PODER JUDICIAL
República de Costa Rica

REGLAMENTO PARA EL TRATAMIENTO DE LOS DATOS PERSONALES CONTENIDOS EN BASES DE DATOS DE ACCESO PÚBLICO DEL PODER JUDICIAL

Comisión Protección de Datos
Aprobado en la sesión N° 33-2024 del 29 de julio de 2024, Art. XV, Corte Plena

CONTENIDO

(DAR **CLICK** EN CADA **TÍTULO** PARA IR AL TEXTO RESPECTIVO)

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto.

El presente reglamento tiene por objeto regular el tratamiento de los datos personales contenidos en las bases de datos de acceso público que administra el Poder Judicial de Costa Rica, que formen parte del ámbito de aplicación establecido en la Ley de Protección de Datos Personales, cualquier otra legislación vigente y este Reglamento, de manera tal que, garanticen y equilibre los derechos de acceso a la información pública, transparencia, privacidad, autodeterminación informativa y la prohibición de toda forma de discriminación, garantizando el manejo adecuado de datos, la seguridad de la información y potenciando los beneficios del uso de las herramientas tecnológicas en el tratamiento de los datos personales.

Artículo 2. Ámbito de aplicación.

Las normas contenidas en este reglamento se aplicarán al tratamiento que se dé a los datos personales que figuran en las bases de datos de acceso público del Poder Judicial, sin distinción de la materia y con independencia de si los respaldos son físicos o electrónicos, escritos u orales, de conformidad a lo establecido en la Ley de Protección de Datos vigente.

Las bases de datos internas o domésticas se regirán por lo dispuesto en la normativa especial que las regule, sin perjuicio de la vinculación que paras ellas pueda tener la ley N°8968 cuando fungen como respaldo de bases de datos de acceso público.

En el caso de las bases de datos que contienen información de uso exclusivo de personas funcionarias judiciales o las partes intervinientes en un proceso o trámite, pero que también contienen otra de naturaleza pública, deberá aplicarse lo dispuesto en este reglamento respecto al segundo tipo de información.

Artículo 3. Definiciones.

Para la aplicación de este reglamento, deben considerarse las siguientes definiciones:

A. **Autodeterminación informativa**: Derecho fundamental derivado del derecho a la privacidad, que consiste en la posibilidad de controlar el flujo y manejo de la información personal frente a terceras personas, de forma tal que evite su empleo arbitrario o inadecuado, lesiones a los derechos fundamentales y que propicien acciones discriminatorias.

B. **Anonimización o despersonalización**: Es la protección otorgada a una persona sobre la que consten datos sensibles o de acceso restringido. Consiste en desvincular o desasociar de las resoluciones judiciales o documentos administrativos los datos de una persona que no deban publicarse o transmitirse a terceros, mediante la

eliminación o sustitución de estos a través de su ocultamiento, de la utilización de acrónimos o de cualquier otra estrategia que los oculte.

C. **Base de datos personales**: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manual, independientemente de la modalidad de su elaboración, organización o acceso.

D. **Base de datos de acceso público**: Aquella que puede acceder a su contenido de forma total o parcial, por cualquier persona que lo solicite o busque.

E. **Base de datos interna o doméstica:** Es aquel archivo, fichero, registro u otro conjunto estructurado de datos personales restringidos, que no es de acceso irrestricto; ya que, aunque forma parte de registros de acceso público, solo es de interés del titular y de la administración pública, para la adecuada prestación de servicios públicos de conformidad con el artículo 8 inciso e) de la Ley N° 8968.

F. **Base de datos secundarias:** Son las bases de datos que se construyen a partir de estadísticas o resúmenes de bases de datos primarias. Ejemplo: El SIGMA, es un repositorio de reportes estratégicos para la ayuda en la toma de decisiones, el cual se regirá por las excepciones del artículo 8 de la Ley N.° 8968.

G. **Comisión de Protección de Datos**: Órgano de trabajo adscrita al Consejo Superior encargada de recomendar a dicho órgano las acciones relacionadas con la protección de datos en el Poder Judicial.

H. **Datos personales**: Cualquier dato relativo a una persona física identificada o identificable, tal como el nombre, número de cédula, dirección domiciliaria, entre otros.

I. **Datos personales de acceso irrestricto**: Son aquellos contenidos en bases de datos públicos de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

J. **Datos personales de acceso restringido**: Son aquellos de interés solo para su titular o para la Administración Pública, aunque formen parte de registros de acceso al público. Por ejemplo: el certificado de delincuencia.

K. **Datos sensibles**: Es toda aquella información perteneciente al fuero íntimo de la persona, que tiene la particular capacidad de afectar la privacidad del individuo o de incidir en conductas discriminatorias, por ejemplo, su origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas; así como la información biomédica, vida personal, la salud, la identidad de género y la orientación sexual, entre otros.

L. **Derecho al olvido**: Es el derecho que tienen todas las personas para que ningún tipo de dato personal esté disponible para terceros, una vez transcurrido el plazo de 10 años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otro plazo para datos concretos. El procedimiento para anonimizar los datos que permiten la tutela del derecho al olvido se encuentra regulado en el artículo 6) del presente reglamento.

M. **Grupo Administrador de Nexus.PJ:** Es un grupo conformado por las jefaturas de cada oficina sistematizadora, o bien, quienes ellas designen en su representación, que se encargan de la administración de la Base de Datos Nexus.PJ.

N. **Oficialía de Protección de Datos**: Es la oficina encargada de velar por la implementación y el cumplimiento efectivo de la normativa, políticas y procedimientos relacionados con la protección de datos en el Poder Judicial.

O. **Oficinas Sistematizadoras**: Todas las oficinas institucionales que clasifican, analizan y publican documentación en el Poder Judicial y en el Nexus.PJ.

P. **Persona interesada**: Es la persona física, titular de los datos que sean objeto del tratamiento automatizado o manual; o bien, quien esa autorice formalmente, tenga su representación legal o sea su heredero o sucesor.

