información que implica un riesgo real de identificación para el titular de los datos de categorías especiales) y los datos que pueden *mantenerse visibles* (por ser información que debe mantenerse pública debido a su relevancia jurídica o porque no permite vincular el documento directamente con una persona específica, asegurando así la transparencia de la función judicial).

Detectar y evaluar los datos mencionados resulta esencial para aplicar el proceso de anonimización adecuado, a fin de preservar la inteligibilidad jurídica del precedente sin comprometer la identidad ni la privacidad de quienes intervienen.

6.6.3. Tercer paso. Anonimización del titular de los datos

Una vez identificada la necesidad de protección (primer paso) y determinados los datos directos e indirectos específicos que deben ser objeto de tratamiento (segundo paso), el tercer paso consiste en materializar la protección mediante la anonimización

[32] El primer paso de este procedimiento, no será de aplicación en aquellos fueros específicos en los que se encuentre prevista la anonimización de todos los fallos judiciales que se publiquen en Jurisemia.

[33] Comprende tanto los indicadores directos como aquellos indirectos que sean necesarios para evitar la identificación de los sujetos de protección.

del titular de los datos personales y de los elementos que permiten su identificación (conf. 6.3.).

Dado que el objeto del presente procedimiento son resoluciones judiciales, los datos sensibles en la mayoría de los casos no pueden ser suprimidos sin afectar la integridad del razonamiento jurídico, en tanto forman parte de los fundamentos que sustentan la decisión adoptada por el órgano jurisdiccional. En consecuencia, el método propuesto en esta Guía no se orienta a la eliminación del dato sensible ni a la supresión del contenido relevante del fallo, sino a impedir su vinculación con una persona determinada, mediante la anonimización del titular de los datos y de todos los indicadores directos e indirectos que permitan su identificación.

Este criterio se aplica de manera integral: cuando en una misma resolución concurren diversas categorías especiales de datos personales, la anonimización no debe limitarse a cada causal de forma aislada, sino contemplar el conjunto de factores detectados y su posible interacción, a fin de garantizar que la información jurídicamente relevante permanezca accesible, pero desvinculada de toda persona concreta cuya dignidad, intimidad o situación de vulnerabilidad deba ser protegida. Así, por ejemplo, frente a la presencia de información relativa a la salud mental, la condición de víctima de violencia de género, minoridad u otros supuestos de protección reforzada, el contenido relevante para la decisión judicial se mantiene visible, mientras que se anonimiza a la persona concreta junto con todos los indicadores que permitan su reidentificación. Este es el principio rector que equilibra la publicidad y transparencia del Poder Judicial con la protección de datos personales en la publicación de resoluciones judiciales.

7. Evaluación del riesgo de identificación: matriz y aplicación práctica

7.1. Gestión de riesgos

La gestión de riesgos es *el proceso mediante el cual se identifica, analiza y valora la probabilidad e impacto de las ocurrencias de amenazas que, mediante la explotación de alguna vulnerabilidad, puedan materializar un riesgo para los derechos de las personas*[34]. Constituye una instancia necesaria para la selección y extensión de los mecanismos de anonimización adecuados, permitiendo priorizar acciones según el nivel de riesgo y garantizar una protección efectiva de los derechos involucrados.

[34] Agencia de Acceso a la Información Pública & Unidad Reguladora y de Control de Datos Personales. (2020). Guía de evaluación de impacto en la protección de datos.

7.2. Matriz de riesgo

La matriz de riesgo es una herramienta metodológica que permite evaluar y representar de manera estructurada el nivel de riesgo asociado a la posible identificación de personas en la publicación de resoluciones judiciales.

El procedimiento de detección establecido en el punto 6.6 constituye el flujo principal de trabajo para la evaluación de anonimización. La matriz opera como herramienta de apoyo complementaria a dicho procedimiento, a la que el gestor de carga y testeo puede recurrir para fundamentar sus decisiones en cualquier etapa del proceso, resultando especialmente útil en los supuestos no previstos (punto 6.5) o en zonas grises donde el procedimiento estándar no ofrezca una respuesta inequívoca.

Su función principal es combinar dos variables clave: la probabilidad de identificación de la persona y el impacto que dicha identificación podría generar sobre sus derechos fundamentales. La combinación de estas variables permite asignar a la resolución analizada un nivel de riesgo específico, lo cual orienta la elección de las medidas de anonimización y mitigaciones necesarias para cada caso concreto.

