Nexo
Oposiciones

TEMA 5

PROTECCION DE DATOS Y TRANSPARENCIA

Indice:

1. Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) – pag 3

2. Principios Fundamentales de Protección de Datos – pag 4

3. Derechos de las Personas: Derechos ARSULIPO y Digitales – pag 5

4. Deberes del Personal Sanitario y Medidas de Cumplimiento en el Sector Salud – pag 7

5. Régimen Sancionador en Materia de Protección de Datos – pag 9

6. Ley 1/2014, de Transparencia Pública de Andalucía – pag 10

7. Órgano gerente: Consejo de Transparencia y Protección de Datos de Andalucía – pag 18

8. Régimen Sancionador en Materia de Transparencia – pag 18

9. Relación entre la Normativa de Protección de Datos (LOPDGDD/ RGPD) y la de Transparencia – pag 20

10. Implicaciones para el Trabajo Diario de un Profesional: Ejemplos Prácticos – pag 22

11. Referencias bibliográficas – pag 25

1. Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

Objetivos, ámbito de aplicación y relación con el RGPD

La Ley Orgánica 3/2018 (LOPDGDD) tiene por objeto adaptar el ordenamiento español al Reglamento (UE) 2016/679, conocido como RGPD, reforzando la seguridad jurídica y garantizando los derechos digitales de los ciudadanos. Esta ley orgánica deroga la anterior LOPD de 1999 e introduce novedades para adecuarse al RGPD. Ámbito de aplicación: se aplica a todos los tratamientos de datos personales de personas físicas, tanto en el sector público como en el privado, con independencia del medio (físico o digital) y del país donde estén ubicados los servidores, siempre que el responsable o encargado esté establecido en España o se traten datos en el contexto de actividades en España. Quedan excluidos únicamente los tratamientos en el marco de actividades personales o domésticas, y algunos tratamientos de seguridad nacional, defensa, etc., según el RGPD. La LOPDGDD complementa al RGPD en aspectos específicos permitidos por éste (por ejemplo, regula la edad de consentimiento digital, los derechos digitales en el entorno laboral y educativo, etc.), pero no lo reemplaza: el RGPD es directamente aplicable y la LOPDGDD lo desarrolla en ámbitos nacionales. Entre sus objetivos destacan garantizar un nivel elevado de protección de la privacidad de las personas y a la vez aportar seguridad jurídica a responsables y encargados de tratamientos de datos en España.

Relación con el RGPD europeo: El RGPD es la norma europea de referencia en protección de datos y la LOPDGDD la desarrolla en España. Por ejemplo, el RGPD permite a los Estados miembros fijar la edad mínima de consentimiento para servicios de la sociedad de la información entre 13 y 16 años: la LOPDGDD la establece en 14 años para España. Esto significa que, en general, un menor a partir de 14 años puede consentir por sí mismo el tratamiento de sus datos en Internet o en entornos digitales; por debajo de esa edad se requiere el consentimiento de padres o tutores (salvo excepciones legales). Otra especificidad nacional es el tratamiento de datos de personas fallecidas: la LOPDGDD dispone que los herederos o personas vinculadas al fallecido (por razones familiares o de hecho) pueden solicitar al responsable acceso, rectificación o supresión de los datos del difunto, salvo que éste lo hubiese prohibido expresamente antes de morir. Estas disposiciones ilustran cómo la ley española completa el marco general europeo, atendiendo a nuestra realidad jurídica.

La estructura legal de la LOPDGDD se divide en diez títulos: disposiciones generales; principios de protección de datos; derechos de las personas; disposiciones relativas al responsable y encargado del tratamiento; autoridades de control (Agencia Española de Protección de Datos y autonómicas en ciertos ámbitos); régimen sancionador; y finalmente un Título X dedicado a la garantía de los derechos digitales. Este último título incorpora derechos novedosos en la era digital (derecho a la desconexión digital laboral, educación digital, neutralidad de Internet, testamento digital, etc.) que complementan la protección de datos clásica. En resumen, la LOPDGDD persigue conjugar la adaptación al RGPD con la inclusión de garantías específicas en el entorno digital español, asegurando que el tratamiento de datos personales se haga respetando los derechos y libertades fundamentales.

2. Principios Fundamentales de Protección de Datos

La LOPDGDD reafirma los principios básicos ya establecidos por el RGPD en su artículo 5, que deben guiar cualquier tratamiento de datos personales. Estos principios fundamentales son:

- Lícitud, lealtad y transparencia: los datos deben tratarse de manera legal (con una base jurídica válida, como el consentimiento del interesado o una obligación legal), de forma leal y transparente frente al interesado. Este principio exige informar claramente a las personas sobre cómo y para qué se usarán sus datos, utilizando un lenguaje comprensible. La transparencia se garantiza, por ejemplo, mediante cláusulas informativas y la información por capas, proporcionando una primera información básica y remitiendo a información adicional más detallada.
- Limitación de la finalidad: los datos personales solo pueden recogerse con fines determinados, explícitos y legítimos, y no podrán ser luego tratados de manera incompatible con esos fines. En el sector sanitario, esto significa que los datos de un paciente se utilizan para su asistencia sanitaria y finalidades conexas (investigación con consentimiento, gestión sanitaria, etc.), pero no para propósitos ajenos (por ejemplo, no se pueden usar listados de pacientes para fines comerciales sin autorización).
- Minimización de datos: se deben tratar únicamente los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines perseguidos. “Sólo los datos que realmente se necesitan”. En la práctica sanitaria, implica no recopilar información excesiva del paciente más allá de lo requerido para su atención.
- Exactitud: los datos han de ser exactos y, si es necesario, actualizados. Se deben tomar medidas razonables para suprimir o rectificar sin dilación los datos inexactos. En un centro de salud, esto obliga a mantener actualizados los datos de contacto del paciente, sus tratamientos, etc., corrigiendo errores cuando se detecten.
- Limitación del plazo de conservación: los datos se conservarán de forma que se permita la identificación de los interesados solo durante el tiempo necesario para los fines del tratamiento. Pasado ese tiempo, deberán suprimirse o anonimizarse (salvo que deban conservarse bloqueados por obligaciones legales). En sanidad, la legislación específica (Ley 41/2002 de historia clínica, normativa autonómica) fija plazos mínimos de conservación de historias clínicas (en Andalucía, al menos 5 años desde el alta, y más para ciertos documentos), pero una vez cumplidos, los datos deben eliminarse o despersonalizarse.
- Integridad y confidencialidad: se exige garantizar la seguridad adecuada de los datos personales, incluida su protección contra el tratamiento no autorizado o ilícito, la pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas. Esto abarca desde medidas informáticas (cifrado, contraseñas, copias de seguridad) hasta medidas organizativas (protocolos de acceso a historiales, armarios bajo llave para expedientes en papel, etc.). En sanidad, donde se tratan datos especialmente sensibles de salud, este principio es crucial: la información médica debe custodiarse con riguroso secreto profesional y altos estándares de seguridad.
- Responsabilidad proactiva (accountability): principio introducido por el RGPD, obliga al responsable del tratamiento a demostrar el cumplimiento de la normativa. No basta con cumplir, sino que hay que documentarlo y probarlo (mediante evaluaciones de impacto, registros de actividades de tratamiento, políticas de privacidad, designación de Delegado de Protección de Datos, etc.). Por ejemplo, un hospital debe tener registrado qué tratamientos

de datos realiza (historias clínicas, investigación, gestión de personal...), haber analizado los riesgos, implantado medidas de seguridad y poder evidenciar ante la AEPD que cumple la normativa.

Estos principios rigen todas las actuaciones con datos personales. Su infracción constituye a menudo una infracción grave o muy grave. Por ejemplo, usar datos para una finalidad distinta a la informada y sin base jurídica es una vulneración del principio de finalidad y podría considerarse infracción muy grave.

En resumen, cualquier profesional sanitario debe conocer y aplicar estos principios: recoger solo la información necesaria del paciente, con su debida información y consentimiento (u otra base legal), usarla únicamente para su atención o fines autorizados, mantenerla exacta, guardarla con seguridad y destruirla o archivarla anonimizada cuando ya no corresponda conservarla.