Q. **Persona identificada o identificable**: **Es toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.**

R. **Persona redactora**: Persona o grupo de personas que redactan el documento administrativo o resolución judicial.

S. **Persona usuaria**: Es cualquier persona (física o jurídica) que acceda por sí o a través de sus representantes o personas designadas a la información, con un interés personal, académico, laboral, de investigación, y cuyo fin sea lícito.

T. **Persona identificadora de datos**: Persona o grupo de personas de un despacho u oficina que tienen la obligación de identificar datos objeto de protección y emitir las alertas correspondientes.

U. **Persona responsable de una base datos:** Persona física o jurídica que funge como responsable final de una base de datos y que tiene competencia para decidir cuál es la finalidad de una base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento se les aplicará.

V. **Persona encargada de una base de datos**: Es la jefatura encargada del respectivo proceso de que se trate, a saber, el proceso de resguardo de la base de datos desde el punto de vista tecnológico (siempre y cuando estén hospedadas en servidores

a cargo de la Dirección de Tecnología de la Información y Comunicaciones), y el proceso de alimentación (contenido) de la base, es decir, la persona que labora en un despacho judicial u oficina administrativa, designada para velar por el cumplimiento de las disposiciones de tratamiento de datos en la base de datos que se encuentra a su cargo.

W. **Persona protectora de datos**: Persona o grupo de personas de un despacho u oficina encargadas de realizar la protección material de los datos previo a su publicación o transmisión a terceras personas.

X. **Tratamiento de datos personales**: Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, registro, la organización, la conservación, la modificación, extracción, identificación, protección, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

Artículo 4. Fuentes que regulan el tratamiento de los datos personales.

Para el tratamiento de los datos personales debe respetarse lo establecido en las normas constitucionales y convencionales que regulen este tema, así como lo dispuesto en la Ley de Protección de la persona frente al tratamiento de sus datos personales, su reglamento y demás normativa que la regulen.

Además, la protección de datos se regirá por los principios de autodeterminación informativa, consentimiento informado y de calidad de la información, así como por los subprincipios de actualidad, veracidad, exactitud y adecuación al fin, todos estos establecidos en la Ley de Protección de la persona frente al tratamiento de sus datos personales.

Dichos principios se describen de la siguiente manera:

a) Consentimiento informado:

La persona titular de información que conste en las bases de datos del Poder Judicial tiene derecho a que se le requiera su consentimiento informado para efectos del uso y transferencia de su información, con las salvedades que establece este reglamento y la ley.

No será necesario obtener consentimiento expreso para tratar datos personales suministrados por obligación legal o constitucional, siempre que esto se circunscriba exclusivamente a los fines procesales o administrativos para los que fueron recabados, o bien, a otros fines no incompatibles según lo dispuesto en el principio de adecuación al fin.

Si los datos entregados por disposición legal o constitucional para participar en procesos judiciales o realizar trámites administrativos se desean utilizar para fines distintos a los

autorizados en el párrafo anterior, será indispensable obtener el consentimiento expreso del titular.

Cuando un particular o institución pública soliciten la transferencia de información contenida en una base de datos del Poder Judicial en la que consten datos personales, requerirá consentimiento expreso y válido de las personas titulares, a excepción de los supuestos contemplados por ley. Dicho consentimiento informado ante el Poder Judicial será exigible en cualquier trámite administrativo o instrumento convencional o contractual que se suscriba y que tenga vinculación con datos personales, previo cumplimiento de los protocolos de actuación que al efecto formule el Poder Judicial.

b) Calidad de la información:

b.1) Actualidad:

Todas las bases de datos de acceso público del Poder Judicial deberán estar conformadas por datos actuales, cuya conservación sea pertinente o necesaria de acuerdo con la finalidad para la que fueron recibidos y registrados, o bien, para fines no incompatibles según lo dispuesto en el subprincipio de adecuación al fin.

Las bases de datos secundarias son fuentes derivadas de bases de datos primarias; para estos casos debe preservar tanto la base de datos primarias como las secundarias.

A efectos de valorar la actualidad y la necesidad de conservación en la base de datos, es obligatorio considerar las disposiciones institucionales sobre archivo y conservación de documentos, así como todas aquellas normas de rango legal y constitucional relacionadas con el tema.

Toda persona interesada en hacer valer el derecho al olvido podrá realizar la respectiva solicitud siguiendo el trámite establecido en el artículo 6.

b.2) Veracidad y exactitud:

Las personas encargadas de las bases de datos velarán porque en los documentos se consignen datos fehacientes y exactos. En caso de consignarse información inexacta, falsa, incompleta, deberá ser suprimida o rectificada dependiendo de la situación concreta.

b.3) Adecuación al fin:

En el marco de procesos judiciales o gestiones administrativas relacionadas con estos, no podrán solicitar datos que no sean absolutamente necesarios para el ejercicio o defensa de los derechos e intereses involucrados para su resolución.

No se considerará incompatible el tratamiento posterior de datos obtenidos en el marco de procesos judiciales o gestiones administrativas, cuando se haga con fines históricos,

estadísticos, científicos, investigativos o de auditoría, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos de las personas involucradas.

Las personas encargadas de las bases de datos deberán velar por una actualización de datos oficiosa y proactiva, de manera tal que de vigencia al cumplimiento de los diversos principios contemplados por esta norma.

Artículo 5. Derechos relacionados con el tratamiento de datos personales.

Con las salvedades de ley, toda persona interesada o quien este legitimada, podrá solicitar el acceso a la información que conste sobre su persona. Asimismo, podrá solicitar la rectificación, actualización, anonimización o eliminación de esta, en atención a los derechos de acceso a la información y de rectificación de todas las personas con respecto a sus datos personales contenidos en la Ley de Protección de la persona frente al tratamiento de sus datos personales.

Las solicitudes relacionadas con los derechos anteriormente indicados deberán ser resueltas en un plazo de cinco días hábiles contados a partir de la recepción de la solicitud. Lo que podrá derivar en:

a) Rechazo de la solicitud, que deberá notificar por escrito y de manera fundamentada.

b) Actualización, eliminación o anonimización de los datos, dependiendo del caso concreto, que se deberá notificar por escrito.