7.2.1. Variables

7.2.1.1. Probabilidad de identificación

Esta variable evalúa la posibilidad de que una persona sea identificada a partir de los datos incluidos en la resolución judicial, ya sea mediante indicadores directos o indirectos. Se clasifica en tres niveles:

- **Elevada**: cuando los datos permiten identificar a la persona de manera directa o en forma sencilla, sin necesidad de información adicional ni de un análisis complejo. Esto ocurre ante la presencia de indicadores directos o de indicadores indirectos suficientemente específicos que, por sí solos o en su conjunto, conduzcan a la identificación.
- **Intermedia**: cuando la información podría llevar a la identificación solo en ciertos contextos o mediante el cruce con datos adicionales no contenidos en la resolución.
- **Remota**: cuando solo existe una posibilidad excepcional o muy limitada de identificación, debido a que los datos presentes en la resolución carecen de especificidad suficiente para vincularlos con una persona determinada.

7.2.1.2. Impacto

Esta variable mide la magnitud del daño o afectación que podría derivarse de una identificación no autorizada, considerando a la sensibilidad de la información revelada, el ámbito involucrado y las consecuencias potenciales para los derechos de la persona. Se clasifica en tres niveles:

- **Grave**: cuando la divulgación puede generar perjuicios significativos o irreversibles para la persona, afectar derechos fundamentales, exponer

categorías especiales de datos personales o provocar revictimización, estigmatización o discriminación.

- **Moderado**: cuando podría producir molestias, exposición pública indeseada o consecuencias negativas, sin llegar a comprometer gravemente los derechos fundamentales de la persona.
- **Leve**: cuando el impacto de una eventual identificación sería acotado o de baja relevancia, limitándose a una exposición mínima que no genera afectaciones significativas a los derechos ni a la vida privada de la persona.

7.2.2. Nivel de riesgo

A partir de la combinación de las dos variables -probabilidad de identificación e impacto potencial de dicha identificación- se determina un nivel de riesgo que permite orientar las medidas de anonimización y protección necesarias para cada resolución judicial.

La matriz de riesgo relaciona ambas variables de la siguiente manera:

↓**Probabilidad || Impacto** →	**Leve**	**Moderado**	**Grave**
Elevada	Riesgo Medio	Riesgo Alto	Riesgo Alto
Intermedia	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Remota	Riesgo Bajo	Riesgo Medio	Riesgo Medio

Cada combinación conduce a los siguientes supuestos:

- **Riesgo alto:** se presenta cuando la probabilidad de identificación es elevada y el impacto es moderado o grave o cuando la probabilidad es intermedia y el impacto resulta grave. Requiere la aplicación de medidas de anonimización reforzadas.
- **Riesgo medio**: se configura cuando la probabilidad de identificación es elevada pero el impacto es leve, cuando la probabilidad es intermedia y el impacto moderado, o cuando la probabilidad es remota y el impacto es moderado o grave. Demanda una revisión cuidadosa del caso concreto para determinar las medidas de protección adecuadas.
- **Riesgo bajo**: corresponde a escenarios en los que la probabilidad de identificación es intermedia o remota y el impacto resulta leve. La necesidad de anonimización es mínima o inexistente.

7.2.3. Consideraciones sobre la naturaleza de la evaluación

La matriz es siempre una herramienta de apoyo, la determinación de la probabilidad de identificación y del impacto asociado constituye una evaluación contextual, que dependerá de las particularidades de cada caso, del tipo de información involucrada y del modo en que los datos puedan combinarse o correlacionarse para generar un potencial perjuicio para los derechos de los involucrados. Por lo que, la toma de decisiones sobre la publicación o anonimización requiere siempre una valoración prudente y fundada de las circunstancias del caso.

Las categorías propuestas funcionan como criterios orientativos destinados a aportar consistencia y transparencia al análisis, pero no sustituyen el juicio del operador especializado que debe aplicarse en cada situación concreta que surge de la práctica judicial.

7.3. Aplicación práctica de la matriz de riesgos

Este apartado presenta una tabla de referencia que vuelve operativos los criterios establecidos en la matriz de riesgo. Para ello, clasifica algunos de los datos correspondientes a categorías especiales de datos personales presentes en resoluciones judiciales según su categoría, probabilidad de identificación, impacto potencial y nivel de riesgo resultante.

La tabla constituye una herramienta orientativa y consultiva que facilita la identificación del nivel de riesgo asociado a los datos presentes en las categorías especiales de datos personales, sin sustituir el criterio profesional de los gestores de carga y testeo ni las pautas específicas de cada fuero. Su aplicación requiere siempre una valoración contextual del caso concreto, fundada en el principio de proporcionalidad.

Los niveles de probabilidad e impacto asignados en esta tabla reflejan el escenario más frecuente para cada categoría. No obstante, la probabilidad de identificación efectiva dependerá de los indicadores directos e indirectos presentes en cada resolución concreta (punto 6.3), por lo que estos valores deben ajustarse según las particularidades del caso.

