



GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO JUDICIAL



ÍNDICE

1.- INTRODUCCIÓN.

2.- OBJETO.

3.- DESTINATARIOS.

4.- NORMATIVA APLICABLE.

5.- CONCEPTOS BÁSICOS.

6.- PRINCIPIOS Y LEGITIMACIÓN.

6.1.- PRINCIPIOS.

6.2.- LEGITIMACIÓN.

7.- DERECHOS DE PROTECCIÓN DE DATOS.

8.- BRECHAS DE SEGURIDAD.

9.- RECOMENDACIONES.

10.- RECURSOS DISPONIBLES.



1.- INTRODUCCIÓN.

En la actualidad, vivimos una auténtica revolución digital con el uso constante de diferentes tecnologías, que si bien, en muchas ocasiones facilitan nuestro día y día, tanto en el ámbito personal como profesional, en ocasiones, incrementan los riesgos asociados a los derechos fundamentales de las personas, pudiendo afectar al derecho fundamental de la protección de datos personales de las personas, el cual se encuentra reconocido en el artículo 18.4 de la Constitución Española, en el artículo 8 del Convenio Europeo de Derechos Humanos y el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Por ello, resulta necesario adoptar medidas que eviten un acceso, tratamiento, conservación y difusión indebida de datos personales, fomentando una cultura de protección de datos en el ámbito judicial, concebida no como una limitación al ejercicio de la función jurisdiccional, sino como una garantía esencial de este derecho.

La Dirección de Supervisión y Control de Protección de Datos del CGPJ, autoridad de control de protección de datos en el ámbito jurisdiccional, ha publicado su [Plan Estratégico 2026-2028](#), que contiene una serie de actuaciones y actividades con el objetivo de sensibilizar a los órganos judiciales y promover el cumplimiento de la normativa vigente y el respeto a los derechos fundamentales en el ámbito de los órganos judiciales.

Así, el eje 1 “Adecuación a la normativa de protección de datos personales” y el eje 2 “Asesoramiento jurídico”, contienen como medidas, respectivamente, las relativas a la elaboración de una Guía sobre protección de datos personales en el ámbito judicial y la elaboración de recomendaciones en aquellos aspectos que sean más relevantes. En consecuencia, la Dirección de Supervisión y Control de Protección de Datos publica esta Guía.

Previamente a su elaboración, se realizó una comunicación a los órganos judiciales, para que trasladasen aquellas, dudas, experiencias y planteamientos que se pudiesen abordar desde un punto de vista práctico.

Desde esta Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial queremos mostrar nuestro más sincero agradecimiento a los miembros de la Carrera Judicial y a los Letrados y



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

Letradas de la Administración de Justicia que han participado en la elaboración de esta Guía, compartiendo sus dudas, experiencias y planteamientos prácticos en materia de protección de datos. Sus aportaciones han sido esenciales para abordar las cuestiones que surgen en el día a día de los órganos judiciales y para que este documento responda de forma útil y realista a las necesidades de quienes aplican la normativa en el ejercicio de la función jurisdiccional.

Hay que destacar también, que esta Guía contiene un último apartado de recursos disponibles de esta Dirección y que pueden ser consultados en la página web del CGPJ.

2.- OBJETO.

La finalidad de esta Guía práctica consiste en sensibilizar a quienes trabajan en los órganos judiciales de la relevancia que tiene garantizar la protección de datos como derecho fundamental y establecer un conjunto de pautas, con el fin de garantizar un tratamiento de los datos personales conforme a la normativa vigente y respetuoso con los derechos de las personas afectadas por la actividad jurisdiccional.

3.- DESTINATARIOS.

El contenido de esta Guía práctica se dirige:

- Jueces, juezas, magistrados y magistradas en el ejercicio de la potestad jurisdiccional.
- Letrados y letradas de la Administración de Justicia en el ámbito de sus funciones.
- Funcionarios, funcionarias y personal laboral al servicio de los órganos judiciales.
- Personal interino, en prácticas o cualquier otra persona que, por razón de su actividad, tenga acceso a datos personales en el ámbito judicial.