Deberá llevar un archivo de control interno de todas las solicitudes con la finalidad de verificar el respeto a los plazos y demás derechos de la persona interesada.

A efectos de estandarizar la atención de solicitudes de los derechos anteriormente indicados, deberá aplicar un procedimiento para atender solicitudes de Protección de Datos, debidamente aprobado por Consejo Superior.

Artículo 6. Derecho al Olvido.

Mediante el derecho al olvido, toda persona tiene derecho a que los datos de carácter personal que pudieran afectarla de alguna forma no estén disponibles para terceros, una vez transcurrido el plazo de 10 años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otro plazo para datos específicos.

Toda persona interesada o quien este legitimada para ello, podrá solicitar que se eliminen de los documentos judiciales o administrativos, los datos personales que consten sobre su persona. Asimismo, podrá solicitar que se eliminen aquellos datos que permitan su identificación, transcurridos diez años desde la emisión del documento judicial o administrativo, o del conjunto estructurado de datos que la contenga.

El plazo podrá variar en supuestos específicos si existe normativa o disposición jurídica vinculante que así lo avale.

Las solicitudes de anonimización deberán ser resueltas en un plazo no mayor a cinco días hábiles.

Deberá llevarse un archivo de control interno de todas las solicitudes con la finalidad de verificar el respeto a los plazos y demás derechos de la persona interesada.

Para efectos de aplicación en el presente reglamento, el derecho al olvido corresponderá exclusivamente a las bases de datos de acceso público del Poder Judicial.

Artículo 7. Sujetos legitimados para ejercer derechos.

La persona física titular de los datos personales, su albacea designado en proceso sucesorio, o aquella a quien designe mediante documento con firma autenticada, estarán legitimados para ejercer los derechos reconocidos en este Reglamento, la Ley de Protección de la persona frente al tratamiento de sus datos personales y demás garantías contenidas en otras disposiciones legales y constitucionales.

Artículo 8. Personas identificadoras de datos.

Son personas identificadoras de datos sensibles o de acceso restringido, todas las personas funcionarias que emitan resoluciones judiciales, documentos administrativos o cualquier otro conjunto estructurado de información que sea de acceso público, o bien, que sin ser quienes los emiten, sean designados formalmente por la coordinación o jefatura de un despacho u oficina en particular para efectuar la labor de identificación de datos.

Artículo 9. Obligaciones de las personas identificadoras de datos.

Toda persona identificadora de datos deberá:

a) Identificar si en las resoluciones judiciales (orales o escritas), documentos administrativos (documentos escritos, videos o audio) o cualquier otro conjunto estructurado de información a su cargo, existen datos sensibles o de acceso restringido que deban ser anonimizados de acuerdo con la normativa vigente.

b) Dejar constancia de cuáles datos deben ser anonimizados y el motivo por el cual son objeto de protección. En casos donde el fundamento no se desprenda de este reglamento, indicar la norma jurídica que lo respalda. Lo anterior debe quedar por escrito en la casilla electrónica o archivo físico que a los efectos se disponga.

c) Remitir los documentos al despacho o a la persona protectora de datos que realizará la protección material. En casos donde la persona identificadora sea la misma que la

que debe realizar la protección material, igualmente se deberá dejar constancia del motivo que justifica la anonimización.

d) Utilizar, de acuerdo con sus atribuciones, las herramientas tecnológicas que facilite la Dirección de Tecnologías de la Información y Comunicaciones, con la finalidad de establecer las medidas de seguridad que garanticen la confidencialidad, disponibilidad e integridad de la información que custodia el Poder Judicial.

e) Guardar confidencialidad respecto de los datos personales tratados.

f) Velar por el cumplimiento de este reglamento y demás normas relacionadas.

Artículo 10. Persona protectora de datos.

Son personas responsables de proteger datos personales, aquellas encargadas de anonimizar datos cuando consten datos sensibles o de acceso restringido.

Artículo 11. Obligaciones de las personas protectoras de datos.

Son obligaciones de las personas protectoras de datos, las siguientes:

a. Anonimizar los datos que le sean alertados por las personas identificadoras de conformidad con los lineamientos vigentes. No obstante, en aquellos casos que la persona protectora de datos detecte información que considera debe protegerse; sin embargo, no le fue así alertado, hará la observación a la persona identificadora correspondiente, para que analice nuevamente el tema y se pronuncie de forma definitiva en el plazo de dos días.

   De no recibirse respuesta, la persona encargada de la anonimización aplicará su criterio, siempre en estricto apego de lo normado en este reglamento y demás instrumentos jurídicos, pero ello no relevará de la responsabilidad correspondiente a quien omitió identificar un dato y/o pronunciarse respecto a las observaciones hechas.

   El procedimiento antes indicado no será necesario si la falta de alerta está relacionada con una causal de mera constatación, como lo es que consten datos de personas menores de edad, se trate de asuntos de familia o violencia doméstica, etc.; no obstante, cuando exista margen de interpretación o duda, deberá procederse según los términos indicados.

b. Remitir solicitud escrita a la Dirección de Tecnología de la Información y Comunicaciones cuando deba proteger los datos personales en la base de datos que el despacho u oficina tenga a su cargo y posterior a la modificación deberá verificar la correcta protección de la información.

c. Implementar las medidas de seguridad y control interno que correspondan, así como, cumplir con lo dispuesto en la Ley de Protección de la persona frente al tratamiento de sus datos personales, el Reglamento institucional y demás disposiciones aplicables.
d. Publicar las resoluciones judiciales y documentos administrativos, cuando corresponda.
e. Guardar confidencialidad respecto de los datos personales tratados.

f. Abstenerse de transferir, difundir o usar los datos sensibles o de acceso restringido para fines distintos a los autorizados.

g. Velar por el cumplimiento de este reglamento y demás normas relacionadas.

Artículo 12. Mecanismos o herramientas tecnológicas para anonimizar datos.