Categoría	Probabilidad	Impacto	Nivel de riesgo
Vida sexual / Identidad de género / Violencia de género / NNyA / Salud	Elevada	Grave	ALTO
Asuntos familiares	Elevada	Moderado	ALTO

Adultos mayores (en situación de dependencia) / Discapacidad	Intermedia	Moderado	MEDIO
Origen étnico o racial / Pueblos originarios	Remota	Moderado	MEDIO
Afiliación sindical	Intermedia	Leve	BAJO
Opiniones políticas	Remota	Leve	BAJO

7.3.1. Zonas grises, revisión humana y control escalonado

Aun contando con categorías predeterminadas de protección y recomendaciones específicas por fueros, siempre existirán zonas grises o supuestos no previstos -correspondientes a los casos contemplados en el punto 6.5 de esta Guía- en los que no resulta evidente si un dato debe anonimizarse. Estas situaciones pueden involucrar identificadores indirectos (atributos que, combinados con otra información, permiten reidentificar a una persona) o datos contextuales que no resultan identificatorios en términos generales pero que pueden identificar a una persona en el contexto específico del fuero o del caso. Por ejemplo, la referencia a “la docente del turno mañana de la Escuela n.° 47 de la localidad de Villa del Totoral” puede funcionar como un identificador directo dentro de la resolución judicial, aun cuando individualmente ninguno de esos datos lo sea en otros contextos: la especificidad del cargo, la institución y la localidad pequeña hacen que la identificación resulte prácticamente inmediata.

En estas zonas grises, la revisión humana es indispensable para evaluar el riesgo de reidentificación y aplicar el principio de proporcionalidad al decidir si corresponde anonimizar y en qué medida. Para garantizar una protección efectiva, Nexo -la plataforma de carga de resoluciones judiciales que funciona como interfaz privada de Jurisemia- implementa un control escalonado por roles cuyo funcionamiento se desarrolla en el punto 8 de esta Guía.

Como parte de este mecanismo, al gestor de carga y testeo le corresponde completar una evaluación de proporcionalidad durante el proceso de carga, conforme al procedimiento establecido en el Manual operativo de Nexo. El supervisor, como segundo nivel de revisión, examina dicha evaluación y valora de forma independiente el riesgo de reidentificación antes de autorizar la publicación.

La siguiente escala de decisión institucional orienta la valoración del supervisor a partir de la probabilidad de reidentificación evaluada en el caso concreto. Esta escala complementa -pero no reemplaza- la evaluación bivariable de la matriz de riesgo (punto 7.2.2).

Probabilidad de reidentificación	Descripción	Acción recomendada
Remota	No existen elementos que permitan identificar directa o indirectamente a una persona o la información residual o contextual es mínima y requeriría conocimiento especializado o acceso restringido para reidentificar. El riesgo es meramente teórico.	Publicación autorizada sin ajustes adicionales, salvo que el impacto potencial de una eventual identificación resulte moderado o grave conforme a la matriz de riesgo (punto 7.2.2), en cuyo caso al supervisor le corresponde evaluar medidas complementarias.
Intermedia	Existen elementos contextuales que podrían permitir inferir la identidad de alguna parte o persona, especialmente en localidades pequeñas o hechos reconocibles.	Revisión adicional o aplicación de medidas complementarias por el supervisor antes de la publicación.
Elevada	El contexto, notoriedad o detalles del caso hacen probable la reidentificación, incluso sin datos directos.	Publicación diferida o sujeta a revisión del Boletín Judicial.

Este procedimiento establece una doble instancia de revisión: la matriz de riesgo orienta la anonimización inicial por parte del gestor y la evaluación de riesgo permite al supervisor validar esa decisión, asegurando la trazabilidad y la proporcionalidad en la protección de datos.

El funcionamiento integral de este control escalonado, junto con los mecanismos de trazabilidad y rendición de cuentas que lo sustentan, se desarrolla en el punto siguiente.

8. El sistema Nexo como mecanismo de control diferenciado por roles

Nexo es la interfaz privada de carga que actúa como puerta de ingreso y control de todo documento que se incorpora a Jurisemia. Esta plataforma de gestión documental permite subir, revisar y publicar resoluciones judiciales mediante un sistema de control diferenciado por roles, diseñado para que cada etapa del proceso -desde la carga inicial hasta la publicación- cuente con funciones claras, verificables y complementarias entre los distintos actores intervinientes.

Nexo constituye una medida organizativa integral del plan de protección de datos y compliance en inteligencia artificial para el sistema Jurisemia implementado por el Poder Judicial de Córdoba. Su arquitectura garantiza controles escalonados sobre dos dimensiones complementarias -la pertinencia de la publicación y la protección de datos personales-, registra las decisiones de manera trazable y asegura que cada resolución judicial haya sido evaluada conforme a los estándares establecidos en esta Guía antes de alcanzar la interfaz pública de Jurisemia. La diferenciación de funciones por roles, desarrollada en el punto 5 de esta Guía, encuentra en Nexo su materialización operativa.