Recuerde

Si trabajas en los juzgados y tribunales, esta Guía contiene una serie de recomendaciones aplicables al tratamiento de los datos personales derivados de los procedimientos judiciales.

4.- NORMATIVA APLICABLE.

Como ya indicamos en la introducción, tanto la Constitución Española, como el Convenio Europeo de Derechos Humanos, así como la Carta de Derechos Fundamentales de la Unión Europea, reconocen la protección de datos personales como un derecho fundamental.

En el ámbito del Derecho de la Unión Europea, el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), establece el marco normativo actual, que se complementa a nivel interno con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD).

El RGPD, a través de su considerando 20, precisa dos cuestiones de especial relevancia para la Administración de Justicia.

En primer lugar, confirma su aplicación al tratamiento de datos personales realizado por los órganos jurisdiccionales.

En segundo lugar, establece que el control del cumplimiento de la normativa de protección de datos en aquellos tratamientos efectuados con ocasión del ejercicio de la función jurisdiccional no debe corresponder a las autoridades de control “tradicionales” —como la Agencia Española de Protección de Datos—, sino a una autoridad de control independiente integrada en el propio poder judicial, con el fin de salvaguardar su independencia. En la actualidad, le corresponde a esta Dirección de Supervisión y Control de Protección de Datos del CGPJ.

No obstante, cuando se trate la jurisdicción penal, no se aplica el RGPD sino la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

Además de estas normas, la LOPJ recoge una serie de precisiones en los artículos 236 bis a 236 decies, incluidos en el Título III, "Actuaciones judiciales", Capítulo I bis, dedicado expresamente a la protección de datos personales en justicia.

Jurisdicción	Normativa aplicable
Civil Contencioso-Administrativo Social Militar	RGPD + LOPDGDD + LOPJ
Penal	LO 7/2021 + LOPJ

5.- CONCEPTOS BÁSICOS.

A continuación, se ofrece una serie de definiciones para ayudar a una mejor comprensión tanto de esta Guía como del cumplimiento de la normativa de protección de datos personales.

- **Dato personal:** Cualquier información que identifique o pueda identificar, directa o indirectamente, a una persona física. Incluye, entre otros: nombre y apellidos, DNI, dirección, imagen, y voz.

También la información que forme parte de un procedimiento judicial en la medida que identifique o pueda identificar, sin esfuerzos desproporcionados, a una persona física.

- **Categorías especiales de datos:** datos personales especialmente sensibles, como los relativos a la salud, ideología, religión, orientación sexual, datos biométricos o genéticos. Su tratamiento exige garantías reforzadas y una justificación específica.

Sobre estas categorías especiales de datos, el RGPD incluye también por su posible impacto en los titulares de los datos personales tres definiciones más:



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de la asistencia sanitaria, que revelen información sobre su estado de salud.
 - **Datos biométricos:** Datos personales obtenidos a partir de características físicas, fisiológicas o conductuales que permiten identificar de manera unívoca a una persona, como huellas dactilares, imagen facial o voz.
 - **Datos genéticos:** Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física.
- **Tratamiento de datos:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no.

Así, y a modo ilustrativo, son de carácter automatizado todo el tratamiento de datos personales a través de los sistemas de gestión procesal; y de carácter no automatizado, toda documentación en papel con datos personales que forme parte de un procedimiento judicial.

Entre las operaciones de tratamiento, se encuentra la recogida, registro, organización, consulta, conservación, comunicación, publicación, archivo o supresión de los datos.

Por ejemplo, el registro de una demanda en el sistema de gestión procesal o la grabación de una vista, suponen un tratamiento de datos personales.

- **Tratamientos con fines jurisdiccionales:** Se refieren al tratamiento de datos personales directamente vinculados al ejercicio de la función jurisdiccional. Incluyen los datos utilizados en la instrucción, tramitación y resolución de los procedimientos judiciales.
- **Tratamientos con fines no jurisdiccionales:** Son aquellos realizados en el ámbito administrativo de la Administración de Justicia que no están directamente relacionados con la resolución de un



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

procedimiento judicial. Ejemplos: Gestión de personal, administración de recursos materiales y financieros, o la interposición de una queja.