La Dirección de Tecnología de la Información y Comunicaciones deberá proporcionar a las personas funcionarias las herramientas tecnológicas que faciliten la debida protección de los datos, según los recursos disponibles a nivel institucional. Así como, establecer las medidas de seguridad que garanticen la confidencialidad, disponibilidad e integridad de la información que custodia el Poder Judicial.

Las personas de las oficinas y despachos encargadas de anonimizar documentos deberán emplear aquellos mecanismos tecnológicos para anonimizar datos con los que cuente la institución, y estos serán utilizados en estricto apego a las recomendaciones técnicas y de seguridad de la información que sean indicadas por la Dirección de Tecnología de la Información y Comunicaciones.

Está prohibido el uso de herramientas tecnológicas no autorizadas u oficiales. No obstante, en casos donde se soliciten documentos o cualquier otro conjunto estructurado de datos que únicamente consten en formato físico y que no se puedan convertir a uno digital compatible con las herramientas de anonimización oficiales o autorizadas, se podrán adoptar medidas de anonimización manuales, siempre que las mismas sean idóneas para lograr un tratamiento de datos adecuado, así como para permitir la comprensión del documento o conjunto estructurado de datos.

La persona responsable y las personas encargadas de las diferentes bases de datos deberán hacer los análisis de riesgos previo y establecer las acciones mínimas a las que obliga la normativa que rige la materia, a efectos de prevenir deficiencias de seguridad de la información. Lo anterior, sin perjuicio de que como parte de la valoración de riesgos permanente que debe realizar cada responsable, posteriormente en cada base de datos se realicen análisis propios según el resultado de la valoración previa.

Artículo 13. Oficialía de Protección de Datos del Poder Judicial.

El Poder Judicial contará con una oficina encargada de velar por la implementación y cumplimiento efectivo de la normativa, políticas y procedimientos relacionados con la protección de datos.

Dicha oficina estará a cargo de un Oficial de Protección de Datos quien, además de las funciones que le atribuya la autoridad institucional competente, deberá:

a) Brindar información y asesoramiento normativo sobre el tema de Protección de Datos.

b) Supervisar el cumplimiento normativo, de políticas y procedimientos de tratamiento de datos personales en bases de datos de acceso público del Poder Judicial.

c) Cooperar y ser el enlace con la autoridad de control de la Protección de Datos (PROHAB).

d) Atender a las personas interesadas e intermediarias en casos de reclamación de la Protección de los Datos.

e) Elaborar e implementar un programa de control de riesgos respecto al tratamiento de datos personales.

f) Verificar la implementación transversal de las disposiciones de tratamiento de datos personales en el Poder Judicial.

g) Promover una cultura institucional de protección de datos.

h) Mantener un inventario de las distintas bases de datos de acceso público del Poder Judicial.

i) Verificar que cada base de datos de acceso público tenga formalmente designadas tanto una persona responsable como a las personas encargadas, así como que estén ejerciendo sus funciones de manera activa.

j) Cualquier otra función relacionada con la Protección de Datos que le designe la Corte Suprema de Justicia.

La Oficialía estará bajo la dirección del órgano que la Corte Suprema de Justicia designe y dependerá del Consejo Superior del Poder Judicial, para efectos de dirección y jerarquía en lo que corresponde a sus competencias.

En caso de no contar con presupuesto suficiente para implementar la oficina correspondiente, las competencias descritas en el presente artículo podrán asignarse temporalmente por la Corte Suprema de Justicia a un órgano existente al momento de vigencia del presente reglamento.

Artículo 14. Respaldos de las bases de datos de acceso público del Poder Judicial.

Las bases de datos de acceso público del Poder Judicial deberán tener dos tipos de respaldos:

a) **Uno interno o doméstico,** que se conservará para consulta interna y contendrá toda la información en forma íntegra, sin ninguna forma de anonimización, pero

siempre observando estrictamente las medidas de seguridad de la información y confidencialidad que impone la legislación vigente y los lineamientos institucionales. Lo anterior, ya que de conformidad con lo señalado en la definición de base de datos interna o doméstica, el Poder Judicial está facultado para mantener documentos originales que conserven los datos sensibles, en su base de datos interna, con el fin de cumplir con la adecuada prestación de servicios, mantener la historia y estadística para rescatar temas de intereses relacionados con derechos humanos, género, violencia doméstica, accesibilidad, entre otros, sin que se dé acceso a esta información a terceros.

b) **Uno de acceso público**, que se conservará para consulta externa. Contendrá la información debidamente anonimizada de conformidad con las disposiciones vigentes. Su acceso podrá ser en línea o a solicitud de las personas usuarias. En el primer caso, la base de datos pública se construirá con toda la información que se publique; en el segundo, con toda aquella que se entregue por gestión de las personas interesadas. En ningún caso podrá publicarse información con datos sensibles o de acceso restringido sin la protección de datos previa.

En caso de que, por error humano o de sistemas, publiquen información con contenido sensible o información de acceso restringido, la persona que detecte el error, deberá comunicarlo inmediatamente a las personas encargadas de la base de datos respectiva, quienes tomarán de inmediato las medidas para proteger la información.

CAPÍTULO II
DISPOSICIONES COMUNES PARA TODAS LAS BASES DE DATOS DE ACCESO PÚBLICO EN EL PODER JUDICIAL, EXCEPTO PARA NEXUS.PJ

Artículo 15. Finalidad de las bases de datos.

Las bases de datos del Poder Judicial deberán especificar el fin o los fines de ésta, por escrito en su creación (legislativa o administrativa), así como, quien es la persona responsable y quienes son las personas encargadas de la misma.

El tratamiento de los datos se realizará respetando el o los fines de cada base de datos.

Las oficinas que tengan a su cargo una base de datos de acceso público velarán porque la información está actualizada y que se tomen las medidas para conservar la información, considerando las disposiciones institucionales sobre archivo y conservación de documentos, así como todas aquellas normas de rango legal y constitucional relacionadas con el tema.

Artículo 16. Persona responsable de la base de datos.