3. Derechos de las Personas: Derechos ARSULIPO y Digitales

La normativa reconoce al ciudadano una serie de derechos sobre sus datos personales, que en el RGPD/LOPDGDD se enumeran a menudo con el acrónimo "ARSULIPO": son los derechos de Acceso, Rectificación, Supresión (derecho al olvido), Limitación del tratamiento, Portabilidad de los datos y Oposición. A estos se suman el derecho a no ser sometido a decisiones automatizadas sin intervención humana (incluyendo perfiles) y, en contextos de servicios de la sociedad de la información, el derecho a retirar el consentimiento en cualquier momento. Veamos en qué consiste cada uno de los principales derechos personales:

- Derecho de acceso: El interesado puede solicitar al responsable si está tratando o no sus datos personales, y en caso afirmativo, obtener copia de dichos datos y información sobre las finalidades, categorías de datos, destinatarios a quienes se comunican, plazo de conservación, origen de los datos, etc. En sanidad, un paciente tiene derecho a acceder a su historia clínica completa 10 (salvo anotaciones subjetivas de profesionales o datos de terceros que figuren en ella). El acceso debe proporcionarse de forma comprensible y, preferiblemente, por medios electrónicos seguros si se solicita así, en el plazo máximo de un mes.
- Derecho de rectificación: Es el derecho a corregir datos inexactos o incompletos. El interesado puede pedir que se modifiquen sus datos personales erróneos. En contexto sanitario, si un paciente detecta un error en su información (por ejemplo, fecha de nacimiento mal registrada, o una alergia mal anotada), puede solicitar la rectificación aportando la documentación adecuada. Cabe señalar que en historia clínica, los profesionales tienen el deber de rectificar datos clínicos erróneos, aunque no se borran las entradas originales sino que se deja trazabilidad de la corrección.
- Derecho de supresión ("derecho al olvido"): Permite pedir la eliminación de los datos personales del interesado cuando, entre otras causas, ya no sean necesarios para la finalidad para la que se recogieron, o se haya retirado el consentimiento, o se han tratado ilícitamente. El derecho al olvido es la manifestación de la supresión aplicado a buscadores de Internet (por ejemplo, pedir a Google que desindexe resultados con nuestros datos personales). En sanidad, este derecho tiene limitaciones: no se puede suprimir una historia clínica mientras

deba conservarse para garantizar la asistencia sanitaria adecuada o por imperativo legal. La Ley 41/2002 impide destruir información clínica antes de ciertos plazos, y prevalece la seguridad del paciente. Por ello, en la práctica los datos de salud no se eliminan a simple petición; a lo sumo se bloquean al concluir los plazos de conservación (quedan inaccesibles salvo para fines legales, administrativos o judiciales).

- Derecho de limitación del tratamiento: Es un derecho menos conocido, que permite al interesado solicitar que se "congelen" sus datos, es decir, que no se apliquen a determinados tratamientos en supuestos concretos, por ejemplo mientras se verifica la exactitud de los datos cuya rectificación se ha solicitado, o cuando el tratamiento sea ilícito pero la persona prefiere la limitación a la supresión. En la práctica, limitar significa marcar esos datos para que solo sean tratados para ciertas finalidades legitimadas (p.ej. defensa de reclamaciones) mientras dure la limitación.
- Derecho de portabilidad: Introducido por el RGPD, permite al interesado recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable sin impedimentos. Aplica a datos tratados por medios automatizados con base en el consentimiento o en un contrato. En salud podría permitir, por ejemplo, que un paciente obtenga sus datos médicos en formato electrónico interoperable para llevarlos a otro proveedor sanitario (aún es un reto técnico, pero es la idea).
- Derecho de oposición: La persona puede oponerse a ciertos tratamientos de sus datos cuando la base jurídica sea interés público o interés legítimo del responsable (incluyendo elaboración de perfiles). Al oponerse, el responsable debe cesar el tratamiento salvo que demuestre motivos imperiosos que prevalezcan sobre los intereses o derechos del interesado. En ámbito sanitario público, es poco frecuente oponerse a tratamientos necesarios para la atención (ya que suelen basarse en obligación legal o interés público en sanidad), pero podría darse en, por ejemplo, uso de datos con finalidades de investigación o docencia: el paciente podría oponerse si no dio consentimiento y el hospital alega interés legítimo. También el RGPD otorga al interesado derecho a oponerse en cualquier momento al procesamiento de sus datos con fines de marketing directo aunque esto no es habitual en un entorno asistencial público.

El ejercicio de estos derechos es gratuito para el ciudadano y debe canalizarse ante el responsable del tratamiento (hospital, centro de salud, etc.), quien tiene la obligación de facilitar su ejercicio con procedimientos sencillos (por ejemplo, formularios accesibles). La LOPDGDD aclara que cada derecho es independiente, no se puede, por ejemplo, exigir que se ejerza primero el acceso para luego atender la supresión y que el responsable puede negarse a actuar solo si la petición es manifiestamente infundada o excesiva (por carácter repetitivo, etc.), en cuyo caso puede incluso cobrar un canon razonable o rechazarla, pero recae sobre el responsable la carga de demostrar ese carácter excesivo. En general, el responsable debe responder en el plazo máximo de un mes (prorrogable a dos en casos complejos, informando al interesado). Si no responde en plazo, se considera denegado por silencio negativo y el ciudadano puede reclamar.

Además de estos derechos "clásicos", la LOPDGDD, en su título final, reconoce derechos digitales de nueva generación que afectan también a trabajadores y usuarios en entornos digitales. Algunos relevantes para un profesional sanitario como empleado público serían:

- Derecho a la desconexión digital en el ámbito laboral: Los trabajadores tienen derecho a no responder comunicaciones (emails, llamadas) fuera de su jornada laboral, para garantizar su tiempo de descanso y conciliación. En la práctica, el Servicio Andaluz de Salud debe evitar requerir la atención del profesional fuera de su horario salvo urgencia justificada, y ha de establecer políticas internas que respeten este derecho.
- Derecho a la intimidad y uso de dispositivos digitales en el trabajo: La ley establece que los empleadores (incluido SAS) pueden monitorizar herramientas digitales corporativas (correo, equipos) para asegurar la productividad y seguridad, pero deben hacerlo respetando la intimidad del trabajador. Deben definir criterios de uso aceptable e informar previamente de cualquier control. Por ejemplo, si un hospital instala videovigilancia, debe informar a los empleados y solo usar las cámaras para finalidades legítimas (seguridad, no para grabar zonas privadas como vestuarios).
- Garantía de derechos digitales en la salud: La LOPDGDD no los detalla específicamente, pero podríamos mencionar el derecho a la educación digital (que implica que los profesionales también reciban formación en competencias digitales, algo cada vez más necesario con la historia clínica electrónica, telemedicina, etc.) y el testamento digital, por el cual cualquier persona puede organizar el destino de sus datos digitales (por ejemplo, redes sociales) tras su fallecimiento. En entornos sanitarios, el testamento digital podría incluir instrucciones sobre qué hacer con la historia clínica tras la muerte, aunque la ley de autonomía del paciente ya permite designar un representante para decisiones clínicas anticipadas.

4. Deberes del Personal Sanitario y Medidas de Cumplimiento en el Sector Salud

En el entorno sanitario, los datos personales (especialmente los relativos a la salud) son de categoría especial, lo que exige medidas reforzadas de protección. Para un profesional, varios deberes se derivan de la normativa:

- Deber de secreto y confidencialidad: Es quizás el más importante. Todos los profesionales sanitarios, están legalmente obligados a mantener la confidencialidad sobre la información de salud de los pacientes a la que acceden en su trabajo. Este deber proviene tanto de la LOPDGDD (art. 5.1.f, integridad y confidencialidad) como de la Ley 41/2002 básica reguladora de la autonomía del paciente, e incluso del código deontológico. Implica no divulgar datos clínicos a terceros no autorizados, no comentar casos identificables fuera del entorno asistencial, y custodiar adecuadamente historias y documentos para que no los vean personas ajenas. Por ejemplo, no dejar a la vista de otros pacientes o visitantes el listado con nombres y diagnósticos, ni hablar de la situación de un paciente concreto con su familia sin permiso del paciente, etc. Este deber perdura incluso después de que el profesional deje su puesto de trabajo. Su incumplimiento puede conllevar sanciones disciplinarias e incluso responsabilidad penal (revelación de secretos). Muchas instituciones requieren que el personal firme compromisos de confidencialidad al incorporarse.
- Obtención legítima y uso adecuado de los datos: El personal sanitario debe asegurarse de que los datos de los pacientes se recaban con base jurídica adecuada (generalmente, el tratamiento de datos de salud se ampara en la necesidad para la prestación de asistencia sanitaria, en un contexto de interés público en el ámbito de la salud, y en el consentimiento

implícito del paciente al proporcionar su información para ser atendido). En ciertas situaciones se requiere consentimiento explícito del paciente: por ejemplo, para usar sus datos o imagen en materiales docentes, en estudios de investigación no amparados por normativa, o para fines de ensayo clínico. Un profesional debe verificar que cuenta con la debida autorización antes de, por ejemplo, divulgar una fotografía del paciente (lo cual, de hecho, suele estar prohibido salvo fines clínicos estrictos).

- Calidad y exactitud de los datos: Los profesionales deben contribuir a que la información registrada sea exacta y actual. Por ejemplo, si un profesional advierte que los datos personales de un paciente (nombre, fecha de nacimiento, etc.) están mal escritos en su pulsera identificativa o en la ficha, debe corregirlo o informarlo para rectificación, en línea con el principio de exactitud. También deben evitar la acumulación de datos irrelevantes en la historia.
- Seguridad de la información: Los centros sanitarios implementan políticas y medidas (contraseñas, perfiles de acceso, cifrado de dispositivos, protocolos de backup, etc.), pero el personal en su día a día debe cumplirlas rigurosamente. Esto incluye: utilizar sus credenciales personales y no compartirlas; no acceder a historias clínicas de pacientes por simple curiosidad o sin que medie una necesidad asistencial (queda registrado quién accede a qué historia, y un acceso indebido es infracción grave); no dejar sesiones abiertas en el ordenador con datos visibles; manejar con cuidado los documentos en papel (expedientes, peticiones) y depositarlos en contenedores seguros para destrucción una vez usados; no sacar información fuera del centro sin autorización; y en general prevenir brechas de seguridad. Si ocurriera un incidente o brecha de seguridad (p. ej., se extravía un informe con datos de pacientes, o alguien accede indebidamente a un registro), existe la obligación de notificarlo a la autoridad de protección de datos (AEPD) en 72 horas y a los afectados si supone un riesgo para sus derechos. El profesional debe informar inmediatamente a sus superiores o al Delegado de Protección de Datos del centro si detecta una posible brecha (por ejemplo, la pérdida de un listado de pacientes) para que se tomen acciones correctivas y se notifique según proceda.
- Designación del Delegado de Protección de Datos (DPD/DPO):Es importante saber que los centros sanitarios están obligados por la LOPDGDD a nombrar un Delegado de Protección de Datos. Este DPD actúa como garante interno de la privacidad: supervisa el cumplimiento, forma al personal, atiende consultas y reclamaciones sobre datos. Un profesional puede acudir al DPD de su hospital si tiene dudas sobre cómo manejar cierta información o para reportar cualquier incidencia en materia de datos personales.
- Formación y concienciación: Los profesionales sanitarios deben formarse periódicamente en protección de datos. Muchos hospitales imparten cursos o manuales de buenas prácticas (por ejemplo, cómo responder cuando un paciente ejerce sus derechos, cómo evitar phishing o ataques informáticos, etc.). Estar al día en estas políticas es tanto un deber profesional como una salvaguarda para el propio trabajador.