Recuerde

Tenga en cuenta el gran volumen de datos personales que son objeto de tratamiento por los órganos jurisdiccionales en la tramitación de los procedimientos judiciales.

Pueden ser de diversa índole, entre ellos, identificativos, económico-financieros, de empleo, salud, infracciones administrativas o de naturaleza penal.

Una vez delimitados los conceptos de datos personal y tratamiento, así como la diferenciación entre tratamiento con fines jurisdiccionales, abordamos los conceptos de responsable y encargado del tratamiento, incluyendo las previsiones contempladas en la LOPJ, sobre los que recae el cumplimiento de la normativa de protección de datos personales, la figura del delegado de protección de datos personales, y el interesado.

- **Responsable del tratamiento:** La autoridad u órgano que determina los fines y medios del tratamiento de datos personales. En el ámbito judicial, la LOPJ precisa que el tratamiento de datos personales lo realizará el órgano competente, y dentro de él, quien tenga atribuida la competencia por la normativa vigente.
- **Encargado del tratamiento:** será quien trate datos personales por cuenta del responsable del tratamiento. En el ámbito de jurisdiccional, ostentan la condición de encargados del tratamiento el Ministerio de Justicia y las Comunidades Autónomas con competencias transferidas en materia de justicia. Así, la LOPJ contiene un mandato dirigido a las citadas a las que les corresponde suministrar los medios tecnológicos adecuados para el tratamiento de los datos personales, debiendo cumplir con las responsabilidades en materia de tratamiento y protección de datos personales que se les atribuya como administración prestacional.
- **Delegado de Protección de Datos:** su función consiste en asesorar y supervisar el tratamiento de datos personales del responsable o



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

encargado del tratamiento al que presta servicios, actuando de forma independiente. Tanto el RGPD como la LOPDGDD regulan una serie de supuestos en los que resulta obligatorio su nombramiento. Sin embargo, se excluye esta obligación cuando los órganos judiciales actúan en el ejercicio de su función jurisdiccional. Esta exclusión también la contempla la Ley Orgánica 7/2021.

No obstante, estas exclusiones no son óbice para que en el ámbito de las Administraciones prestacionales en materia de justicia hayan designado sus delegados de protección de datos.

- **Interesado:** Persona física cuyos datos personales son objeto de tratamiento. En el procedimiento judicial pueden ostentar la condición de interesados, como las partes procesales, testigos, o peritos.





CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

Para finalizar este apartado de conceptos, referirnos a un ámbito esencial en el tratamiento de datos personales como es la seguridad. En el apartado de recomendaciones se ofrecen algunas al respecto.

- **Seguridad de los datos:** Conjunto de medidas técnicas y organizativas destinadas a garantizar la protección de los datos personales frente a accesos no autorizados, pérdida, destrucción o alteración. Entre ellas, el doble factor de autenticación, contraseñas robustas, control de accesos, copias de seguridad, trazabilidad, y custodia documental. En el ámbito de justicia, se debe adoptar el Esquema Judicial de Interoperabilidad y Seguridad.
- **Seudonimización:** Tratamiento de datos personales de manera que ya no puedan atribuirse a un interesado si utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos no se atribuyan a una persona física identificada o identificable.

Por ejemplo, la eliminación de determinados datos personales de las resoluciones que se entregan a las partes y que no son necesarios que aparezcan.

- **Brecha de seguridad:** incidente que provoca la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma o la comunicación o acceso no autorizado de dichos datos.

La sección web de la Dirección de Supervisión y Protección de Datos del CGPJ, contiene un apartado dedicado a la [seguridad](#), incluyendo el [formulario](#) para notificar las brechas de seguridad a la propia Dirección.

6.- PRINCIPIOS Y LEGITIMACIÓN.

6.1.- PRINCIPIOS.

