PRINCIPADO DE ASTURIAS

PLAN ANUAL DE LA INSPECCIÓN GENERAL DE SERVICIOS CORRESPONDIENTE AL AÑO 2023

ÁREA IV: Administración del Principado de Asturias, sus organismos y entidades públicas. Estudio de las políticas de protección de datos, en especial, de los datos de mayor sensibilidad.

Fecha de emisión

30/06/2023

1 OBJETO Y JUSTIFICACIÓN DE ESTA INSPECCIÓN

El artículo 1 de la Ley del Principado de Asturias 11/2018, de 16 de noviembre, de la Inspección General de Servicios, atribuye a la Inspección la función de velar, por el cumplimiento de las disposiciones vigentes en materia de personal y de organización, de funcionamiento, régimen jurídico y procedimiento administrativo, así como por la idoneidad de los medios dispuestos para el logro de los objetivos asignados y la utilización racional de los recursos empleados.

En concreto, corresponde a esta Inspección la competencia para realizar inspecciones, emitir los informes que le sean requeridos en relación con las funciones que le son propias, formular e informar propuestas de reforma y modernización, organizativas y funcionales.

Y los resultados de estas actuaciones se plasmarán, sigue diciendo el artículo 7.2 de la referida Ley que regula la Inspección General de Servicios, en un informe que, junto al análisis y diagnóstico de la situación, contendrá recomendaciones para corregir las deficiencias que puedan haberse observado, con propuesta, en su caso, de apertura de expediente disciplinario.

De forma detallada, el artículo 5 de dicha Ley prevé que en el último trimestre de cada año, la Inspección General de Servicios someterá a la aprobación del Consejo de Gobierno, a través de la Consejería de la que dependa orgánicamente, un plan anual de actuaciones.

En cumplimiento de lo anterior y, por Acuerdo de 10 de febrero de 2023 del Consejo de Gobierno, se aprobó el Plan Anual de la Inspección General de Servicios correspondiente al año 2023 (BOPA 20 de febrero de 2023).

Y en ejecución de lo anterior, se ha fijado como **cuarta área de actuación del plan del año 2023**, la referente a esta inspección, que versa **sobre la realización de un estudio de las políticas de protección de datos, en especial, de los datos de mayor sensibilidad** en el ámbito de la Administración del Principado de Asturias, sus organismos y entidades públicas.

La realización del referido trabajo analítico encomendado se fundamenta en el propio acuerdo del Consejo de Gobierno, estimándose la necesidad de "*analizar la situación de la implementación en el ámbito de la Administración del Principado y sus organismos y entidades públicas, de las obligaciones que le incumben en el ámbito de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*"

2 METODOLOGÍA

El ámbito de aplicación de la inspección encomendada se realiza sobre los siguientes ámbitos de aplicación, considerando las siguientes perspectivas:

2.1 MATERIAL

Ciclo del tratamiento de datos en la organización entendiendo como tal la cadena de las actividades implicadas que comienza por la recogida de datos, su tratamiento, cesión o transferencia y su conservación, junto con las oportunas tareas de evaluación de riesgos y auditorías.

2.2 TEMPORAL

Respecto al ámbito temporal de esta inspección se ha tomado como referencia la situación actual, transcurridos casi cinco años desde la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, a fin de diagnosticar el grado de implantación del nuevo sistema de protección de datos basado en la "responsabilidad proactiva" que impone la normativa vigente.

2.3 SUBJETIVO

La encomienda de la inspección afecta a las distintas Consejerías, organismos y entidades públicas por lo que se ha seleccionado a la totalidad de las consejerías junto con aquellos organismos y entidades públicas que tratan datos personales de más sensibilidad y/o aquellos que gestionan un mayor volumen de datos por afectar a un porcentaje amplio de la ciudadanía.

En consecuencia, se ha analizado la situación de la protección de datos correspondiente a:

- Presidencia del Principado de Asturias (01).
- Consejería de Administración Autonómica, Medio Ambiente y Cambio Climático (10).
- Consejería de Presidencia (11).
- Consejería de Hacienda (12).
- Consejería de Industria, Empleo y Promoción Económica (13).
- Consejería de Educación (14).
- Consejería de Salud (15).
- Consejería de Derechos Sociales y Bienestar (16).
- Consejería de Medio Rural y Cohesión Territorial (17).
- Consejería de Cultura, Política Lingüística y Turismo (18).
- Consejería de Ciencia, Innovación y Universidad (19).
- Ente Público de Servicios Tributarios (83).
- Instituto Asturiano de Prevención de Riesgos Laborales (IAPRL) (84).
- Servicio Público de Empleo del Principado de Asturias (SEPEPA) (85).
- Servicio de Emergencias del Principado de Asturias (SEPA) (87).
- Establecimientos Residenciales para Ancianos de Asturias (ERA) (96).
- Servicio de Salud del Principado de Asturias (SESPA) (97).