8.1. Estructura del control en Nexo: dos dimensiones, dos niveles de revisión

El sistema Nexo estructura el control de cada resolución judicial en torno a dos dimensiones de evaluación complementarias, que responden a finalidades distintas:

La primera dimensión se refiere a los criterios de publicación: determina si la resolución posee relevancia jurisprudencial que justifique su incorporación a Jurisemia. Esta evaluación responde a la función institucional de conformar un repositorio de precedentes que reflejen la evolución doctrinaria, los cambios de criterio y los casos de interés público, depurando la base de datos de resoluciones reiterativas o de trámite que no aportan valor jurisprudencial diferenciado.

La segunda dimensión se refiere a los criterios de protección de datos personales: determina si la resolución contiene datos que requieran anonimización conforme a los lineamientos establecidos en esta Guía y, en caso afirmativo, si las medidas aplicadas resultan adecuadas y proporcionales.

Ambas dimensiones operan de manera simultánea dentro del flujo de trabajo de Nexo. Cada resolución es evaluada tanto en su pertinencia para la publicación como en el cumplimiento de los estándares de protección de datos antes de alcanzar la interfaz pública de Jurisemia.

A su vez, dentro de cada una de estas dimensiones, Nexo implementa un control escalonado mediante dos niveles de revisión por roles diferenciados: el gestor de carga y testeo realiza la primera evaluación y el supervisor ejerce una revisión independiente que valida, complementa o corrige la decisión inicial. Este mecanismo asegura que ninguna resolución sea publicada sobre la base de una única valoración individual, fortaleciendo tanto la calidad del repositorio jurisprudencial como la protección efectiva de los datos personales.

8.1.1. Criterios de publicación: conformación del repositorio jurisprudencial

Los criterios de publicación determinan qué resoluciones judiciales merecen ser incorporadas al sistema Jurisemia. Estos criterios no responden a una selección discrecional, sino a parámetros institucionales objetivamente establecidos que orientan la conformación de un repositorio jurisprudencial coherente y representativo. Su fundamento se inscribe en el principio de transparencia judicial y máxima divulgación

establecida en la Ley n.° 27275 de Acceso a la Información Pública, garantizando que la ciudadanía pueda conocer las decisiones adoptadas por el Poder Judicial.

La plataforma Nexo incorpora estos criterios de publicación como opciones predeterminadas dentro del sistema. En el primer nivel de revisión, al gestor de carga y testeo[35] le corresponde evaluar la pertinencia de cada resolución, verificando que el documento se encuadre en alguno de los criterios disponibles en la plataforma -tales como la novedad doctrinaria, el cambio de criterio jurisprudencial o el interés público del caso-. Esta verificación inicial constituye un filtro institucional que asegura coherencia en la difusión de jurisprudencia, en tanto los criterios sobre los cuales se puede elegir han sido determinados de manera previa y objetiva.

Cuando el gestor considera que una resolución posee relevancia jurisprudencial pero no encuadra en ninguno de los criterios vigentes, puede elevar una solicitud de incorporación de nuevo criterio al Boletín Judicial. Esta funcionalidad garantiza que los criterios de publicación puedan evolucionar conforme a las necesidades institucionales, manteniendo siempre el control centralizado sobre su aprobación. El administrador[36], tras analizar la solicitud, decide fundadamente su incorporación o rechazo, asegurando que toda modificación responda a razones objetivas y no a decisiones individuales de operadores judiciales.

En el segundo nivel de revisión, al supervisor[37] le corresponde confirmar o cuestionar la decisión inicial del gestor sobre la pertinencia de la publicación. Esta revisión verifica el correcto encuadramiento de la resolución en los criterios institucionales vigentes, asegurando que solo se incorporen a Jurisemia aquellas resoluciones que efectivamente correspondan según los lineamientos establecidos.

Este control escalonado sobre los criterios de publicación asegura que la conformación del repositorio jurisprudencial responda a criterios institucionales verificables y no a valoraciones subjetivas de operadores individuales. De este modo, se evita tanto la omisión de resoluciones relevantes como la incorporación de documentos que no aporten valor jurisprudencial diferenciado. Adicionalmente, la posibilidad de proponer nuevos criterios garantiza flexibilidad institucional sin comprometer la coherencia del sistema.

8.1.2. Criterios de protección de datos personales: control de la anonimización

Los criterios de protección de datos personales establecidos en esta Guía determinan qué información corresponde anonimizar para resguardar la intimidad, dignidad y derechos de las personas involucradas en procesos judiciales. Como se expuso en este documento, el cumplimiento de estos criterios no es optativo, sino que

[35] Gestor de carga: el agente judicial designado por el titular de una dependencia judicial, capacitado por el Boletín Judicial y habilitado para incorporar resoluciones al sistema.
[36] Administrador: el agente del Boletín Judicial o del área técnica del Poder Judicial, que cuenta con acceso completo a todas las funcionalidades del sistema, incluyendo tanto las funciones operativas como las herramientas de configuración propias de la plataforma.
[37] Supervisor: el agente designado por el Boletín Judicial con funciones de verificación de calidad y control del cumplimiento de los criterios de protección de datos personales, previo a la publicación efectiva de los documentos.

constituye una obligación legal derivada de la Ley n.° 25326 de Protección de Datos Personales y de los compromisos internacionales asumidos por el Estado argentino.