El tratamiento de datos personales en el ámbito de los órganos judiciales debe regirse por una serie de principios generales que actúan como criterios interpretativos y límites materiales al ejercicio de la función jurisdiccional y a



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

la actividad de la oficina judicial. Estos principios, de aplicación transversal, garantizan el respeto efectivo a los derechos fundamentales de las personas afectadas y contribuyen a una administración de justicia diligente, proporcional y respetuosa con la vida privada.

Su observancia debe integrarse de forma natural en la práctica diaria de jueces/as, magistrados/as, letrados/as de la Administración de Justicia y del personal al servicio de los órganos judiciales. Y los sistemas de gestión procesal deben diseñarse de manera que se garantice en todo momento su cumplimiento.

El RGPD regula estos principios (art.5):

Principio de Licitud, lealtad y transparencia

La licitud supone que todo tratamiento de datos personales realizado en el ámbito judicial se fundamente en una base legal suficiente, derivada del ejercicio de la potestad jurisdiccional o de las funciones legalmente atribuidas al órgano judicial. Ningún tratamiento puede realizarse al margen del marco normativo aplicable ni con fines ajenos al procedimiento judicial.

La lealtad implica que el tratamiento de los datos se lleve a cabo de manera honesta y respetuosa con los derechos del interesado, evitando prácticas encubiertas, desproporcionadas o abusivas, incluso cuando concurren limitaciones legítimas al derecho de información propias del proceso judicial.

La transparencia, en la medida compatible con la naturaleza del procedimiento, exige que las personas afectadas conozcan qué datos están siendo tratados, con qué finalidad, así como la posibilidad de ejercitar sus derechos de protección de datos, sin perjuicio de las restricciones legalmente previstas para garantizar la eficacia de la investigación o la tutela judicial efectiva.

Principio de limitación de la finalidad

Implica que los datos personales obtenidos o incorporados a un procedimiento judicial solo pueden ser tratados para los fines concretos y legítimos que justificaron su recogida.

Supone también, desde su vertiente de necesidad y proporcionalidad, que el tratamiento de datos personales se limite a aquellos supuestos en los que



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

resulte imprescindible para la correcta tramitación y resolución del procedimiento judicial.

Recuerde

La LOPJ (art.236 quinquies apartado 1) presta especial atención este principio de finalidad

"las resoluciones y actuaciones procesales deben contener los datos adecuados, pertinentes y limitados en relación a los fines para los que son tratados, en especial garantizar la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión"

Principio de minimización

Su aplicación deriva en que los órganos judiciales deben tratar únicamente los datos personales adecuados, pertinentes y limitados a lo estrictamente necesario en relación con la finalidad del procedimiento. Este principio se proyecta tanto en la incorporación de datos al expediente como en su reflejo en resoluciones judiciales, escritos y comunicaciones.

En la práctica judicial implica evitar la inclusión innecesaria de datos personales cuando no resulten relevantes para la fundamentación jurídica de la decisión adoptada. Para ello, se debe proceder a la seudonimización de los datos personales que no sean necesarios.

Recuerde

La LOPJ (art.236 quinquies apartado 2) presta especial atención este principio de minimización de datos

"Los Jueces/as y Magistrados/as, los Fiscales y los Letrados/as de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión".



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

Dada la relevancia y trascendencia de este principio, el Real Decreto-ley 6/2023, de 19 de diciembre, contiene un mandato (art.100) a las Administraciones prestacionales para que doten a las oficinas judiciales de medios tecnológicos para la realización automatizada de la anonimización, seudonimización y disociación de los datos personales.

El traslado de resoluciones judiciales a las Oficinas de Comunicación se realizará en los términos descritos en la LOPJ, y en el Protocolo de Comunicación de la Justicia, y sin perjuicio de que por las citadas cumplan con la normativa de protección de datos siguiendo las Instrucciones que para tal fin dicte la Oficina de Comunicación del CGPJ.

Principio de exactitud

Exige que los datos personales tratados por los órganos judiciales sean veraces y exactos, adoptándose las medidas razonables para su actualización cuando sea necesario. Los datos inexactos o desactualizados pueden generar decisiones erróneas o afectar de manera injustificada a los derechos del interesado.