En esencia, para un profesional proteger los datos significa proteger la confianza que el paciente deposita en el sistema sanitario. La intimidad del paciente es un derecho esencial en la relación asistencial, por lo que todas estas obligaciones desde guardar secreto hasta asegurar los historiales forman parte de la ética y de la legalidad. El personal, al tener acceso directo a información muy sensible (diagnósticos, tratamientos, vida privada reflejada en la

historia), tiene la responsabilidad de actuar con máxima prudencia y respeto a la privacidad.

5. Régimen Sancionador en Materia de Protección de Datos

El incumplimiento de la normativa de protección de datos puede acarrear sanciones muy severas. El RGPD establece multas administrativas de hasta 20 millones de euros o el 4% de la facturación global de una empresa (la cifra que resulte mayor) para las infracciones más graves. La LOPDGDD, por su parte, clasifica las infracciones en leves, graves y muy graves (siguiendo la tradición de la antigua LOPD) y prevé sanciones acordes a esa graduación, aunque supeditadas a los límites del RGPD. Por ejemplo, constituyen infracciones muy graves: vulnerar los principios básicos (como tratar datos sin base legal, o con fines ilícitos), tratar categorías especiales de datos (salud, origen étnico, ideología, etc.) sin autorización, ceder datos sin legitimación, obstaculizar de forma reiterada el ejercicio de derechos ARSULIPO, incumplir las resoluciones de la AEPD, o no atender los deberes de confidencialidad y seguridad. Las graves incluyen, entre otras, no nombrar DPD cuando es obligatorio, no realizar evaluaciones de impacto cuando proceda, no notificar brechas de seguridad, o tratar datos de menores de 14 años sin el consentimiento adecuado. Las leves podrían ser, por ejemplo, no informar completamente al interesado (incumplir el deber de información) o pequeñas demoras en atender derechos. Las multas se gradúan según múltiples criterios: gravedad, duración, número de afectados, medidas preventivas tomadas, reincidencia, etc.

Particularidad en el sector público: La LOPDGDD introdujo un régimen especial: para las Administraciones Públicas (Estado, CCAA, entidades locales) en caso de infracción, la Agencia de Protección de Datos no impondrá multas dinerarias, sino que sancionará mediante apercibimiento (advertencia) y ordenará las medidas correctoras oportunas. Es decir, a un hospital público o consejería de salud no se le va a multar con dinero (lo que en el fondo repercutiría en el erario público), sino que se le requerirá que corrija la infracción. No obstante, si esa Administración no atiende el apercibimiento, entonces sí podrían imponerse sanciones coercitivas o informarse a las autoridades de control. Esta diferenciación ha generado debate, pues se quiere evitar impunidad en el sector público. En cualquier caso, el hecho de que no haya multa económica directa no exime de responsabilidad: un centro sanitario público apercibido verá publicado ese apercibimiento, con el consiguiente daño reputacional, y además deberá cumplir estrictamente las medidas ordenadas por la AEPD. Adicionalmente, en el ámbito interno, cuando la infracción sea imputable a una acción u omisión dolosa o negligente de empleados, puede iniciarse responsabilidad disciplinaria contra los implicados. Un profesional que, por ejemplo, filtrara expedientes de pacientes en redes sociales se expondría no solo al apercibimiento de la AEPD al Servicio Andaluz de Salud, sino a un expediente disciplinario grave que podría conllevar suspensión o incluso despido, y eventualmente a denuncias penales de los afectados.

Resumiendo, el régimen sancionador busca fomentar el cumplimiento más que recaudar, especialmente en lo público. Pero las consecuencias de vulnerar la normativa de protección de datos son importantes: en lo organizativo, obliga a corregir procedimientos; en lo económico, puede suponer multas cuantiosas a entidades privadas; y en lo personal, puede implicar sanciones laborales e incluso delitos (el Código Penal castiga el descubrimiento y revelación de secretos, art. 197). Por ello, la cultura de cumplimiento (auditorías, formación, DPD, etc.) es esencial en las instituciones sanitarias para evitar llegar a ese escenario.

6. Ley 1/2014, de Transparencia Pública de Andalucía

Objetivos y ámbito de aplicación

La Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (LTPA), tiene como finalidad principal garantizar la transparencia de la actividad de los poderes públicos andaluces, fomentar la participación y el control ciudadanos, e instaurar obligaciones de buen gobierno. Es una ley autonómica que desarrolla y amplía en el ámbito andaluz la normativa básica estatal (Ley 19/2013, de transparencia, acceso a la información y buen gobierno). Sus objetivos fundamentales son: acercar la gestión pública a la ciudadanía mediante la publicidad activa de información relevante, reconocer el derecho de acceso a la información pública a cualquier persona, y establecer mecanismos para promover la cultura de transparencia (formación, difusión) y para asegurar su cumplimiento (un órgano de control y un régimen sancionador). Todo ello se orienta a lograr una Administración más abierta, responsable y sometida al escrutinio público, lo cual redunda en prevenir la corrupción y mejorar la eficiencia y legitimidad de lo público.

Ámbito subjetivo de aplicación: La ley se aplica a un amplio conjunto de sujetos en la Comunidad Autónoma de Andalucía. En primer lugar, abarca a la Administración de la Junta de Andalucía y su sector público instrumental (agencias, empresas públicas, fundaciones, consorcios, etc. de la Junta). También incluye a las entidades locales andaluzas (ayuntamientos, diputaciones) y a sus entes dependientes, en lo relativo a sus competencias propias (aunque la normativa básica ya obligaba a entes locales, Andalucía puede añadir obligaciones adicionales). Además, la ley alcanza a otras instituciones autonómicas: el Parlamento de Andalucía, el Defensor del Pueblo Andaluz, la Cámara de Cuentas, el Consejo Audiovisual, universidades públicas andaluzas, etc., en cuanto a sus actividades sujetas a derecho público. Importante: la ley extiende ciertas obligaciones a personas o entidades privadas que, sin ser Administración, reciben fondos públicos o ejercen funciones públicas. En concreto, el art. 5 incluye como sujetos obligados: partidos políticos, organizaciones sindicales y empresariales en Andalucía (por su financiación pública), así como cualquier entidad privada que perciba subvenciones o ayudas públicas relevantes o gestione servicios públicos por concesión/contrato. Estas entidades deben suministrar información relativa a los fondos públicos percibidos y su gestión. En resumen, el ámbito es amplio: prácticamente cualquier institución pública andaluza y quienes se vinculan a recursos públicos están obligados por la ley de transparencia.

Para un profesional, esto significa que su propio empleador (el Servicio Andaluz de Salud, perteneciente a la Junta) está sujeto a la ley. La transparencia afecta a información de los centros sanitarios públicos (por ejemplo, la Cartera de Servicios, las listas de espera, memorias anuales, contratos de suministro, etc.), y también a cierta información de personal (puestos directivos, retribuciones de altos cargos, ofertas de empleo, procesos selectivos, etc.). Más adelante detallaremos qué información concreta debe ser publicada.

Principios básicos de la transparencia pública

El artículo 6 de la LTPA establece los principios generales que inspiran la transparencia. Estos principios orientan tanto la interpretación de la ley como la actuación de los sujetos obligados. Son

los siguientes:

- Principio de transparencia: Regla general de publicidad de la información pública. Toda la información en poder de sujetos obligados se presume accesible y solo podrá retenerse o reservarse por motivos legítimos previstos en la ley (protección de otros derechos o intereses, ver límites más adelante). Por tanto, la excepción es la opacidad; la norma es la apertura informativa.
- Principio de libre acceso: Cualquier persona puede acceder a la información pública, sin necesidad de justificar interés ni motivar su solicitud. La transparencia se concibe como un derecho universal.
- Principio de responsabilidad: Los sujetos obligados (y sus directivos/empleados) son responsables de cumplir las obligaciones de transparencia. Deben rendir cuentas y asumir consecuencias si no lo hacen. Este principio enlaza con el régimen sancionador y con la noción de accountability en la gestión pública.
- Principio de no discriminación tecnológica: La información debe ofrecerse de modo que no excluya a nadie por razones tecnológicas. Esto implica usar estándares abiertos y formatos accesibles a distintos sistemas y dispositivos, evitando requerir tecnología propietaria para acceder.
- Principio de veracidad: La información pública difundida debe ser cierta, exacta y actualizada. No se puede publicar datos incorrectos o desfasados que induzcan a error. Por ejemplo, si se publican las listas de espera sanitarias, deben reflejar fielmente la situación real en las fechas indicadas.
- Principio de utilidad: La información publicada ha de ser relevante y útil para la ciudadanía, facilitando el conocimiento de la gestión pública. No se trata de publicar por publicar, sino aquello cuyo conocimiento sea significativo para controlar la actuación pública.
- Principio de gratuidad: El acceso a la información será gratuito (salvo, a lo sumo, el costo de reproducción de copias o soportes si se piden en formato físico). No se puede cobrar tasas por ejercer el derecho de acceso.
- Principio de simplicidad y comprensión: La información se presentará de forma clara, estructurada y comprensible para el público general. Se deben evitar tecnicismos innecesarios y, en su caso, acompañar los datos con explicaciones o contextos que faciliten su entendimiento.
- Principio de accesibilidad universal: Se garantizará que la información esté disponible de manera accesible para todas las personas, incluidas aquellas con discapacidad. Esto implica publicar en formatos que cumplan estándares de accesibilidad web (por ejemplo, PDF etiquetados, texto alternativo en imágenes, etc.) y garantizar que quien tenga discapacidad pueda ejercer el derecho de acceso con apoyos.
- Principio de interoperabilidad y reutilización: La información pública debe ofrecerse en formatos abiertos y estructurados que permitan su reutilización por terceros y la interconexión entre sistemas. Por ejemplo, publicar datos en CSV, JSON o XML antes que en PDFs cerrados, para que puedan ser analizados y reutilizados fácilmente (open data). La ley promueve que los datos se puedan cruzar y aprovechar por la sociedad civil, empresas, etc., generando valor añadido.

Estos principios crean el marco de cómo se debe llevar a cabo la transparencia. Para el personal sanitario, implican que la Administración sanitaria (hospitales, distritos, SAS central) debe actuar siguiendo estas pautas: divulgar información veraz y relevante sobre la sanidad andaluza, mantenerla actualizada, facilitar su acceso sin trabas tecnológicas, y ser proactiva en la rendición de cuentas.

Derechos de los ciudadanos en materia de transparencia

La ley reconoce a cualquier ciudadano una serie de derechos asociados a la transparencia (art. 7). Son cuatro derechos fundamentales:

- Derecho a la publicidad activa: Es el derecho a que las instituciones públicas publiquen de forma periódica y actualizada la información cuya difusión sea relevante para garantizar la transparencia de su actividad 26 . En otras palabras, el ciudadano tiene derecho a que la Administración publique por iniciativa propia información esencial sobre su organización, funcionamiento y resultados, sin necesidad de que alguien la solicite. Este derecho se plasma en las obligaciones de publicidad activa que veremos (por ejemplo, un ciudadano tiene derecho a encontrar en la web del SAS datos sobre la estructura del servicio de salud, las listas de espera, las memorias de actividad, etc., porque la ley obliga a publicarlos).
- Derecho de acceso a la información pública: Es el derecho de cualquier persona a solicitar y obtener información pública en los términos previstos en la ley 27 . Cubre los documentos y contenidos que obren en poder de las entidades obligadas, y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones. Este derecho permite al ciudadano preguntar prácticamente cualquier cosa sobre la gestión pública (por ejemplo: estadísticas de un hospital, criterios de contratación, actas de procesos selectivos, gasto en medicamentos, etc.) y, salvo que concurra alguna limitación, la Administración debe proporcionarle dicha información. El solicitante no está obligado a motivar la solicitud, y puede presentarla por medios electrónicos o físicos según se habilite.
- Derecho a obtener una resolución motivada en caso de restricciones: Esto significa que si alguien solicita acceso a una información y la Administración decide denegarlo (total o parcialmente) o bien proporcionar la información de un modo distinto al pedido, dicha resolución debe ser expresamente motivada. El ciudadano tiene derecho a saber las razones de una denegación (por ejemplo, que tal información está protegida por la ley de datos personales, o por secreto comercial, etc.), o de una inadmisión (por ejemplo, la petición es imprecisa o ya fue resuelta previamente), y esa respuesta debe citar los preceptos legales aplicables. También si le conceden solo una parte de lo pedido o le ofrecen consulta in situ en vez de copias, todo ello debe justificarse. Este derecho a una resolución motivada refuerza las garantías procedimentales y facilita que el ciudadano pueda, con conocimiento de causa, recurrir si no está conforme.
- Derecho al uso libre de la información obtenida: Cualquier información pública obtenida por un ciudadano, ya sea vía publicidad activa o por solicitud de acceso, puede ser utilizada libremente sin necesidad de autorización previa 29 . Solo se le pueden imponer las limitaciones derivadas de esta u otras leyes, por ejemplo, respetar la protección de datos personales o citar la fuente. Pero en general, el ciudadano puede reutilizar los datos en investigaciones, artículos, aplicaciones, etc. Este derecho entronca con la filosofía de datos abiertos (open data): lo público, una vez publicado, puede ser aprovechado por la sociedad.

Todos estos derechos de transparencia cuentan con el respaldo de un órgano garante: el Consejo de Transparencia y Protección de Datos de Andalucía, creado por la misma ley para velar por su cumplimiento. Si un ciudadano ve vulnerado su derecho (por ejemplo, no le responden a tiempo, o le deniegan información sin justificación válida), puede presentar una reclamación ante el Consejo para que éste revise el caso y, en su caso, ordene a la Administración entregar la información.

Conviene destacar que el ejercicio del derecho de acceso está sujeto a ciertas obligaciones del solicitante (art. 8) pensadas para evitar abusos. Entre ellas: actuar de buena fe (no inundar de solicitudes malintencionadas), concretar lo más posible la petición para no entorpecer gravemente el servicio público, respetar las normas sobre reutilización de la información (por ejemplo, no alterar su sentido), y cumplir las condiciones materiales que se establezcan para el acceso presencial (si se consulta in situ un archivo). Son requisitos de sentido común para un uso responsable del derecho.

Para un profesional, estos derechos de la ciudadanía significan que ha de existir una actitud colaborativa desde el sistema sanitario: si un paciente u otra persona solicita información pública (no datos personales privados, sino información administrativa), el personal debe orientar y ayudar en lo posible. De hecho, la ley (art. 31) impone el deber de auxilio y colaboración: todos los empleados públicos deben ayudar a los solicitantes indicándoles cómo y dónde pueden presentar sus solicitudes, especialmente si tienen discapacidad o dificultades. Por ejemplo, si alguien pregunta en Admisión de un hospital cómo conseguir los datos de infecciones nosocomiales del centro, el personal debería dirigirle al portal de transparencia o al departamento correspondiente, en lugar de simplemente ignorar la petición.

Publicidad activa: obligaciones de publicación de información

La publicidad activa es uno de los ejes centrales de la Ley 1/2014. Obliga a los sujetos incluidos en su ámbito a publicar de oficio una amplia variedad de información, de manera periódica, actualizada, clara y accesible, sin necesidad de petición previa por parte de la ciudadanía. El Título II de la ley detalla estas obligaciones. Enumeraremos las principales categorías de información que deben ser publicadas (normalmente en los portales web de transparencia):

- Información institucional y organizativa (Art. 10): Estructura orgánica de cada consejería, hospital u organismo (organigramas, funciones de cada unidad); la normativa que les es de aplicación; su ubicación, horarios de atención al público, datos de contacto y medios de participación ciudadana. En el caso del SSPA (Servicio Sanitario Público Andaluz), esto implica publicar la estructura del SAS, de cada Área Sanitaria, los organigramas de hospitales, con indicación de responsables de unidades.
- Información sobre altos cargos y responsables (Art. 11): Identidad y perfil de los altos cargos o directivos (por ejemplo, el Director Gerente de un hospital), incluyendo su biografía profesional, funciones y retribuciones anuales que perciben, dietas, indemnizaciones si las hay, así como las declaraciones de bienes, intereses o actividades que pudieran causar conflicto de interés. Esta es información sensible pero la ley obliga a publicarla por transparencia. También se deben publicar los empleados eventuales o de confianza y sus retribuciones.
- Información de relevancia jurídica (Art. 13): Las disposiciones normativas en trámite (proyectos de ley, reglamentos) con documentación relevante; también los documentos que deban someterse a información pública; y las resoluciones administrativas que afecten a derechos e intereses colectivos (salvaguardando datos personales). Por ejemplo, la

Consejería de Salud debe publicar los anteproyectos de ley sanitaria, o un hospital podría publicar sus protocolos si son de interés general.