En el primer nivel de revisión, al gestor de carga y testeo le corresponde evaluar la necesidad de anonimización de cada resolución antes de su carga en el sistema, aplicar las medidas de protección correspondientes conforme a los criterios establecidos en esta Guía y verificar que los archivos cargados respeten la normativa de protección de datos personales. Esta primera evaluación requiere criterio jurídico, conocimiento de la normativa aplicable y comprensión del contexto fáctico del caso, a fin de identificar correctamente la presencia de categorías especiales de datos personales (siguiendo los lineamientos del punto 6 de esta Guía) y aplicar las técnicas de anonimización que correspondan de manera previa a la incorporación del documento en Nexo.

En el segundo nivel de revisión, al supervisor le corresponde revisar críticamente las decisiones adoptadas por el gestor, verificar la correcta aplicación de las medidas de anonimización y decidir fundadamente si la resolución cumple los estándares institucionales de protección de datos personales para su publicación. Esta revisión no constituye una mera verificación formal: el supervisor analiza sustancialmente si la protección aplicada resulta adecuada al caso concreto -evaluando que se hayan identificado correctamente todos los datos que requieren protección-, si la anonimización aplicada resulta apropiada, la existencia de posibles riesgos de reidentificación y si se ha respetado el principio de proporcionalidad en la difusión de la información.

Cuando la resolución contiene datos anonimizados y el supervisor confirma que las medidas de protección aplicadas resultan adecuadas, le corresponde incorporar una leyenda que informe al público que se han aplicado medidas de protección de datos personales conforme a esta Guía y a la normativa vigente. Esta leyenda cumple una doble función: por un lado, garantiza la transparencia del proceso al comunicar al lector que la resolución fue objeto de tratamiento; por otro, constituye un registro verificable del cumplimiento de los estándares de protección, en línea con el principio de rendición de cuentas establecido en el punto 4.2.5 de esta Guía.

Cuando el supervisor detecta errores, omisiones o medidas de protección insuficientes, le corresponde rechazar la carga. Nexo ofrece al supervisor un menú de motivos de rechazo predeterminados que contemplan las deficiencias más recurrentes en materia de protección de datos personales. Adicionalmente, el supervisor puede complementar esta información mediante el campo “observaciones”, proporcionando orientación específica al gestor sobre las correcciones necesarias. El sistema notifica el rechazo y sus motivos al gestor, quien debe subsanar las observaciones antes de reenviar la resolución. Este diálogo institucionalizado entre gestor y supervisor fortalece progresivamente la calidad de las decisiones de anonimización, generando un proceso de aprendizaje continuo que mejora los estándares de protección de datos en el ámbito judicial.

Este control escalonado garantiza que ninguna resolución judicial sea publicada sin haber transitado por dos instancias independientes de evaluación en materia de protección de datos.

Adicionalmente, el rol de administrador -reservado al personal del Boletín Judicial y del área técnica del Poder Judicial- garantiza la seguridad del sistema, la correcta configuración de permisos y el cumplimiento de las medidas organizativas necesarias para resguardar la confidencialidad, disponibilidad e integridad de los datos personales durante todo el proceso. Como medida de control adicional, este rol posee la facultad de retirar resoluciones ya publicadas en Jurisemia cuando resulte necesario para subsanar errores de anonimización o proteger datos personales inadvertidamente expuestos.

8.2. Proporcionalidad en la protección de datos

El control escalonado por roles que Nexo implementa en la dimensión de protección de datos resulta particularmente relevante para garantizar la aplicación efectiva del principio de proporcionalidad, desarrollado en el punto 4.2.4 de esta Guía. Este principio exige equilibrar adecuadamente la protección de los datos personales con la preservación del contenido jurídico de las resoluciones, evitando tanto la difusión innecesaria de información que permita identificar a las personas protegidas como la supresión desproporcionada de datos que torne incomprensible el fallo.

La evaluación de la proporcionalidad requiere análisis contextual y criterio jurídico especializado; no puede realizarse mediante la aplicación mecánica de reglas predeterminadas, sino que demanda considerar las particularidades de cada caso. El hecho de que esta evaluación sea realizada sucesivamente por dos operadores judiciales distintos -el gestor en el momento de la carga y el supervisor en la instancia de revisión- reduce significativamente el riesgo de errores en ambas direcciones: el supervisor puede detectar tanto excesos en la anonimización que afecten la inteligibilidad del precedente como insuficiencias que expongan categorías especiales de datos personales de manera innecesaria.

Cuando ambos niveles de revisión confirman de forma independiente que las medidas de protección resultan adecuadas al caso, existe mayor certeza institucional sobre el cumplimiento de los estándares normativos aplicables.