Principio de Limitación del plazo de conservación

El principio de limitación del plazo de conservación impone que los datos personales se conserven únicamente durante el tiempo necesario para cumplir la finalidad que justificó su tratamiento. Una vez finalizado el procedimiento judicial y agotadas las responsabilidades legales derivadas del mismo, los datos deben ser archivados, bloqueados o suprimidos conforme a la normativa aplicable en materia de archivos judiciales.

Este principio exige una gestión responsable de los expedientes judiciales, tanto en soporte papel como electrónico, evitando la conservación indefinida de información personal sin justificación legal y garantizando el cumplimiento de los plazos de archivo, expurgo y conservación establecidos.

Principio de integridad y confidencialidad

Conlleva la adopción de medidas técnicas y organizativas para garantizar la seguridad del tratamiento de datos personales, evitando accesos no autorizados o ilícitos o la pérdida de documentación judicial. Estas medidas,



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

sobre todo las de carácter técnico, deben adoptarse por la Administración prestacional, pero algunas también dependen de los jueces/as, magistrados/as, letrados/as de la Administración de Justicia y demás personal. En el apartado de recomendaciones se incide en ello con algunos ejemplos.

A su vez, cuando estemos ante el tratamiento de datos personales en la jurisdicción penal, la LO 7/2021, de 26 de mayo, también ha reflejado estos principios de manera muy similar, si bien con alguna peculiaridad.

Recuerde

LO 7/2021, de 26 de mayo

Art.6 regula los principios del tratamiento de datos en la jurisdicción penal

Art.8 especificaciones al plazo de conservación

- *Plazo máximo 20 años salvo excepciones*
- *Revisión al menos cada tres años*

Art.10 especificaciones de la calidad de los datos (exactitud)

- *Diferenciar entre datos personales basados en hechos y los basados en apreciaciones personales*
- *Los datos inexactos, incompletos o no actualizados no deben transmitirse ni ponerse a disposición de terceros*

6.2.- LEGITIMACIÓN.

Además de los principios de protección de datos, el otro elemento esencial lo constituye la legitimación, es decir, que exista una base que permita el tratamiento de datos, y que además forma parte, como hemos adelantado ya, del principio de licitud.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

El RGPD establece las bases legitimadoras en el artículo 6, y en el artículo 9 cuando afecten a las categorías especiales de datos. Además de estos dos preceptos, el artículo 10 regula el tratamiento de datos de naturaleza penal.

Para fines jurisdiccionales, los Juzgados y Tribunales están legitimados para el tratamiento de datos personales en base al artículo 6.1.e) del RGPD, es decir, cuando el *"tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento"*. Cuando el tratamiento engloba algún dato personal encuadrado dentro de la denominación de "categorías especiales de datos", como pueden ser los datos de salud, biométricos o genéticos, el artículo 9.2 del RGPD permite el tratamiento de estos datos cuando *"es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en el ejercicio de su función judicial"*.

Recuerde

La LOPJ (art.236 ter) descarta como base legitimadora el consentimiento

"No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba"

Por su parte, en el ámbito penal, la Ley Orgánica 7/2021, de 26 de mayo, determina también la legitimación para el tratamiento de datos personales, pero con una serie de diferencias respecto al RGPD:

- No existe un precepto similar al artículo 6 del RGPD.
- Se encuentran legitimadas aquellas que tengan la condición de autoridad competente, como las autoridades judiciales del orden penal, y realicen el tratamiento de datos con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- Para tratar categorías especiales de datos sólo cuando sea estrictamente necesario, con garantías adecuadas para los derechos y libertades del interesado y se cumpla una de estas circunstancias:
 - Previsto en una norma con rango de ley o Derecho de la Unión Europea.
 - Sea necesario para proteger intereses vitales, así como derechos y libertades fundamentales del interesado u otra persona física.
 - El tratamiento se refiere a datos que el interesado haya hecho manifiestamente públicos.

7.- DERECHOS DE PROTECCIÓN DE DATOS.