Toda base de datos de acceso público del Poder Judicial deberá tener un responsable final de la base de datos. Esta persona será la que tenga competencia para definir cuál es la finalidad de una base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento se les aplicará. Lo anterior deberá verse reflejado en un protocolo o reglamento que regule las especificidades de la base de datos.

Artículo 17. Persona encargada de la base de datos.

Toda base de datos de acceso público del Poder Judicial deberá tener una persona encargada de la parte tecnológica y de seguridad de la información y una persona encargada del contenido que se sube a la base de datos. La función principal de las personas encargadas de la base de datos es la de velar por el cumplimiento integral de las disposiciones de tratamiento de datos, lo que en ningún caso releva a las persona identificadoras o protectoras de datos de la responsabilidad en la que puedan incurrir por no cumplir con sus respectivas obligaciones.

Esta responsabilidad recaerá en las jefaturas de las oficinas que administran las diferentes bases de datos de acceso público, tanto desde el punto de vista tecnológico y de seguridad de la información, como desde el punto de vista de alimentación de contenido.

Cuando en una misma base de datos existan diferentes oficinas o despachos encargados, como sucede con la base de datos oficial Nexus.PJ, deberá nombrarse un grupo coordinador que ejerza la representación de todos, mismo que será integrado por las respectivas jefaturas o quienes estas designen.

Es deber de cada oficina administrativa y despacho jurisdiccional que emita resoluciones o documentos de acceso público no disponibles en Nexus.PJ, tener un respaldo de estos, que será conservado y custodiado por el plazo y en la forma en que dispongan los lineamientos institucionales y el ordenamiento jurídico nacional.

En las oficinas administrativas y los despachos jurisdiccionales que tengan información organizada tipo archivos, ficheros, registros o cualquier otro conjunto estructurado de datos, que contengan resoluciones judiciales o documentación administrativa de acceso público que no consten en Nexus.PJ, el órgano emisor o el Archivo Judicial, según sea el caso, deberá brindar el tratamiento adecuado a los datos personales, en los documentos, de acuerdo con las disposiciones legales y reglamentarias.

Artículo 18. Deber de anonimizar datos cuando medie una causal de protección.

Siempre que en una base de datos de acceso público consten datos de acceso restringido o sensibles, se deberá realizar la anonimización u ocultamiento de los datos, según los procedimientos establecidos para el tipo de base de datos en específico.

Como norma general, cuando lo que consten sean datos de acceso restringido lo que se ocultarán serán estos datos, mientras que cuando lo que consten sean datos sensibles lo que se anonimizará serán los datos de identificación del titular, así como aquellos otros datos circunstanciales, fácticos o que por asociación permitan individualizarlo.

CAPÍTULO III
BASE DE DATOS OFICIAL DE ACCESO PÚBLICO NEXUS.PJ

Artículo 19. Del Nexus y su finalidad.

Nexus.PJ es la base de datos oficial del Poder Judicial que contiene resoluciones judiciales y documentación administrativa de acceso público mediante Internet. Tiene las siguientes finalidades:

a) **Respaldo histórico**: Mediante la utilización de técnicas de indización, archivística y análisis documental se preservan documentos de interés público.

b) **Insumo científico**: Los documentos almacenados fungen como materia prima para diferentes ramas de la investigación, incluyendo la jurídica, estadística y sociológica.

c) **Transparencia y acceso a la información pública**: Se busca que la sociedad en general y la comunidad jurídica en particular conozcan el contenido de las resoluciones judiciales y documentación administrativa y puedan efectuar control ciudadano.

Este objetivo no implica necesariamente que publiquen los datos de identificación de todas las personas intervinientes en los procesos o trámites, ya que, pueden existir datos sensibles o de acceso restringido que hagan necesario anonimizar total o parcialmente documentos, así como materias que por disposición legal o constitucional tengan restringido el acceso a la identidad de las partes; en este último supuesto, quien desee conocer la existencia de antecedentes o los documentos íntegros, deberá acudir a las oficinas encargadas de custodiar estos registros o la información original, a efectos de que se determine si se cumplen con los supuestos de ley necesarios para acceder a la información requerida.

Artículo 20. Tipos de documentos que pueden publicarse en la base de datos pública Nexus.PJ.

La base de datos oficial Nexus.PJ se alimentará de las resoluciones judiciales y documentos administrativos, que agreguen las oficinas sistematizadores incluidas dentro del "Procedimiento para autorizar oficinas sistematizadoras y definir el tipo de documentos que se publican en Nexus-PJ", siempre que dichos documentos sean de acceso público según la normativa procesal de cada materia y no exista ningún otro impedimento de orden legal para su difusión.

Los textos que se publiquen deben ser fiel reflejo del original, con la salvedad de las anonimizaciones de datos que deban realizarse.

En ningún caso, podrán publicarse en esta base de datos la fotografía de una parte interviniente o testigo.

Los despachos y oficinas emisoras de documentos administrativos y resoluciones judiciales tendrán la responsabilidad de verificar que lo que se envíe para publicación a las oficinas sistematizadoras esté dentro del marco de lo permitido por las ordenanzas procesales de cada materia.

Artículo 21. Responsable de Nexus.PJ.

El Poder Judicial, a través de su Administración Superior, será el responsable de la base de datos oficial Nexus.PJ.

Artículo 22. Encargados de Nexus.PJ.

La base de datos oficial Nexus.PJ será administrada por las oficinas sistematizadoras incluidas en el "Procedimiento para autorizar oficinas sistematizadores y definir el tipo de documentos que se publican en Nexus-PJ".

Nexus.PJ será administrada por las siguientes oficinas sistematizadoras:

a. Centro Electrónico de Información Jurisprudencial.
b. Centro de Jurisprudencia de Sala Constitucional
c. Centro de Jurisprudencia de Sala Primera
d. Centro de Jurisprudencia de Sala Segunda
e. Centro de Jurisprudencia de Sala de Casación Penal
f. Departamento de Artes Gráficas
g. Dirección Ejecutiva
h. Dirección Junta Administradora del Fondo de Jubilaciones.
i. Sección Administrativa de la Carrera Judicial.
j. Secretaría General de la Corte
k. Y cualquier otra oficina sistematizadora que se llegue a crear y a incorporar en el Nexus.PJ

Cada oficina sistematizadora será encargada individualmente respecto de la información a su cargo.