- Información sobre planificación y evaluación (Art. 12): Planes y programas anuales o plurianuales (por ejemplo, el Plan Andaluz de Salud, planes estratégicos de un hospital) junto con el grado de cumplimiento y evaluación de resultados de dichos planes. También se incluyen aquí indicadores de calidad y resultados de servicios públicos. En salud, podría implicar publicar indicadores asistenciales, encuestas de satisfacción, etc.
- Información económica, financiera y presupuestaria (Art. 16): Los presupuestos anuales (desglosados por programas, capítulos, etc.), con sus actualizaciones y estados de ejecución periódica; las cuentas anuales, informes de auditoría y fiscalización (por ejemplo, informes de la Cámara de Cuentas sobre el SAS); información detallada sobre la deuda pública andaluza y sus indicadores; gastos de personal (coste global, por categorías). Los hospitales públicos deben publicar datos de su presupuesto y ejecución, al menos agregados.
- Información sobre contratos, convenios y subvenciones (Art. 15): Todos los contratos formalizados por la Administración andaluza y entes obligados, con indicación del objeto, importe de adjudicación, procedimiento empleado, adjudicatario, duración, etc. Igualmente, los convenios suscritos con terceros (p. ej. un convenio de colaboración entre el SAS y una universidad) y las encomiendas de gestión. Y las subvenciones y ayudas públicas concedidas: indicando beneficiarios, importe, objetivo, y procedimiento de concesión. Esto supone que, por ejemplo, el SAS publique las licitaciones de suministros médicos, las adjudicaciones de obras sanitarias, los conciertos con clínicas privadas, así como las subvenciones otorgadas a asociaciones de pacientes, ONGs en salud, investigación, etc.
- Información sobre procedimientos y servicios (Art. 14): Se debe dar publicidad a los procedimientos administrativos más importantes: cartas de servicios, formas de participación ciudadana, procedimientos de quejas y sugerencias, etc. En sanidad, esto implica tener accesible información sobre cómo acceder a los servicios de salud, cómo presentar reclamaciones sanitarias, derechos del paciente, etc. También los requisitos y trámites para acceder a prestaciones (por ejemplo, cómo solicitar una segunda opinión médica, cómo tramitar la tarjeta sanitaria europea).
- Información sobre personal y recursos humanos: Aunque la ley no lo lista como categoría separada, en la práctica incluye publicar las ofertas de empleo público, las convocatorias de oposiciones o bolsas (esto se suele enlazar al portal de empleo público), así como estadísticas de personal. Por transparencia, muchos portales publican el número de empleados por categorías, los acuerdos con sindicatos, etc. También se publica el catálogo de puestos de trabajo y la relación de puestos (en Junta).
- Información sobre bienes y patrimonio: La ley estatal obligaba a publicar el inventario de bienes inmuebles de la Administración. Andalucía seguramente publica listados de edificios públicos, terrenos, etc., a disposición pública. En sanidad, esto equivale a saber qué hospitales, centros de salud, etc. son propiedad del SAS, cuáles alquilados, etc.
- Información medioambiental: Si bien hay normativa específica (Ley 27/2006), también entra en transparencia: datos sobre calidad ambiental, control sanitario ambiental, etc., en lo que afecte a la Junta.

La ley indica que esta información de publicidad activa debe publicarse de forma clara,

estructurada, comprensible y reutilizable, en las sedes electrónicas, portales web o páginas correspondientes 34 . Debe actualizarse periódicamente: con carácter general, al menos trimestralmente 35 (salvo que normativa específica fije otro plazo). Además, toda la información debe ser accesible para personas con discapacidad y presentarse con lenguaje no sexista ni discriminatorio, cuidando la perspectiva de género en la redacción. Un punto crítico: cuando la información a publicar contenga datos personales especialmente protegidos (p. ej., salud, ideología, etc.), solo se podrá hacer pública previa disociación de los datos personales 37 . Es decir, hay que anonimizar o eliminar cualquier dato que identifique a la persona antes de publicar el documento. Esto refleja la necesaria armonización con la protección de datos: por transparencia se pueden, por ejemplo, publicar listas de subvenciones con nombres de beneficiarios salvo que sean datos sensibles que deban protegerse (como podría ser una ayuda por razón de salud). En caso de datos personales no especialmente sensibles, la publicación debe respetar la normativa de protección de datos y, en general, la política seguida es publicar nombres y apellidos de altos cargos y personas en función pública, pero no de ciudadanos particulares salvo que esté justificado.

Para el Servicio Andaluz de Salud, estas obligaciones se traducen en que debe mantener un Portal de Transparencia (integrado en el de la Junta o propio) donde se vuelque toda esta información. De hecho, la Junta de Andalucía tiene su Portal de Transparencia donde se encuentran, en el apartado de Salud, muchas de estas publicaciones: memorias del SAS, datos de listas de espera quirúrgicas, concertaciones, contratos de suministro de medicamentos, etc. Un TCAE no será quien suba estos datos (eso corresponde a unidades administrativas específicas), pero conviene que conozca qué tipo de información de su centro es pública. Por ejemplo, las ratios de enfermeras/TCAE por paciente, los tiempos de espera en urgencias, las encuestas de satisfacción de pacientes, etc., podrían ser objeto de publicidad activa si se consideran relevantes para evaluar la calidad asistencial. Así la ciudadanía puede conocer cómo funciona el sistema de salud y comparar.

El derecho de acceso a la información pública: procedimiento y límites

Junto a la publicidad activa, el otro gran pilar es el derecho de acceso. Cualquier persona puede solicitar información pública que no encuentre publicada o que sea más específica. La Ley 1/2014 regula el procedimiento de acceso, que en términos generales sigue la Ley estatal 19/2013 pero con algunos matices:

- Solicitud: El ciudadano dirige una solicitud identificando la información que quiere. No está obligado a explicar para qué la quiere (no se exige motivación). La solicitud se puede presentar por medios electrónicos (preferentemente, a través del portal de transparencia o registros telemáticos) o en papel en cualquier registro oficial. Debe dirigirse al órgano que posea la información si se conoce; si no, cualquier órgano la debe tramitar internamente.
- Plazo de resolución: La Administración debe resolver y notificar lo antes posible. El plazo máximo en Andalucía es similar al estatal: 1 mes desde la recepción de la solicitud en el registro del órgano competente. Cabe prorrogar excepcionalmente otro mes (2 meses en total) si la información o su compilación es muy voluminosa o compleja, notificando la prórroga al solicitante. En la práctica, en el ámbito del Servicio de Salud, existe el compromiso de responder en plazo y a menudo se hace antes si la información es sencilla. Si transcurre el plazo sin respuesta, la solicitud se entiende desestimada por silencio administrativo (silencio negativo), lo que faculta al interesado a recurrir.

- Límites al acceso: No toda la información es accesible. La ley establece límites para proteger otros bienes jurídicos. Los límites más comunes son: la seguridad y defensa del Estado, la seguridad pública, la prevención y sanción de delitos, los secretos oficiales, la protección de datos personales, la propiedad intelectual o industrial, el secreto comercial y económico, la confidencialidad de procedimientos abiertos, y la garantía de la igualdad de las partes en procesos judiciales. En contexto sanitario, los límites más relevantes suelen ser protección de datos personales y secreto comercial. Por ejemplo, si alguien pidiera "historias clínicas de pacientes atendidos en tal hospital", se denegaría por afectar a datos personales y al deber de confidencialidad médica. Si pide el contrato con una empresa proveedora de prótesis, podría facilitarse pero quizás tachando datos confidenciales comerciales (precios desglosados si revelan secretos industriales, etc.). La ley andaluza seguramente remite a la estatal en cuanto a que cuando la información solicitada contenga datos personales, habrá que ponderar el derecho de acceso con el derecho a la protección de esos datos, siguiendo los criterios de la Ley 19/2013 (que distingue entre datos meramente identificativos de cargos públicos accesibles, datos personales privados no accesibles en general, o datos de personas que pueden ser accesibles con disociación). En todo caso, cuando algún límite aplique, se puede denegar el acceso total o parcialmente. La denegación debe ser motivada indicando el límite y por qué aplica.
- Consulta a terceros afectados: Si la información solicitada pudiera afectar a derechos o intereses de terceros, la Administración debe dar traslado de la solicitud a esos terceros antes de resolver, para que hagan las alegaciones que estimen. Esto sucede típicamente con información que contiene datos personales de alguien: se le avisa para que pueda oponerse. Por ejemplo, si se solicita copia de un expediente sancionador a un médico, el médico sería tercero afectado cuyos datos podrían revelarse; se le consultaría y probablemente se deniegue por protección de su privacidad o se otorgue acceso parcial.
- Resolución y entrega: Como vimos, la resolución ha de ser expresa y motivada si es denegatoria (derecho a resolución motivada). Si es estimatoria, se concede el acceso. La ley prevé modalidades: la entrega puede ser proporcionando copias (en papel o electrónicas), o bien permitiendo consulta in situ en dependencias oficiales, o enviando un enlace si es algo publicado. Lo habitual hoy es facilitar copias electrónicas por correo o descarga. Si el solicitante pidió un formato específico, se intenta respetar (por ej., “dame los datos en Excel”). Solo se puede ofrecer en otro formato por causa justificada. La información se entrega preferentemente de forma gratuita, salvo costes de reproducción materiales (ej: imprimir cientos de folios, grabar DVD). En Andalucía, muchas respuestas de transparencia se publican luego en el portal (transparencia pasiva publicada), especialmente si la información puede ser de interés general.
- Recursos en caso de denegación: Si al solicitante se le deniega, restringe o no se le contesta, puede recurrir. La Ley 1/2014 establece un sistema ágil: antes de ir a vía contencioso-administrativa, cabe una reclamación ante el Consejo de Transparencia y Protección de Datos de Andalucía. Esta reclamación es gratuita y se interpone en el plazo de un mes desde la denegación (o desde que vence el plazo sin respuesta). El Consejo analizará el caso y emitirá una resolución estimando o desestimando la reclamación. Si estima, ordenará a la Administración entregar la información en un plazo. Sus resoluciones agotan la vía administrativa, es decir, ya solo quedaría recurrir a los tribunales contencioso-administrativos si alguna parte no está conforme. Cabe destacar que las resoluciones del Consejo son vinculantes: la Administración debe cumplirlas. De hecho, el incumplimiento

de una resolución del Consejo estimatoria del acceso se considera infracción muy grave para el responsable. Esto da fuerza al derecho de acceso.