La LOPJ, el artículo 236 septies apartado 1, establece que las solicitudes del ejercicio de los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados. Estos derechos se ejercitan ante los órganos judiciales, fiscalías u oficina judicial en los que se tramita el procedimiento, siendo resuelto por quien tenga la competencia atribuida en la norma orgánica y procesal.

También procede resaltar que el propio artículo 236 septies apartado 2, determina que se negará el derecho de acceso a los datos personales objeto de tratamiento con fines jurisdiccionales cuando las diligencias judiciales en que se haya recabado la información hayan sido declaradas secretas o reservadas.

Recuerde

La [sección web](#) de la Dirección de Supervisión y Protección de Datos del CGPJ contiene un apartado dedicado a "[Derechos](#)" con modelos de formularios para ejercitar los derechos de acceso, limitación, oposición, rectificación y supresión.

Los órganos jurisdiccionales pueden poner a disposición de los interesados estos formularios para que, si así lo consideran, ejerciten sus derechos de protección de datos ante los mismos.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

En el ámbito penal, la Ley Orgánica 7/2021, de 26 de mayo, contempla que se puedan ejercitar los derechos de acceso, rectificación, limitación, y supresión.

No obstante, la norma contempla unos supuestos, aplicables también al derecho de información, en los que se puede aplazar, limitar u omitir la información, así como denegarla total o parcialmente, teniendo en cuenta los derechos fundamentales e intereses legítimos de la persona afectada, y sea necesario y proporcional para conseguir los siguientes fines:

- No obstaculizar indagaciones, investigaciones o procedimientos judiciales.
- Evitar causar perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.
- Proteger la seguridad pública, la Seguridad Nacional o los derechos y libertades de otras personas.

8.- BRECHAS DE SEGURIDAD.

Anteriormente, en el apartado de definiciones nos hemos referido a las denominadas brechas de seguridad que pueden sufrir los datos personales objeto de tratamiento. El RGPD establece en sus artículos 33 y 34, respectivamente, la obligación de notificar una brecha de seguridad de los datos personales a la autoridad de control, así como la obligación de comunicar una brecha de seguridad de los datos personales a los interesados. También lo recoge en su ámbito de aplicación, la Ley Orgánica 7/2021, de 26 de mayo, en los artículos 38 y 39.

Estas comunicaciones son también una muestra del principio de responsabilidad proactiva de los responsables del art.5.2 del RGPD, y del artículo 27 de la Ley Orgánica 7/2021, de 26 de mayo, debiendo los órganos judiciales demostrar diligencia en el tratamiento de los datos personales.

Además, de esta comunicación, de los citados preceptos se desprenden otras obligaciones como son la necesidad de documentar internamente la brecha, así como adoptar medidas para mitigar los daños que se hayan podido



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

producir, y aquellas que sean necesarias para que en el futuro no ocurran este tipo de incidentes.

Estas brechas pueden ser de tres tipos:

Tipo de brecha	Definición
Brecha de confidencialidad	<i>cuando exista una divulgación no autorizada o accidental de acceso a datos personales</i>
Brecha de disponibilidad	<i>cuando exista una pérdida accidental o no autorizada de acceso o destrucción de datos personales</i>
Brecha de integridad	<i>cuando se produce una alteración no autorizada o accidental de los datos personales.</i>

A su vez, entre los casos más comunes de brechas de seguridad se encuentran:

- Revelación verbal no autorizada;
- Documentación perdida, robada o depositada en localización insegura;
- Correo postal perdido o abierto;
- Eliminación incorrecta de datos personales en papel;
- Datos personales enviados por error de forma electrónica o en papel;
- Datos personales eliminados o destruidos;
- Abuso de privilegios de acceso por parte de miembros de la organización (p.ej. trabajadores) para extraer, reenviar o copiar datos personales;
- Datos personales residuales en dispositivos obsoletos;
- Publicación no intencionada/autorizada;
- Envío de correo electrónico a múltiples destinatarios sin copia oculta o en una lista de distribución visible;
- Dispositivo perdido o robado.