Las obligaciones, en cuanto al tratamiento de datos serán las mismas que las indicadas en las disposiciones comunes de este reglamento. A su vez, deberán mantener estrecha coordinación con los encargados de identificar datos y, en caso de ser tanto identificadoras como protectoras de datos, cumplir con las obligaciones de ambas figuras.

La inclusión o exclusión de oficinas sistematizadoras en la administración de Nexus.PJ se regirá por lo dispuesto en el procedimiento anteriormente indicado.

Artículo 23. Grupo Administrador de Nexus.PJ.

La administración de la Base de Datos Nexus.PJ estará a cargo de un Grupo Administrador conformado por las jefaturas de cada oficina sistematizadora, o bien, quienes ellas designen en su representación.

El grupo coordinador deberá elegir, bianualmente, a una persona que lo presida, sin que existan obstáculos de reelección.

Artículo 24. Adecuación de documentos ya publicados al nuevo Reglamento.

Cuando una persona interesada, cuyos datos consten en una resolución o documento ya publicado en Nexus.PJ, considere que sus datos deben tratarse de acuerdo con las disposiciones de este Reglamento, podrá gestionar la readecuación de su caso.

Ante este tipo de solicitudes, la oficina sistematizadora encargada del documento o resolución tendrá un plazo de 5 días hábiles para resolver la gestión, cuyo resultado deberá ser notificado por escrito y de manera fundamentada a la persona interesada.

CAPÍTULO IV.
ANONIMIZACIÓN DE DOCUMENTOS ADMINISTRATIVOS Y RESOLUCIONES JUDICIALES.

Artículo 25. Datos que deben protegerse.

Deberán anonimizarse, previo a cualquier publicación, todos aquellos datos personales contenidos en resoluciones judiciales o documentos administrativos que permitan identificar a una persona sobre la que consten datos sensibles o de acceso restringido.

Los datos sensibles se conservarán con el fin de mantener la historia y facilitar la investigación jurídica, así como para rescatar temas relacionados con derechos humanos, género, violencia doméstica, accesibilidad, entre otros; no obstante, no se podrán revelar los datos personales que permitan identificar a los titulares de la información sensible.

Los datos de acceso restringido, tales como números de teléfono privados, correos electrónicos personales, dirección exacta del domicilio, cuentas bancarias y cualquier otro que la ley o disposiciones constitucionales cataloguen como tal, lo que se anonimizará será el dato restringido específico.

En aquellos casos en los que datos sensibles o de acceso restringido consten en imágenes insertadas en el documento o resolución, éstas deberán sustituirse a efectos de no vulnerar la autodeterminación informativa del titular de los datos.

Artículo 26. Anonimización mediante etiquetado de datos.

Al momento de utilizar el etiquetamiento como mecanismo para anonimizar, se utilizarán las etiquetas que indica el siguiente cuadro, sin perjuicio de que una autoridad competente las modifique posteriormente:

Tipo de Datos	Etiquetas
Nombres de las personas físicas, seudónimos, sobrenombres	**[Nombre 001], [Nombre 002], [Nombre 003]...**
Datos numéricos o alfanuméricos: Placas, matrículas, números de cédula, números de teléfono, números de cuenta bancaria, etc.	**[Valor 001], [Valor 002], [Valor 003]...**
Otros datos: Direcciones, correos electrónicos, nombres de lugares, puestos de trabajo.	**[...]**
Imágenes con datos sensibles o de acceso restringido	**[Imagen 001], [Imagen 002], [Imagen 003]...**

Lo anterior, en el entendido que los números corresponden a consecutivos que irán aumentando conforme a la cantidad de datos que sean objeto de protección en el mismo documento.

Artículo 27. Protección de resoluciones orales.

Deberán protegerse previo a su publicación o difusión, todas aquellas resoluciones orales que contengan datos sensibles o de acceso restringido. No obstante, hasta tanto no se cuente con las herramientas tecnológicas que permitan dicha protección, no se podrá publicar este tipo de información.

Artículo 28. Datos que requieren especial atención.

Además de lo dispuesto en este reglamento sobre datos sensibles y de acceso restringido, se deberá prestar especial atención y realizar la anonimización correspondiente cuando se trate de datos:

1. De personas menores de edad, incluyendo situaciones en las que la persona era menor de edad, aunque ya no lo sea.

2. De personas con discapacidad.

3. De víctimas de acoso sexual o laboral y víctimas de delitos sexuales o violencia doméstica.

4. De partes o intervinientes procesales que estén en condición de vulnerabilidad o que tengan una protección procesal especial derivada de una norma legal.

5. De partes o intervinientes procesales cuya divulgación de datos permita identificar a una persona respecto a la que se deban anonimizar datos.

6. Que, en virtud de disposiciones legales o de rango superior vinculantes, tengan carácter confidencial o privado.

7. Que revelen direcciones de residencia, números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular, así como las fotografías de personas.

8. No podrán publicarse datos que permitan identificar a las personas actoras, demandadas, ofendidas, testigos o imputadas, en procesos penales, penales juveniles, de familia, violencia doméstica y pensiones alimentarias. Cuando en resoluciones de materias distintas a las señaladas, se vincule a una persona con un proceso de esa naturaleza, se deberá aplicar la protección respecto a esa persona en particular.

9. Los datos de personas indígenas o que involucren derechos colectivos del pueblo indígena que consten en peritajes antropológicos.

10. Los datos agregados a bases de datos anonimizadas sobre poblaciones en condición de vulnerabilidad pueden ser tratadas y divulgadas, siempre y cuando, se establezcan las garantías oportunas para salvaguardar los derechos contemplados en la legislación.

Artículo 29. Datos que no deben anonimizarse.