En resumen, el derecho de acceso es un instrumento poderoso para la ciudadanía, pero equilibrado con salvaguardas. Para el sector sanitario, supone que un ciudadano puede obtener información como, por ejemplo, cuántos especialistas hay en cierto hospital, las tasas de infección hospitalaria, el contrato de mantenimiento de equipos de radiología, las actas de la junta facultativa, etc., siempre que no se revelen datos personales de pacientes o información que comprometa intereses legítimos. Muchas veces las peticiones de transparencia en salud versan sobre datos estadísticos (no hay problema), sobre actuaciones administrativas (tampoco suele haber problema, salvo partes confidenciales), o sobre resultados del sistema (indicadores, listas de espera, etc., que deben darse). Si alguna solicitud afectase a datos personales (por ejemplo, "quiero los correos donde se mencione mi caso entre el personal médico"), entraría en colisión con protección de datos y probablemente se reconduciría a un derecho de acceso de la persona a sus datos (LOPDGDD) más que por transparencia. La coordinación entre ambas normativas es clave: generalmente, la información de carácter personal de terceros está protegida y será la razón principal de denegación de acceso en entornos sanitarios.

Fomento de la transparencia: conservación, formación y divulgación

La Ley 1/2014 no solo impone obligaciones, sino que también prevé medidas para fomentar la cultura de transparencia en las instituciones (Título IV). Entre ellas:

- Integrar la transparencia en la gestión cotidiana (art. 35): Las administraciones deben incorporar procedimientos que garanticen que la transparencia sea parte de su forma de actuar. Esto implica planificar la gestión documental pensando en facilitar luego su publicidad; designar responsables internos de coordinar la información a publicar; etc.
- Conservación de la información (art. 36): Se obliga a conservar los documentos de forma que se facilite su acceso y longevidad. Deben usarse formatos estándares abiertos que garanticen la perdurabilidad y lectura a futuro. Esto evita que la información se pierda o quede inaccesible por obsolescencia tecnológica. Por ejemplo, guardar datos en formatos como PDF/A, CSV, etc., y mantenerlos organizados para su recuperación.
- Interoperabilidad (art. 37): La Administración andaluza debe promover iniciativas para que los distintos sistemas de información intercambien datos eficazmente. Esto favorece que, si un ciudadano pide datos que implican varias consejerías, se pueda compilar fácilmente, o que los portales de datos abiertos se alimenten de bases comunes. En salud, la interoperabilidad es también relevante para transparencia: por ejemplo, conectar la base de datos de personal con el portal de transparencia para actualizar automáticamente las listas de altos cargos o las ofertas de empleo.
- Formación de empleados públicos (art. 38): La Junta debe proporcionar instrumentos para la formación y cualificación en transparencia de sus empleados. Esto significa cursos, guías, etc., de manera que el personal conozca sus obligaciones en esta materia. Un profesional, por ejemplo, podría recibir formación básica sobre qué se considera información pública, cómo proceder ante una solicitud de acceso (aunque normalmente la gestionará la unidad de atención al ciudadano o similar), y cómo difundir información sin violar la privacidad.

- Divulgación institucional (art. 39): Las administraciones deben incluir en sus campañas de comunicación institucional aspectos de transparencia para que la ciudadanía conozca sus derechos y las vías de participación. Por ejemplo, difundir la existencia del Portal de Transparencia, animar a usarlo, publicar informes anuales de cumplimiento de transparencia.

Estas medidas buscan consolidar un cambio de mentalidad: de la opacidad tradicional a una verdadera apertura. En sanidad, fomentar la transparencia puede traducirse en, por ejemplo, instruir a los directivos de hospitales para que ofrezcan datos a la prensa y al público de manera proactiva, o en formar a los mandos intermedios (incluido personal de administración sanitaria) para que identifiquen qué información de su servicio podría ser publicable sin esperar solicitud (por ejemplo, un informe anual de resultados de su unidad). La transparencia efectiva requiere que el personal entienda su valor y no la vea como una carga burocrática sino como parte de la calidad democrática.

7. Órgano gerente: Consejo de Transparencia y Protección de Datos de Andalucía

Una particularidad en Andalucía es que se ha creado un órgano unificado que vela tanto por la transparencia como por la protección de datos en el ámbito andaluz: el Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA). Este Consejo, adscrito al Parlamento de Andalucía (para asegurar su independencia del Gobierno), tiene competencias para supervisar el cumplimiento de la Ley 1/2014 y también, en coordinación con la AEPD, algunas funciones en protección de datos en la Comunidad (especialmente respecto a autoridades autonómicas y locales).

En cuanto a transparencia, el Consejo tramita las reclamaciones de ciudadanos a quienes se les ha denegado o no respondido una solicitud de información, emitiendo resoluciones vinculantes. También puede realizar informes, recomendaciones y evaluaciones sobre cómo las entidades cumplen con la publicidad activa. Cada año publica un informe anual con estadísticas (por ejemplo, número de solicitudes de acceso recibidas por los organismos andaluces, tiempo medio de respuesta, número de denegaciones, reclamaciones presentadas y su resultado, etc.). Este Consejo es, en Andalucía, equivalente a la Agencia de Transparencia existente en otras comunidades o al Consejo de Transparencia y Buen Gobierno a nivel estatal, pero con la peculiaridad de aunar también funciones de autoridad de protección de datos autonómica. Así, por ejemplo, si hay conflictos entre acceso a información y datos personales, el Consejo es competente para resolver la reclamación integrando ambas perspectivas.

Para un profesional, el conocimiento del Consejo puede ser útil si, por ejemplo, necesita asesorarse sobre hasta dónde puede facilitar cierta información pública sin vulnerar privacidad, o simplemente como cultura general. Desde el punto de vista de la ciudadanía, cualquier persona que no obtenga respuesta a una solicitud de información a un hospital o centro de la Junta puede acudir al Consejo, el cual ha demostrado ser bastante garantista con el derecho de acceso (salvo cuando colisiona con datos personales especialmente protegidos).

8. Régimen Sancionador en Materia de Transparencia

La Ley 1/2014 prevé un capítulo específico (Título VI) de régimen sancionador para casos de incumplimiento de las obligaciones de transparencia. Distingue entre infracciones disciplinarias (para autoridades, directivos y personal) e infracciones de otro tipo (para personas jurídicas, contratistas, beneficiarios de subvenciones, etc.). Resumamos los puntos clave:

- Responsables de las infracciones: Son sujetos responsables tanto personas físicas (autoridades y empleados públicos) como jurídicas (empresas, entidades) que incumplan dolosa o negligentemente lo dispuesto en la ley 44 . Esto incluye: a) autoridades, directivos y personal al servicio de las entidades públicas (art. 3); b) personas físicas y jurídicas obligadas a suministrar información a esas entidades (art. 4); c) entidades privadas obligadas por transparencia (art. 5).
- Infracciones del personal público (art. 52): Para autoridades, directivos y empleados públicos, se consideran infracciones disciplinarias:
- Muy graves: i) El incumplimiento deliberado de las obligaciones de publicidad activa tras requerimiento expreso del Consejo de Transparencia (es decir, si el Consejo te pidió publicar algo que debías y no lo haces); ii) la denegación arbitraria de una solicitud de acceso (negar sin fundamento legal válido); iii) el incumplimiento de las resoluciones del Consejo en reclamaciones de acceso. Estos supuestos evidencian una resistencia grave a la transparencia.
- Graves: i) El incumplimiento reiterado (reincidente) de las obligaciones de publicidad activa; ii) no resolver en plazo las solicitudes de acceso de forma reiterada (dejar vencer plazos sistemáticamente); iii) la falta de colaboración con el Consejo en sus investigaciones; iv) suministrar información falseando el principio de veracidad (dar información pública sabiendo que es incorrecta). Por ejemplo, si el SAS le pide a una empresa concesionaria de limpieza que le facilite datos para publicarlos (costes, pliegos, etc.) y ésta se niega, podría incurrir en infracción.
- Sanciones previstas: Para empleados públicos, las sanciones son las disciplinarias (amonestación, suspensión, etc.) según su estatuto. Para entidades o personas privadas, la ley prevé multas económicas. En concreto, las infracciones leves pueden sancionarse con amonestación o multa de 200€ a 5.000€; las graves con multa de 5.001€ a 30.000€; las muy graves con multa de 30.001€ hasta 400.000€. Además, a las entidades infractoras de graves o muy graves se les puede imponer como sanción accesoria la devolución de subvenciones recibidas o la rescisión del contrato público que tengan 56 , proporcional al caso. Esto es un elemento contundente: por ejemplo, una empresa adjudicataria que oculte información relevante podría no solo ser multada, sino perder el contrato.
- Procedimiento sancionador: Se iniciará de oficio (por la Administración o a instancia del Consejo) y sigue el procedimiento administrativo común o el régimen disciplinario interno si son personal. El Consejo de Transparencia, cuando detecte incumplimientos que constituyan infracción, debe instar a que se abra expediente sancionador, y el órgano competente estará obligado a iniciarlo y comunicar el resultado al Consejo. Esto implica que el Consejo es vigilante y, aunque él mismo no impone la sanción (excepto quizá multas en algunos casos), sí fuerza a que la Administración sancione a sus empleados o colabore en sancionar a terceros.