Es, por ello, que se estima que la muestra objeto de análisis es, desde un punto de vista subjetivo, lo suficientemente representativa como para concluir de su estudio la afectación a toda la administración autonómica.

2.4 METODOLÓGICO

El análisis de la situación de la protección de datos en la Administración del Principado de Asturias que se ha realizado, se nutre de la siguiente documentación:

- Información publicada, tanto en las páginas web libremente accesibles, en particular en la de la Agencia Española de Protección de Datos (EDPD), como en los portales de transparencia.

- Información suministrada por las Consejerías, organismos autónomos y entidades públicas a instancia de la Inspección General de Servicios mediante entrevistas realizadas a los principales responsables de tratamiento de datos, delegados de protección de datos nombrados así como responsables de la política de seguridad de los sistemas de información.
- Consulta especifica de expedientes a través del Escritorio Electrónico del Principado de Asturias (SITE).
- Respectivos decretos de estructura orgánica de las distintas Consejerías, organismos y entidades públicas analizadas.

3 MARCO NORMATIVO

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución Española. Es por ello que su regulación está sujeta a ley orgánica, tal y como determina el artículo 86 del citado texto normativo, la cual constituye, a su vez, legislación básica ostentando las comunidades autónomas competencias de desarrollo normativo y ejecución en su ámbito de actividad.

Conforme a dicho reparto competencial, es aprobada la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), que deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

No obstante, tal y como señala el preámbulo de esta norma legal, el derecho fundamental de las personas físicas a la protección de datos personales, se ejercerá no sólo con arreglo a lo establecido en dicha ley, sino también y sobre todo, conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD).

El RGPD, que a su vez deroga la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, es–a diferencia de ésta directiva- de aplicación directa, sin requerir transposición previa, siendo por tanto directamente vinculante para los estados miembros desde el 25 de mayo de 2018.

Por su parte, y por lo que al tratamiento de datos por las Administraciones Públicas se refiere, el artículo 13 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas, establece el derecho de las personas en sus relaciones con las Administraciones Públicas a la protección y confidencialidad de sus datos y a la seguridad de los mismos cuando figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

Asimismo, la protección de los sistemas de información, utilizados para la prestación de servicios públicos y de la información tratada en el ámbito de la Administración Electrónica se rige por el Real Decreto 311/2022, de 23 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Respecto a la competencia de desarrollo normativo y ejecución autonómica, señalar la ausencia de normativa al respecto en el ámbito del Principado de Asturias.

4 ASPECTOS GENERALES

El RGPD define **datos personales** como toda información sobre una persona física identificada o identificable («el interesado»).

A estos efectos, se considerará **persona física identificable** toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Asimismo, el RGPD (artículo 4) entiende por **tratamiento** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Cualquier tratamiento de datos personales que se lleve a cabo ha de contar con una habilitación previa, esto es, una **base legitimadora**, dentro de las recogidas en la normativa aplicable, y que son:

-Consentimiento.

-Relación contractual.

-Intereses vitales del interesado o de otras personas.

-Obligación legal cuyo cumplimiento conlleve y exija un tratamiento de datos.

-Interés público o ejercicio de poderes públicos.

-Intereses legítimos prevalentes de la organización que trate los datos o de terceros a los que se comunican los datos.

En efecto, no solo ha de concurrir base legal, sino que la misma ha de identificarse y justificarse inexcusablemente y de forma expresa con carácter previo a la realización del tratamiento.

La persona física, jurídica o autoridad que tiene la competencia para decidir los fines (para qué) y los medios (cómo) del tratamiento concreto es, conforme a la normativa aplicable, el **responsable del tratamiento**, sobre el que recae, en lo sustancial, la responsabilidad del cumplimiento de las obligaciones impuestas por la normativa en orden a la efectiva protección del derecho fundamental.

Identificada la base legitimadora, el tratamiento de datos subsiguiente ha de llevarse a cabo indefectiblemente con arreglo a las prescripciones establecidas en el RGPD y en la LODPDGDD, competiendo al responsable del tratamiento la acreditación de su implementación, aplicación y cumplimiento.

Constituye, precisamente, objeto de la presente actuación inspectora la comprobación del cumplimiento, en su caso, de dicha normativa en los tratamientos de datos personales que se realizan por las distintas Consejerías y organismos y entidades públicas adscritas a la Administración del Principado de Asturias.