Los supuestos en que no corresponderá la anonimización de datos son los siguientes:

a) Cuando una resolución esté relacionada con un delito cometido por un funcionario público en el ejercicio de su cargo, no se anonimizarán sus datos, salvo que medien datos sensibles o de acceso restringido.

b) Respecto a resoluciones administrativas disciplinarias anteriores al acto final, se deberá anonimizar o despersonalizar el nombre de las personas funcionarias procesadas, ofendidas o testigos. No obstante, respecto a la resolución que concluye el procedimiento, sí deberá prevalecer la publicidad de los datos salvo que medien datos sensibles o de acceso restringido.

c) Los nombres de quienes intervienen como personas juzgadoras, defensores y defensoras, fiscales y fiscalas, personas investigadoras, peritos y peritas, abogados y abogadas de las partes; lo anterior, en tanto no gocen de una medida de protección prevista por ley o disposición constitucional.

d) Los nombres de sociedades, empresas o establecimientos comerciales, números de cédula jurídica, marcas y nombres comerciales, salvo que deban eliminarse para no identificar a personas físicas con derecho de protección o exista norma legal especial que declare su confidencialidad.

e) Nombres de personas autoras de obras citadas.

f) Los nombres de las personas físicas que son partes en los respectivos procesos y que son mencionados en sentencias firmes con carácter de cosa juzgada material, dictas por las Salas de la Corte Suprema de Justicia o de Tribunales Superiores. Esta excepción no aplicará a las resoluciones dictadas en las materias penal, penal juvenil, de familia, violencia doméstica y pensiones alimentarias. Tampoco cuando se haga alusión a datos sensibles o de acceso restringido de alguna de las partes.

g) La información sensible o restringida de las personas que expresamente, señalen su deseo de que sus datos no sean anonimizados, siempre que tengan capacidad jurídica para tomar dicha decisión y no se comprometan los derechos de privacidad y autodeterminación informativa de otras personas.

CAPÍTULO V
DEL ACCESO A LA INFORMACIÓN, LA TRANSMISIÓN O LA DIFUSIÓN DE LA INFORMACIÓN DEL PODER JUDICIAL Y OTROS.

Artículo 30. Acceso a documentación que consta en Nexus.PJ.

Cuando alguna persona interesada solicite resoluciones judiciales y/o documentos administrativos que estén disponibles en Nexus.PJ, se procurará entregar la información contenida en ese medio oficial, sea mediante el enlace de acceso específico, descarga digital o versión impresa. Lo anterior, toda vez que la información contenida en la base de datos en línea ya ha pasado por el proceso de tratamiento de datos personales.

Artículo 31. Acceso a documentación de bases de datos distintas a Nexus.PJ.

Podrán ser accesadas mediante gestión personal, aquellas bases de datos cuya regulación legal y por el tipo de información que contengan, así lo permitan.

Cada oficina llevará un registro de las solicitudes de información que les sean remitidas, en dicho registro debe indicarse al menos; nombre y número de cédula de la persona que solicita información, la información que requiere, fecha de la solicitud, si se entregó o no la información solicitada, en caso de que no se entregara se debe indicar el motivo. En los casos que la solicitud de información se haga por medios electrónicos la solicitud deberá contar con la firma digital.

El acceso a la información que, por el estado procesal en que se encuentra una causa, sea privada o de acceso restringido solo para las partes, se regirá por los lineamientos y normativa legal especial que exista al respecto y no por lo dispuesto en este Reglamento.

Artículo 32. Protección de datos personales de documentación de acceso público no disponible en Nexus.PJ.

En el momento en que soliciten una resolución judicial y/o documento administrativo de acceso público no disponible en Nexus.PJ, el despacho u oficina emisor del documento deberá analizar si en el texto existen datos sensibles o de acceso restringido.

En ningún caso podrá suministrar, transferir o difundir resoluciones judiciales y/o documentos administrativos con datos sensibles o de acceso restringido sin una despersonalización previa, salvo que haya autorización expresa del titular de la información y que la legislación lo permita. Para dar esta información, la legislación debe autorizarlo en forma expresa o en caso de que haya una orden emanada por la autoridad judicial competente.

En el caso de las oficinas administrativas, éstas serán las responsables de efectuar la protección material de los datos conforme a este Reglamento. Respecto a los despachos jurisdiccionales, la persona encargada deberá remitir el documento al Centro Electrónico de Información Jurisprudencial (C.E.I.J) para que esta oficina realice la protección respectiva;

sin embargo, en todos los casos deberá indicar el motivo por el que se requiere la anonimización. Además, es responsabilidad del despacho emisor brindar los documentos en formatos compatibles con los sistemas de despersonalización con los que cuenta la institución

Una vez que el C.E.I.J. realice la protección material de los datos, lo devolverá al despacho jurisdiccional para lo que corresponda.

Artículo 33. Solicitudes canalizadas por medio del Departamento de Prensa y Comunicaciones.

En el momento en que soliciten un documento o resolución que no conste en Nexus.PJ por medio del Departamento de Prensa y Comunicaciones del Poder Judicial, esta oficina deberá coordinar con el emisor del texto, imagen o video a efectos de que éste determine si lo gestionado es de acceso público y si existen datos sensibles o de acceso restringido.

En caso de estimar procedente entregar la información, el trámite continuará de la siguiente forma:

a) Respecto a documentos administrativos, la oficina emisora lo deberá remitir al Departamento de Prensa y Comunicación listo para entregarse a la persona solicitante, lo que incluye que el texto, imagen o video esté debidamente anonimizado cuando así corresponda.

b) En el caso de las resoluciones judiciales, el despacho emisor deberá remitir una copia fiel al Departamento de Prensa y Comunicación, pero será su responsabilidad alertar si existen datos sensibles o de acceso restringido. En caso de que no alertar la presencia de datos objeto de protección, el Departamento de Prensa y Comunicación entregará lo solicitado. No obstante, de advertir que existen datos sensibles o de acceso restringido, estará obligado a solicitar al C.E.I.J. que proteja los datos señalados, por lo que el texto suministrado deberá ser compatible con los sistemas de anonimización con los que cuenta la institución. Una vez que el C.E.I.J. efectué la protección de los datos, devolverá el documento al Departamento de Prensa y Comunicación, quien lo entregará a la persona solicitante.