8.3. Trazabilidad y rendición de cuentas en la protección de datos

Nexo registra automáticamente todas las acciones realizadas sobre cada resolución judicial: quién la cargó, cuándo, qué metadatos se le asignaron, si se aplicaron medidas de anonimización, quién la revisó, si fue rechazada y por qué motivos y cuándo se publicó finalmente. Esta información constituye un registro de auditoría que permite verificar el cumplimiento de los procedimientos institucionales y reconstruir íntegramente el proceso seguido para cada documento.

La trazabilidad registrada por Nexo vuelve operativo el principio de rendición de cuentas establecido en el punto 4.2.5 de esta Guía. Cada decisión adoptada en materia de protección de datos personales queda registrada, lo que permite demostrar que el Poder Judicial adoptó medidas organizativas apropiadas para proteger los datos

personales tratados y que cada agente actuó conforme a las funciones que le fueron asignadas.

Asimismo, si se detectase una publicación inadvertida de categorías especiales de datos personales, el registro de Nexo permite identificar en qué etapa del proceso ocurrió el error, qué decisiones se adoptaron y qué controles se efectuaron. Esta información resulta esencial para implementar medidas correctivas, prevenir la reiteración del problema y cumplir con el deber de diligencia que la normativa de protección de datos personales impone a quienes intervienen en el tratamiento.

Los registros de auditoría trazables constituyen, además, un respaldo para los agentes judiciales que operan en Nexo: ante cualquier cuestionamiento sobre una publicación, la documentación del proceso permite acreditar que se siguieron los procedimientos establecidos en esta Guía y que las decisiones adoptadas fueron fundadas.

8.4. Integración de Nexo con los lineamientos operativos

A los agentes judiciales que operan en la plataforma Nexo les corresponde observar, además de los criterios establecidos en esta Guía, los lineamientos específicos contenidos en el Manual operativo de Nexo, que traduce estos principios en instrucciones paso a paso para la carga, revisión y publicación de resoluciones judiciales. Ambos documentos se interpretan de manera integrada: los criterios de protección aquí establecidos se aplican siguiendo los procedimientos descriptos en el Manual operativo, cuyo uso correcto resulta indispensable para garantizar la efectividad de las medidas organizativas de protección de datos personales.

9. Reidentificación

9.1. La reidentificación como riesgo permanente

Aun cuando un documento haya sido sometido a un proceso de anonimización, pueden darse situaciones en las que una persona sea identificada nuevamente al combinar distintos datos o al utilizar herramientas automatizadas. Este fenómeno, conocido como reidentificación, puede producirse por errores humanos, fallas técnicas o cruces de información que permiten vincular los datos anonimizados con una persona real. Prevenir este riesgo es uno de los desafíos más relevantes en la era de la inteligencia artificial y del creciente volumen de datos judiciales.

En el ámbito judicial, la reidentificación constituye un riesgo significativo porque puede exponer categorías especiales de datos personales de las personas involucradas en una causa, lo que puede derivar en daño en la reputación -cuando quienes participan en procesos sensibles son identificados públicamente y su vida profesional o social se ve afectada-, exposición de información íntima -al revelarse datos sobre salud o situaciones de violencia- y uso indebido de la información -permitiendo que terceros la empleen con fines de extorsión, acoso, discriminación o prácticas no autorizadas-.

Por estas razones, la anonimización efectiva no es un mero trámite administrativo sino una obligación legal y ética orientada a proteger la integridad, privacidad y dignidad de las personas involucradas en las resoluciones judiciales.

9.2. Tipos más comunes de reidentificación y prácticas de prevención

Seguidamente se resumen los tipos más comunes de reidentificación y las formas de prevenirla.

9.2.1. Por combinación de datos

Ocurre cuando diferentes fragmentos de información, que individualmente no permiten identificar a una persona, se combinan entre sí y, en conjunto, hacen posible inferir su identidad. Estos fragmentos se denominan cuasi-identificadores y pueden incluir datos como la edad, el género, la localidad, la profesión, el cargo que ocupa o incluso la fecha de un evento relevante. Aunque cada uno de estos elementos, tomado por separado, no constituye un dato personal, su combinación dentro de un documento judicial o su contraste con otras fuentes públicas (como registros oficiales, redes sociales o noticias periodísticas) puede permitir reconocer a una persona específica.

Ejemplo: "edad + municipio + cargo público" = identificación de una persona aun sin su nombre.

Para minimizar este riesgo es importante reducir los cuasi-identificadores, evitando publicar combinaciones de atributos (edad exacta + ocupación + barrio + fecha precisa) que, en conjunto, permitan la identificación. Ello también podría lograrse mediante la utilización de rangos (edad: 40-45), categorías generales (ocupación: “trabajador” en lugar de “repositor”) y la supresión de fechas exactas cuando no resulten imprescindibles para la comprensión del fallo.