Recuerde



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

La Dirección de Supervisión y Control de Protección de Datos del CGPJ
facilita un [formulario](#) para notificar las brechas de seguridad

9.- RECOMENDACIONES.

A continuación, se ofrecen una serie de criterios, pautas y medidas a adoptar con un enfoque práctico con la finalidad de garantizar el cumplimiento de la normativa de protección de datos personales.

Principio de minimización de datos

- Verificar, antes de recabar o utilizar datos personales, que el tratamiento resulta necesario para la finalidad jurisdiccional concreta, evitando la incorporación de datos superfluos o irrelevantes al procedimiento.
- Limitar el contenido de escritos, autos y sentencias a los datos estrictamente imprescindibles para fundamentar la decisión judicial, evitando la mención innecesaria de datos personales.
- Las resoluciones judiciales objeto de publicación o difusión deben estar adecuadamente seudonimizadas, eliminando o disociando cualquier dato que permita la identificación directa o indirecta de las personas afectadas, prestando especial cautela a los procedimientos de familia, violencia de género, menores y otros especialmente sensibles.
- Adoptar medidas específicas para preservar la confidencialidad de los datos personales en la publicación de señalamientos, conforme a la normativa procesal vigente. Podrían utilizarse números, letras u otro tipo de sistema para la citación de testigos, peritos u otros, y con ello salvaguardar su identidad.

Principio de finalidad

- Utilizar los datos personales exclusivamente para el ejercicio de la función jurisdiccional, no pudiendo usarlos para finalidades distintas sin habilitación legal expresa.

Principio de integridad y confidencialidad



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- Recordar periódicamente a todo el personal del órgano judicial el deber de confidencialidad que rige durante el ejercicio de sus funciones y subsiste tras el cese.
- Recordar también a las partes, testigos, peritos, traductores y demás profesionales designados judicialmente su obligación de confidencialidad, tanto durante la actuación como con posterioridad a la misma.
- Incorporar en notificaciones y comunicaciones judiciales un aviso expreso sobre la protección de los datos personales y la obligación de preservar su confidencialidad.

Legitimación para el tratamiento de datos personales

- No realizar consultas al PNJ o a SIRAJ sin que exista resolución procesal previa que las autorice.
- Verificar, antes de cualquier comunicación o cesión de datos a otras autoridades u organismos, que existe base legal suficiente y que responde a una finalidad legítima y concreta.
- Extremar las precauciones cuando se traten categorías especiales de datos (entre ellos los relativos a salud, ideología, afiliación sindical, religión, orientación sexual, datos biométricos o genéticos) asegurando que su inclusión esté debidamente justificada.
- En procedimientos que afecten a menores de edad, víctimas de violencia de género o personas especialmente vulnerables, aplicar siempre el criterio del interés superior, reforzando las medidas de confidencialidad y seguridad.

Derecho de información de protección de datos

- Para dar cumplimiento a este derecho, al menos debe constar en la primera notificación realizada por el órgano judicial a las partes.
- En la sección web de la Dirección de Supervisión y Control de Protección de Datos se ofrece un [modelo](#) para cumplir con este derecho, y también uno [específico](#) para las sala de vistas.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

Audiencias públicas y grabaciones

- Las grabaciones de audiencias públicas se destinarán exclusivamente a finalidades jurisdiccionales.
- La seudonimización (pixelado de imágenes y distorsión de voz) será obligatoria cuando las grabaciones se utilicen con fines docentes, formativos o de difusión, preservando la identidad de las personas intervinientes.
- En el desarrollo de las vistas se recomienda emplear fórmulas neutras de llamamiento, especialmente en procedimientos sensibles.

Acceso a actuaciones por el personal del órgano judicial

- Restringir el acceso a los expedientes judiciales, tanto si se encuentran en el sistema de gestión procesal o en carpetas, exclusivamente a las personas que intervengan legítimamente en el procedimiento.
- Reflejar en las carpetas de los expedientes judiciales únicamente el número del procedimiento y el nombre del Ponente.