Artículo 34. Registro de entrega de la información.

De entregar una resolución judicial o documento administrativo de acceso público no disponible en Nexus.PJ, estará obligado a llevar una bitácora o registro que permita dar trazabilidad al suministro de la información.

Como mínimo el control deberá indicar el nombre completo de la persona usuaria, tipo y número de identificación, documentos o resoluciones suministradas, forma en el que se le entregó y confirmación, en caso de existir, de que se protegieron los datos sensibles y/o de acceso restringido.

Artículo 35. Conservación de textos originales.

Para efectos de uso institucional, procesal y para garantizar a las partes su derecho de acceso a la información, es deber de los despachos y oficinas emisoras de las resoluciones judiciales y documentos administrativos mantener los textos originales por el tiempo y la forma que lo dispongan los lineamientos institucionales y el ordenamiento jurídico, así como seguir las políticas y disposiciones relacionadas con conservación de documentos.

Las oficinas sistematizadoras recibirán una copia fiel de los textos originales.

Artículo 36. De la responsabilidad.

El Poder Judicial es custodio de la información que ha solicitado a las personas usuarias, por lo que, es responsable de guardar reserva, proteger datos o informaciones sensibles de terceros, a fin de tutelar los derechos de las personas usuarias de quienes recibe y produce información de la relación del servicio público justicia que brinda.

Asimismo, toda persona servidora judicial es responsable por el tratamiento que realice sobre los datos que, con ocasión de sus respectivas funciones, haga.

Artículo 37. Generación de bases de datos particulares.

Se prohíbe a todas las personas físicas y jurídicas generar respaldos particulares de las bases de datos del Poder Judicial. Lo anterior incluye la construcción de bases de datos paralelas mediante la utilización de herramientas robotizadas, de inteligencia artificial o que de cualquier forma comprometan la finalidad de las bases de datos y la seguridad de la información.

CAPÍTULO VI
DE LOS DEBERES DE LAS PERSONAS USUARIAS QUE ACCEDAN A LA INFORMACIÓN DE LAS BASES DE DATOS DEL PODER JUDICIAL

Artículo 38. Del alcance subjetivo del presente capítulo.

Las obligaciones establecidas en el presente capítulo serán de aplicación obligatoria a las partes, sus representantes, auxiliares de la justicia, estudiantes y en general a toda persona que, con motivo de un proceso, labor académica, profesional o investigativa tenga acceso a una base de datos del Poder Judicial que contenga información personal.

Artículo 39. De las obligaciones de las personas usuarias.

Son deberes de las personas usuarias que accedan a información personal de terceros en las bases de datos del Poder Judicial:

1. Guardar la confidencialidad respecto de cualquier información que llegue a tener acceso con motivo del conocimiento de datos personales en las bases de datos del Poder Judicial.

2. Prevenir y hacer de conocimiento del oficial de protección de datos si llega a determinar la existencia de algún error u omisión en la protección de datos personales en algún archivo o expediente del Poder Judicial, a que haya tenido conocimiento.

3. Cumplir y respetar las políticas, lineamientos y regulaciones que emita el Poder Judicial en materia de uso, almacenamiento, trasiego y control de datos personales en sus bases de datos.

4. Guardar las medidas de seguridad de los dispositivos electrónicos mediante los cuales se le brinde acceso e información a las bases de datos del Poder Judicial en donde pueda haber datos personales.

5. Hacer uso de la información que tengan acceso en las bases de datos del Poder Judicial exclusivamente para los fines que fueron solicitadas.

6. Realizar cualquier tratamiento de los datos personales de manera responsable, aplicando el deber de confidencialidad, absteniéndose de emplear dicha información para usarla con fines descalificantes, discriminatorios, contrarios a la dignidad humana o falsos.

7. Adoptar medidas de prevención de uso, custodia y trasiego de la información recopilada en los dispositivos de almacenamiento y equipos tecnológicos en donde la misma sea guardada, para evitar que la misma sea modificada o destinada otros usos distintos a los que originan su acceso en las bases de datos del Poder Judicial.

8. Abstenerse de trasladar total o parcialmente la información personal que obtenga de las bases de datos del Poder Judicial hacia terceros, con el fin de que estos la empleen para obtener un lucro o la destinen a afectar la privacidad los derechos e intereses subjetivos de las personas titulares de dicha información.

Artículo 40. Del incumplimiento de las obligaciones establecidas en el presente capítulo.

El incumplimiento de las obligaciones en el presente capítulo facultará al Poder Judicial a adoptar medidas para limitar total o parcialmente el acceso a las bases de datos con datos personales, para la persona que sea determinada como responsable de la respectiva acción u omisión, previa aplicación del procedimiento ordinario establecido en el libro segundo de la Ley General de la Administración Pública.

Mientras se desarrolla el indicado procedimiento administrativo, el Poder Judicial podrá adoptar cautelarmente la suspensión de acceso a las bases de datos y hasta que no se emita el respectivo acto administrativo firme.

CAPÍTULO VII
DISPOSICIONES FINALES.

Artículo 41. Capacitaciones.

La Escuela Judicial y el Departamento de Gestión Humana deberán incorporar en los programas y cursos por ellos impartidos, el componente de protección de datos, así como todo lo relacionado con los conocimientos propios de la materia, las regulaciones legales establecidas al efecto, lo dispuesto en el presente reglamento y lo referente a los protocolos internos que la regulan.

Artículo 42. Derogaciones.

Se deroga el Reglamento de actuación de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos personales en el Poder Judicial aprobado por la Corte Suprema de Justicia en la sesión N° 39-2014 celebrada el 11 de agosto del 2014, artículo XVIII y el Protocolo de despersonalización de datos para las oficinas administrativas del Poder Judicial aprobado por la Corte Plena en la sesión N° 21-2016 celebrada el 20 de junio del 2016, artículo V.

Artículo 43. Vigencia.

Este reglamento será de acatamiento obligatorio a partir de su publicación en el boletín judicial.