9.2.2. Por inferencia o contexto

Incluso si todos los datos personales directos (nombres, DNI, direcciones) fueron eliminados, el contexto narrativo o los detalles del caso pueden permitir deducir la identidad de una persona. Esto se conoce como reidentificación por inferencia. Se trata de información que, combinada o aislada, no es explícitamente personal, pero permite identificar a alguien por características únicas o circunstancias específicas. Puede incluir: características físicas distintivas (altura, cicatrices, tatuajes); hechos notorios o públicos relacionados con la persona; lugares poco poblados o situaciones que reducen el grupo de posibles personas a una sola; y combinaciones de fechas, cargos o eventos que, aunque sean datos generales, permiten deducir la identidad.

Ejemplo: un médico de una especialidad muy específica del único hospital de una localidad pequeña. Aunque no se mencione el nombre, la persona es fácilmente identificable.

En estos casos, resulta indispensable el control humano del agente capacitado, quien tras la lectura comprensiva del documento judicial puede valorar el riesgo de

reidentificación. Este tipo de evaluación contextual es precisamente la que fundamenta el control escalonado por roles previsto en el punto 8 de esta Guía.

9.2.3. Por error humano o automatización sin control

Aunque las herramientas automáticas de anonimización pueden ser eficaces, no son infalibles. Publicar documentos sin una revisión humana final puede generar riesgos relevantes de reidentificación.

En materia de automatización, la inteligencia artificial puede pasar por alto datos poco evidentes -como segundos apellidos, apodos, fechas o ubicaciones específicas- y no siempre interpreta correctamente el contexto, por ejemplo, combinaciones de hechos que permiten deducir la identidad de alguien. En materia de errores humanos, los operadores pueden omitir la revisión del documento final antes de cargarlo al sistema, dejando sin proteger metadatos residuales o categorías especiales de datos personales.

Para prevenir estos riesgos constituyen buenas prácticas: la implementación de un control humano como instancia de revisión final en forma previa a la publicación, la documentación del proceso de anonimización para garantizar su trazabilidad y posibilitar la auditoría y el uso de herramientas automatizadas de manera complementaria, como apoyo al criterio humano y no como reemplazo de este.

10. Próximos pasos: hacia la anonimización asistida por inteligencia artificial

El proceso de anonimización que el Boletín Judicial lleva adelante actualmente es de carácter manual: cada resolución es revisada por el equipo de trabajo, que identifica y suprime los datos personales conforme a los criterios establecidos en esta Guía. Este procedimiento, si bien garantiza un alto nivel de control y sensibilidad contextual, demanda tiempos significativos de revisión y depende enteramente de la disponibilidad y la atención del personal.

En ese marco, el Boletín Judicial dará inicio al desarrollo un prototipo de herramienta de anonimización semiautomatizada asistida por inteligencia artificial, destinada a optimizar el tratamiento de datos personales en las resoluciones judiciales incorporadas al sistema Jurisemia. Esta herramienta contempla un sistema de etiquetado y una clasificación orientativa de las principales categorías de datos personales con sus posibles estrategias de anonimización.

El modelo al que se apunta es el de anonimización automatizada con control humano: la tecnología actúa como asistente de detección inicial, y el agente judicial o supervisor valida, ajusta y aprueba el resultado final antes de su publicación. Este enfoque permite conjugar eficiencia tecnológica y garantías jurídicas, asegurando la trazabilidad de las decisiones y la protección efectiva de los derechos de las personas.

10.1. Antecedentes en el ámbito judicial argentino

El desarrollo del Boletín Judicial se inscribe en un proceso más amplio de consolidación y expansión de experiencias de anonimización automatizada en el ámbito judicial argentino. Entre los proyectos más destacados que han implementado sistemas de inteligencia artificial orientados a detectar y suprimir datos sensibles en resoluciones judiciales, se pueden mencionar varios ejemplos. Uno de ellos es el sistema de código abierto adoptado por el Juzgado n.° 13 de la ciudad Autónoma de Buenos Aires, el cual fue desarrollado en 2020 por la Oficina de Estadísticas Judiciales del Poder Judicial de la ciudad de Buenos Aires[38].

Otro hito importante es el desarrollo de AymurAI por parte de DataGénero, en alianza estratégica con el Juzgado Penal, Contravencional y de Faltas n.° 10 de la Ciudad Autónoma de Buenos Aires, a cargo del Dr. Pablo Casas. Cabe destacar que esta herramienta ha sido testeada también en el Poder Judicial de Córdoba[39]. AymurAI emplea técnicas de procesamiento del lenguaje natural (PLN) y de reconocimiento de entidades nombradas (NER) para identificar información sensible y proponer su reemplazo o supresión, manteniendo la coherencia del texto y reduciendo los tiempos de revisión.