Información sobre procedimientos judiciales

- No facilitar información, ni presencial ni telefónicamente, sobre actuaciones judiciales a personas que no sean parte ni estén legalmente personadas, limitando además la información telefónica incluso a las partes, dada la imposibilidad de verificar con certeza la identidad del interlocutor.
- Las consultas telefónicas se limitarán a información general (existencia del procedimiento, órgano judicial, estado procesal básico).
- No se facilitarán por vía telefónica datos personales, información sensible ni el contenido de resoluciones.

Entrega de información sobre procedimientos

- Identificación del solicitante:



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- Para la entrega presencial de información será necesaria la exhibición del DNI original u otro documento oficial equivalente, sin necesidad de que se deba realizar una fotocopia.
- Solicitudes por correo electrónico:
 - No se remitirán copias de actuaciones ni información sensible al no poderse garantizar la confidencialidad.
- Acceso por terceros autorizados:
 - La autorización para el acceso de un tercero deberá ser expresa y por escrito, acompañada de copia del DNI del interesado.
 - Comprobada la autorización, se procederá a la destrucción del DNI del interesado al no ser ya necesaria.
 - El acceso se limitará estrictamente al alcance de la autorización concedida.
- Comunicaciones por correo postal:
 - Han de ir siempre en sobre cerrado.

Medidas de seguridad organizativas y técnicas

- Proteger el puesto de trabajo, bloqueando el equipo informático siempre que quede desatendido.
- Utilizar exclusivamente la cuenta de correo corporativo para comunicaciones e intercambios de información con fines profesionales.
- Acceder a sistemas y aplicaciones únicamente cuando se cuente con la autorización formal correspondiente.
- Custodiar adecuadamente los certificados digitales y tarjetas criptográficas, evitando el acceso de terceros.
- Mantener las claves de acceso como personales e intransferibles, no compartiéndolas ni revelándolas a terceros.
- Cambiar periódicamente las contraseñas y siempre que así lo solicite el sistema o la Administración.



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

- No facilitar tus contraseñas a terceros.
- No utilices ni instales programas que no hayan sido autorizados por las Administraciones prestacionales o el CGPJ. Tampoco programas que permitan el almacenamiento en la nube e igualmente no conste la citada autorización.
- Custodiar los expedientes judiciales con medidas adecuadas de seguridad, cerrando armarios y dependencias judiciales.
- Destruir o borrar de forma segura cualquier documento o soporte que contenga datos personales cuando vaya a ser desechado, impidiendo su recuperación posterior.
- Utilizar exclusivamente el correo electrónico, los equipos y programas puestos a disposición para fines profesionales.
- Solicita a tu administración prestacional que implemente las debidas medidas de seguridad.

Herramientas de inteligencia artificial

- No utilizar sistemas de inteligencia artificial que no hayan sido autorizados por las Administraciones prestacionales o el propio CGPJ.
- Para más información consulta la [Instrucción 2/2026 del CGPJ](#) sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional.

10.- RECURSOS DISPONIBLES.

La Dirección de Supervisión y Control de Protección de Datos del CGPJ cuenta con una [sección web](#) en la que se pueden consultar diferente material como las [resoluciones](#) adoptadas en el ejercicio de la actividad de inspección e investigación, así como [informes jurídicos](#) en los que se da respuesta a consultas planteadas. También se pueden encontrar [cláusulas de protección](#)



CONSEJO GENERAL DEL PODER JUDICIAL

Dirección de Supervisión y Control de
Protección de Datos

[de datos](#) dirigidas a las Administraciones prestacionales para la relación entre encargados y sub-encargados de tratamiento, y unas [nociones básicas](#) sobre seguridad, así como otros documentos a los que ya se ha hecho referencia, como los [modelos](#) para ejercitar los derechos de protección de datos, el [formulario](#) para notificar brechas de seguridad, y los modelos para cumplir con el [derecho de información](#), incluyendo en la [sala de vistas](#).

Recuerde

Conozca la [sección web](#) de la
**Dirección de Supervisión y Control de Protección de Datos del
CGPJ**