En la práctica, la aplicación del régimen sancionador en transparencia ha sido limitada, pues se suele buscar antes la corrección voluntaria. No obstante, su sola existencia incentiva el cumplimiento. Para un profesional, es importante saber que incumplir adrede las obligaciones de transparencia puede acarrear consecuencias serias. Si, por ejemplo, se le ordena actualizar cierta información en la web de un hospital (supongamos que trabaja en admisión y debe publicar las listas de espera de consulta) y deliberadamente no lo hace o manipula los datos, estaría incurriendo en un incumplimiento sancionable. O si recibe una solicitud de información y la "encierra en un cajón" sin tramitarla, podría estar vulnerando el derecho de acceso. Evidentemente, casos tan extremos serían gestionados por superiores, pero la responsabilidad puede alcanzar a quien cause la opacidad.

En resumen, la ley se toma en serio la transparencia: no es opcional, es obligatoria, y para garantizarlo prevé sanciones disciplinarias y económicas. La sola amenaza de sanción ha llevado a que las Administraciones habiliten unidades de transparencia y protocolos internos para responder en plazo. Un entorno sanitario transparente no solo evita sanciones, sino que mejora la confianza de la población en el sistema de salud.

9. Relación entre la Normativa de Protección de Datos (LOPDGDD/ RGPD) y la de Transparencia

Aunque a primera vista pudieran parecer normas en tensión una busca publicar información y la otra proteger la información personal, en realidad la transparencia y la protección de datos deben convivir de forma armónica, encontrando equilibrios caso a caso. La legislación reconoce explícitamente esta necesidad de coordinación:

- La Ley 1/2014 establece que la publicidad de información con datos personales especialmente protegidos (salud, ideología, etc.) requiere disociarlos previamente 34 . Y para datos personales en general, la ley andaluza se aplica respetando lo dispuesto en la normativa básica (Ley 19/2013) que a su vez remite a la protección de datos: en caso de colisión, hay que ponderar qué derecho prevalece en función de cada supuesto. Por ejemplo, la transparencia obliga a publicar los sueldos y nombres de altos cargos; en ese caso se entiende que prevalece el interés público en conocer el uso de fondos públicos sobre la privacidad de ese alto cargo (además, su posición conlleva menor expectativa de privacidad). En cambio, la mayoría de datos personales de empleados de nivel medio o bajo (TCAEs, enfermeros, médicos de base) no son relevantes para la transparencia y por tanto no se publican sus datos nominativos (salvo quizás nombre en organigramas).
- La LOPDGDD, por su parte, reconoce en su artículo 19 que el tratamiento de datos personales con fines de transparencia se ampara en la existencia de una obligación legal y en el cumplimiento de misiones en interés público. Es decir, cuando una administración divulga datos personales cumpliendo la ley de transparencia, está legitimado por el RGPD (art. 6.1.c y e). Sin embargo, también advierte que deberá hacerse conforme a lo previsto en la propia ley de transparencia y respetando los límites de ésta y del RGPD.

En la práctica, la relación se plasma así: la Ley de Transparencia delimita hasta dónde llega el acceso público a la información cuando hay datos personales. Por ejemplo, en información

meramente organizativa (nombre y puesto de un jefe de servicio) sí se publica; pero la información que afecte a la intimidad o datos sensibles de personas se reserva. Un caso típico en salud: las esperas quirúrgicas se publican con número medio de días y número de pacientes esperando, pero no con la lista de nombres de pacientes que esperan, porque son datos personales sanitarios. Otro caso: se publican listados de contratos adjudicados a empresas, incluyendo nombres de empresas (que no son datos personales) y CIFs, pero si una adjudicación la obtiene una persona física (digamos un autónomo), ahí hay un dato personal (nombre y apellidos) y en principio se publica porque es información contractual pública, aunque habría que valorar si supone divulgar, por ejemplo, su domicilio (ese podría ocultarse).

Conflictos y cómo se resuelven: Cuando un ciudadano solicita por transparencia algo que contiene datos personales, la Administración debe aplicar los límites. Por ejemplo, si pide correspondencia interna de un hospital sobre un paciente X, seguramente se denegará por protección de la intimidad. Si pide "¿Cuántas denuncias por mala praxis tiene el Dr. Fulano?", se tendría que valorar: es información personal del médico (afecta a su honor, posiblemente) vs. interés público en conocer si ha habido reclamaciones. Probablemente se negaría por ser datos personales de carácter disciplinario/profesional no públicos, a menos que se trate de un alto cargo y de casos ya sancionados. Cada caso requiere ponderación: la ley estatal sugiere que tratándose de empleados públicos, se pueden dar datos meramente identificativos y relacionados con la organización del servicio, pero no datos referidos a su vida privada o desempeño individual salvo que afecte al interés público de control (por ejemplo, datos de recaudación de un médico individual no se dan, pero quizás datos globales del servicio sí). El Consejo de Transparencia juega un papel clave mediando estos conflictos. Al tener también competencias en protección de datos, busca soluciones de equilibrio. A veces se recurre a la anonimización o seudonimización: facilitar la información solicitada eliminando nombres. Ejemplo: un periodista pide informes de inspección sobre centros de salud. Se pueden dar quitando los nombres de pacientes o profesionales implicados, pero dejando el contenido evaluativo. Así se cumple transparencia sin violar la privacidad.

Otro aspecto de la relación es que la transparencia legitima ciertas publicaciones de datos personales que de otro modo estarían protegidos. Por ejemplo, publicar las retribuciones y bienes de altos cargos es un tratamiento de datos personales que se permite porque una ley de rango suficiente (Ley 1/2014, en consonancia con Ley 19/2013) así lo exige para asegurar la integridad pública. En estos casos, la persona afectada (alto cargo) no podría invocar protección de datos para impedirlo, ya que su propio estatus conlleva ese sacrificio de privacidad en pro del interés general.

En el ámbito sanitario, un claro ejemplo de balance es la publicación de indicadores sanitarios por centro. Se puede y debe informar a la población de, por ejemplo, la tasa de infecciones hospitalarias de cada hospital, pero no se puede publicar la lista de pacientes que las contrajeron. Se puede publicar cuántos profesionales tiene un hospital, pero no necesariamente la ficha completa de cada uno. Se publican los nombres de jefes de servicio, pero no de todos los subordinados. Se publica qué empresas proveen ciertos servicios (limpieza, ambulancias) y sus contratos, pero no los datos personales de los empleados de esas empresas.

La relación entre ambas normativas se institucionaliza también en que el mismo Consejo de Transparencia andaluz lleva la protección de datos en su nombre. Esto enfatiza que en Andalucía se

busca una visión conjunta: transparencia y protección de datos no son enemigas, sino complementarias. Una administración moderna debe ser transparente en su gestión, salvaguardando a la vez la privacidad de las personas. De hecho, la propia Ley 1/2014 menciona en su preámbulo y articulado que se asegurará la confidencialidad de los datos personales especialmente protegidos en la difusión de información.

Para un profesional, esto significa que debe entender que no toda información puede divulgarse alegremente. Por mucho afán de transparencia que tengamos, hay datos, sobre todo clínicos o personales, que no pueden compartirse públicamente. Incluso ante compañeros de trabajo, rige la protección de datos: por ejemplo, no se debe difundir el diagnóstico de un paciente salvo a quien corresponda. Pero a la vez, en lo institucional, el profesional debe asumir que cierta información de su centro es pública (por ejemplo, los protocolos de atención pueden estar publicados, las cifras de pacientes atendidos, etc.), y que eso redunda en mayor confianza. Si alguna vez cree haber detectado un choque (por ej., le piden publicar un documento que contiene nombres de pacientes), debe consultar al Delegado de Protección de Datos o al responsable de transparencia para anonimizar esos nombres antes de publicarlo.

En síntesis, la LOPDGDD y la Ley de Transparencia andaluza se relacionan constantemente: la primera protege datos de carácter personal; la segunda garantiza la apertura de la información pública. La clave es el equilibrio: publicar todo lo público, proteger todo lo privado. Y en la zona gris (información mezclada), hacer ponderaciones caso a caso con criterio y, cuando es viable, disociar datos personales para permitir la máxima transparencia posible sin dañar derechos individuales.

10. Implicaciones para el Trabajo Diario de un Profesional: Ejemplos Prácticos

Para aterrizar todo lo anterior, veamos situaciones concretas que puede vivir un profesional en su día a día y cómo se conectan con estas normas:

- Confidencialidad del paciente: Un profesional en planta tendrá acceso a historiales, listados de pacientes, puede oír conversaciones clínicas, etc. La LOPDGDD refuerza el deber de secreto: ningún dato de paciente debe trascender fuera del equipo asistencial. Por ejemplo, si familiares de otro paciente preguntan "¿qué le pasó al señor de la cama de al lado?", el profesional no puede revelar diagnósticos ni datos personales. Debe contestar con respeto pero sin divulgar nada: "Lo siento, no puedo dar información de otros pacientes". Asimismo, si un medio de comunicación acude al hospital por una noticia (imaginemos, un accidente con múltiples heridos), el profesional no debe dar datos a periodistas; el centro tiene portavoces oficiales y protocolos para información pública. La transparencia en salud se refiere a datos agregados o institucionales, pero jamás a datos clínicos individualizados sin consentimiento.
- Gestión de documentación clínica: Un profesional maneja con frecuencia documentos (peticiones, resultados, hojas de registro). Debe seguir medidas de seguridad: no dejarlos olvidados en zonas comunes, depositarlos en contenedores de destrucción cuando ya no sirven, custodiar los carros de historias clínicas cerrados. Si ve documentos con datos de

pacientes extraviados (por ejemplo, un informe olvidado en una fotocopiadora), debe recogerlo y entregarlo al responsable de documentación o destruirlo. Esto evita brechas de seguridad. La normativa de protección de datos impondría notificar a la AEPD si se pierden papeles con datos de salud; por tanto, hay que extremar el cuidado para que no ocurra.