Más recientemente, se suma la Plataforma JusticIA (inteligencia artificial aplicada a procesos judiciales), una plataforma inteligente implementada en el Poder Judicial de San Juan que, entre las herramientas que ofrece, incorpora un anonimizador de documentos judiciales.

Estas experiencias confirman el potencial de la automatización para agilizar la publicación de fallos, aumentar la consistencia de los criterios y optimizar los recursos humanos, y constituyen un marco de referencia para el trabajo que el Boletín Judicial tiene en desarrollo.

10.2. Herramienta de anonimización semiautomatizada asistida por inteligencia artificial

No se busca trabajar en una herramienta completamente automatizada con inteligencia artificial, ello por cuanto, los modelos de inteligencia artificial pueden identificar patrones, pero no siempre comprenden la carga jurídica o social de la información residual que puede permitir una reidentificación indirecta. Por ello, ningún sistema automatizado resuelve por completo la complejidad lingüística y contextual de los documentos judiciales y la intervención humana sigue siendo indispensable como instancia de validación.

[38] Aguerre, C. (Ed.). (2020). Inteligencia artificial en América Latina y el Caribe: Ética, gobernanza y políticas. CETyS-Universidad de San Andrés. Pág.50.

[39] Poder Judicial de la Provincia de Córdoba. (2024). Informe del Boletín Judicial sobre demostración del sistema “AymurAI”.

Desde una perspectiva técnica e institucional, los sistemas más convenientes son aquellos que:

- Se basan en software libre o de código abierto, lo que permite auditoría, transparencia y adaptación a las necesidades locales.
- Son portables, de modo que puedan alojarse en los servidores propios del Poder Judicial, garantizando la soberanía tecnológica y evitando dependencias externas.
- Permiten la incorporación progresiva de nuevas categorías o reglas de anonimización, facilitando su mejora continua mediante entrenamiento supervisado y retroalimentación del personal judicial.

En conclusión, la automatización con revisión humana constituye actualmente la mejor práctica disponible: equilibra la eficiencia de las herramientas tecnológicas con la sensibilidad jurídica, ética y contextual que solo la intervención humana puede garantizar. La práctica y la evolución tecnológica demandan un sistema abierto, flexible y actualizable, que permita incorporar nuevos criterios, ajustar procedimientos y mejorar continuamente la protección de la información personal según los contextos de uso.

11. Conclusiones

Esta Guía constituye un instrumento institucional integral que articula la protección de datos personales, la transparencia judicial y el uso responsable de inteligencia artificial en el sistema Jurisemia por parte del Poder Judicial de la Provincia de Córdoba. Su implementación representa un compromiso con estándares internacionales de derechos humanos, *compliance* en inteligencia artificial y rendición de cuentas en la administración de justicia.

La anonimización judicial no debe entenderse como un obstáculo a la transparencia, sino como una herramienta que permite conciliar los derechos fundamentales de las personas en materia de protección de datos con el acceso a la información pública de manera responsable. Mediante la protección fundada en criterios objetivos y proporcional al riesgo de cada caso, se preserva el valor jurídico y el contenido informativo de las resoluciones, fomentando un ecosistema judicial más abierto, seguro y confiable.

El trabajo presentado en esta Guía se sustenta en un marco normativo robusto que integra instrumentos internacionales, regionales y nacionales, junto con normativa específica del Tribunal Superior de Justicia de la Provincia de Córdoba. Los principios rectores establecidos operan de manera integrada, orientando una anonimización proporcional y adaptada a los distintos fueros, contextos y tipos de casos. La matriz de riesgo permite evaluar la probabilidad de identificación y el impacto potencial, facilitando la toma de decisiones sin sustituir el criterio profesional de los operadores judiciales. La arquitectura de Nexo, a su vez, garantiza trazabilidad completa, diferenciación clara de funciones por roles y registro automático de todas las acciones realizadas sobre cada documento judicial.

La Guía no constituye un documento cerrado sino un marco de referencia dinámico que orienta la práctica institucional. La efectividad de sus lineamientos depende de la capacitación continua de los agentes judiciales, la participación activa de gestores y supervisores y su actualización periódica conforme a la evolución tecnológica, el desarrollo jurisprudencial y la experiencia acumulada. En esa línea, se aspira a una herramienta de anonimización semiautomatizada asistida por inteligencia artificial con control humano, conjugando eficiencia tecnológica con garantías jurídicas, sin delegar en la automatización la decisión final sobre la publicación.

El Poder Judicial de la Provincia de Córdoba, a través del Boletín Judicial, asume el compromiso de mantener este documento alineado con los estándares internacionales y adaptado a los desafíos que plantea el uso de inteligencia artificial en el ámbito judicial. El sistema Jurisemia, operando bajo estos lineamientos y con el soporte de Nexo, representa un modelo de gestión judicial que concilia la transparencia, la protección de datos y la aplicación ética de la inteligencia artificial.