- Sistemas informáticos e historia digital: El profesional probablemente use sistemas como Diraya (historia electrónica andaluza). Debe usar sus propias credenciales, no dejarlas anotadas en papeles visibles, y cerrar sesión al ausentarse. Solo debe consultar las historias de pacientes a su cargo o por motivos laborales justificados. Curiosidad o comentarios están prohibidos. La LOPDGDD y el RGPD exigen trazabilidad: cada acceso queda registrado, y se auditan accesos indebidos. Ha habido casos sancionados de personal sanitario que accedió a la historia de un famoso sin estar implicado en su cuidado. Eso es infracción grave de confidencialidad. Un profesional debe resistir la tentación de mirar historias que no le corresponden.
- Consentimientos informados y datos especialmente protegidos: A veces el profesional apoya en la recogida de consentimientos (por ejemplo, firma de consentimiento quirúrgico, o para cesión de datos a investigación). Debe verificar, si está en su función, que el paciente recibe la información adecuada (normalmente el médico informa y el profesional puede gestionar el papel). Si un paciente se niega a dar cierto consentimiento (por ejemplo, a que su muestra se use en investigación), se respeta absolutamente. Aquí la protección de datos se conecta con la ética asistencial: el paciente decide sobre sus datos de salud en muchos contextos.
- Derechos ARCO del paciente: Si un paciente solicita copia de su historia clínica (derecho de acceso a datos de salud), el profesional debe indicarle el procedimiento formal: normalmente un formulario de solicitud en Atención al Usuario o Gestión de Pacientes. La Ley 41/2002 y el RGPD le amparan para obtenerla en máximo 1 mes. El profesional puede facilitar ese ejercicio informándole dónde acudir, o incluso gestionando la solicitud si está en sus competencias. Nunca debe obstaculizarlo ni cuestionar por qué la quiere; es su derecho. Igualmente, si pide corregir algún dato (rectificación), se canaliza a Documentación Clínica para hacer la anotación oportuna, y si pide cancelar algo, se explica que la historia no se borra pero puede aportar añadidos o ejercer su derecho a supresión dentro de los límites (por ejemplo, que sus datos no se usen con fines docentes si así lo manifiesta).
- Transparencia en la atención al ciudadano: Un profesional, sobre todo en Atención Primaria o en urgencias, puede recibir preguntas genéricas de los usuarios: "¿Dónde puedo informarme de las listas de espera?" "¿Cómo van las obras del centro de salud nuevo?" Gracias a la transparencia, muchas de esas informaciones están públicas: el profesional debe mostrar una actitud de servicio, indicando: "Mire, en la página web del SAS hay un apartado de Listas de Espera donde salen los datos actualizados; si quiere, le puedo ayudar a consultarlo". O derivar a Atención al Usuario para más detalles. Antes, quizá estas preguntas se ignoraban; ahora, con la cultura de transparencia, el personal sabe que el ciudadano tiene derecho a saber y hay que facilitarle la información (dentro de lo permitido).
- Peticiones formales de información: Si un profesional es consciente de una solicitud de transparencia dirigida a su unidad (por ejemplo, llega una petición formal al servicio preguntando "¿Cuántos profesionales había de guardia en la noche tal?" tras un incidente), debe colaborar con sus superiores aportando los datos para responder, siempre y cuando no involucren datos personales protegidos. En este ejemplo, se pide número de personal (dato estadístico), no nombres, así que se puede dar. Si pidieran nombres, se daría número o

categorías en su lugar, para proteger identidades. Colaborar en la respuesta es una obligación interna: la ley dice que todos los departamentos deben facilitar al responsable de informar los datos necesarios. No debe ver esto con recelo, sino con naturalidad: la ciudadanía escruta la dotación de personal, los recursos, etc., y es legítimo.

- Publicación de listas o datos de usuarios: Un aspecto delicado: a veces se publican listados (p.ej. admitidos a una bolsa de empleo, resultados de un concurso de traslados, etc.). Esos listados contienen datos personales (nombre, DNI parcialmente). Se publican amparados por normativa de función pública, pero incluso así se deben extremar medidas: por ejemplo, en los tablones digitales, no exponer más datos de los necesarios (nunca DNI completo, nunca dirección personal). Un profesional que participe en esa gestión debe aplicar ese criterio. Y si un ciudadano pidiera, por transparencia, información que incluye datos personales de terceros, se deberá denegar o anonimizar. Imaginemos que alguien pide "registro de visitantes ilustres al hospital X". Si esa lista existe, tendría nombres de personas (datos personales). Si son cargos públicos, quizá se podría dar; si son pacientes VIP, no, por privacidad. Ante la duda, el profesional elevaría la consulta a la dirección y al DPD.
- Redes sociales y móviles: La LOPDGDD y el deber de secreto implican que un profesional no debe compartir en redes sociales o mensajería información privada del trabajo. Por ejemplo, está prohibido hacer fotos a pacientes con el móvil personal. Incluso fotos sin personas pero dentro de áreas clínicas pueden revelar información (un monitor con datos, un historial abierto). Debe evitarse. Respecto a WhatsApp u otras apps para coordinarse en el equipo, hay que ser muy cautos: lo ideal es no usar datos personales de pacientes en apps no seguras. Si se comparte alguna información por agilizar (hecho que ocurre en ocasiones), que sea minimizada y sin identificadores (iniciales en vez de nombre completo, etc., aunque estrictamente no es plenamente conforme RGPD usar WhatsApp para datos de salud). Muchos hospitales ya instruyen sobre esto, incluso proporcionando apps corporativas seguras. Un profesional debe seguir las directrices de su centro en comunicación digital.
- Derechos como trabajador público: No hay que olvidar que el profesional es también sujeto de derechos. Gracias a la Ley de Transparencia, puede acceder a información de su propia institución que antes era difícil. Por ejemplo, puede solicitar vía transparencia datos sobre plazas vacantes, sobre criterios de distribución de material, etc., que tal vez como empleado no le facilitan fácilmente. Mientras no sea información interna restringida por otras normas, la puede obtener como cualquier ciudadano. También la LOPDGDD le protege: su correo profesional no puede ser monitorizado sin causa ni sus conversaciones grabadas sin aviso. Y tiene derecho a desconectar fuera de turno: si la supervisión le envía WhatsApps fuera de horario reiteradamente, podría invocar el derecho a desconexión. Son aspectos a tener presentes para su bienestar laboral.

En conclusión, para un profesional el cumplimiento de la normativa de protección de datos significa garantizar la confidencialidad y seguridad de la información de pacientes (lo cual es parte esencial de la deontología sanitaria), y el cumplimiento de la transparencia implica formar parte de un sistema sanitario abierto en lo relativo a su gestión y resultados (pero nunca en lo tocante a datos personales sensibles). Ambos aspectos confluyen en su trabajo: deberá ser reservado con lo privado y transparente con lo público. Adoptar esta cultura redunda en beneficio de todos: el paciente confía porque sabe que sus datos están seguros, y la sociedad confía porque sabe qué se hace con los recursos sanitarios.

Para estudiar este tema, el profesional debe interiorizar los principios y derechos clave, y estar al tanto de cómo aplicarlos en situaciones reales. Así estará preparado no solo para responder un examen de oposición, sino para ejercer con profesionalidad en el día a día, respetando la legislación vigente y contribuyendo a una sanidad andaluza confidencial en lo personal y transparente en lo público.

11. Referencias Bibliograficas:

- **Constitución Española. (1978)**. Boletín Oficial del Estado, 311, 29313–29424.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L119, 1–88.

- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018).** Boletín Oficial del Estado, 294, 119788–119857. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

- **Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. (2002).** Boletín Oficial del Estado, 274, 40126–40132.

- **Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía. (2014).** Boletín Oficial de la Junta de Andalucía, 124, 2–23.

- **Junta de Andalucía. (s. f.).** Tus derechos y obligaciones en materia de Transparencia. Portal de Transparencia. https://www.juntadeandalucia.es/organismos/transparencia/conoce-transparencia/tus-derechos.html

- **Setemcat. (2019).** Novedades de la LOPDGDD 3/2018: consentimiento de menores y personas fallecidas. https://www.setemcat.com/novedades-de-lopdgdd-3-2018/

- **Grupo Ático34. (2023).** Guía: Protección de datos sanitarios. Obligaciones en centros de salud. https://protecciondatos-lopd.com/empresas/sanitarios/

- **Noticias RGPD. (s. f.).** Consecuencias de imponer solo apercibimientos a las administraciones públicas por la infracción del RGPD. https://rgpdblog.com/consecuencias-de-imponer-solo-apercibimientos-a-las-administraciones-publicas-por-la-infraccion-del-rgpd/

- **PI22. (s. f.).** Ley 1/2014 Transparencia Pública de Andalucía. Título VI: Régimen sancionador. https://pi22.eu/index.php/zona-clientes/legislacion/ley-1-2014-transparencia-publica-de-andalucia/131-ley-1-2014-transparencia-publica-de-andalucia-titulo-vi-regimen-sancionador

- **Servicio Andaluz de Salud (SAS). (2022).** Tema 5 – La protección de datos. https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud/sites/default/files/sincfiles/wsas-media-mediafile_sasdocumento/2022/temario_comun_tema_5_la_proteccion_de_datos_iapp.pdf