La comprobación, en su caso, de la adecuación a la vigente normativa exige partir de las novedades introducidas por ésta. Y es que la nueva regulación del derecho fundamental aporta, respecto a la normativa previa, elementos innovadores en cuanto a la protección efectiva del tratamiento de datos personales, que se centran fundamentalmente en dos aspectos:

- El **principio de responsabilidad proactiva**. El tratamiento de datos de carácter personal exige la aplicación de medidas técnicas y organizativas, a fin de garantizar y poder demostrar que el tratamiento es conforme a las exigencias contenidas en la citada normativa reguladora. Esto es, se exige una actitud consciente, diligente y proactiva por parte de las organizaciones que acometan tratamientos de datos personales.

- El **enfoque de riesgo**. La aplicación de las medidas de protección contenidas en la normativa reguladora del derecho debe tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas que la normativa establece, se aplicarán sólo cuando existe un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.

Fusionando ambos principios, cabría concluir que la novedad en la que se sustenta la vigente normativa es la evolución de un modelo basado, fundamentalmente, en el control a otro modelo -el actual- que descansa en el principio de responsabilidad proactiva, lo que exige una previa valoración del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan.

La implementación de las políticas de tratamiento de datos personales exige el diseño y cumplimiento por parte del responsable, de una "suerte" de **hoja de ruta**, comprensiva, en líneas generales, de los siguientes hitos:

1.- Elaborar un diseño preventivo del respectivo tratamiento de datos personales a ejecutar, mediante el enfoque de riesgos (análisis de riesgos y evaluación de impacto).

2.- Diseño, propuesta y aplicación de medidas de seguridad.

3.- Someter la práctica de las actividades de tratamiento de datos a una previsión y gestión llevada a cabo desde la privacidad.

4.- Garantizar el ejercicio de derechos.

5.- Elaborar el Registro de actividad de tratamiento y conferir publicidad al inventario.

6.- Diseñar y ejecutar controles y auditorías de cumplimiento.

7.- Implementar la estructura organizativa y competencial, con especial referencia a la asunción de las funciones legalmente atribuidas a la figura del delegado de protección de datos.

Procede, a continuación, poner de manifiesto el grado de cumplimiento de la normativa aplicable en materia de protección de datos personales, tanto por la Administración del Principado, como por las distintas Consejerías, organismos y entidades públicas adscritas, en sus respectivos ámbitos competenciales y en relación con cada uno de los hitos expuestos.

5 ELABORACIÓN DE UN DISEÑO PREVENTIVO DEL RESPECTIVO TRATAMIENTO DE DATOS PERSONALES A EJECUTAR, MEDIANTE EL ENFOQUE DE RIESGOS (ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO)

5.1 CONTENIDO

Cualquier actividad que conlleve un tratamiento de datos personales requiere que, con carácter previo a su realización, se lleve a cabo un análisis, una identificación y evaluación de los posibles riesgos a los derechos y libertades de los interesados, así como de las medidas necesarias para minimizar dichos riesgos, de forma que no lleguen a concretarse en daños.

En efecto, el proceso de gestión de riesgos implica realizar inicialmente dos tareas: identificarlos y evaluarlos.

-**Identificar los riesgos**: consiste en determinar las amenazas y vulnerabilidades que pueden afectar a cada activo, así como las fuentes y los agentes que pueden originarlas o aprovecharlas.

-**Evaluar los riesgos**: consiste en estimar la probabilidad y la gravedad de que se materialicen los riesgos identificados, teniendo en cuenta las medidas de seguridad existentes y el nivel de exposición de los datos personales.

En este sentido, se entiende por riesgo la probabilidad y el impacto de que una amenaza se materialice, siendo una amenaza cualquier elemento o factor que potencialmente pueda provocar un daño o perjuicio.

Para identificar todas las amenazas a las que pueden estar expuestos los tratamientos de los datos personales hay que tener en cuenta todo el ciclo de vida de los datos, identificando todos los escenarios en el que se pueda producir un daño o una violación de los datos y/o de los derechos y libertades de los interesados.

Exige, pues, la adopción de medidas proactivas que se anticipen a las amenazas, identificando las debilidades de los sistemas para neutralizar o minimizar los riesgos en lugar de aplicar medidas correctivas para resolver los incidentes de seguridad una vez sucedidos.

Es por ello que resulta obligatorio mantener documentados todos los procesos, en especial, en lo que se refiere a la identificación del riesgo relacionado con el tratamiento y la evolución del mismo. Así pues, la identificación y análisis de factores de riesgo han de estar siempre documentados y justificados a fin de que el responsable pueda demostrar que, las decisiones tomadas en cada momento con relación a la gestión del riesgo han sido las más adecuadas en función de la información de la que se disponía ("accountability").

La gestión del riesgo desde el punto de vista de la protección de datos se desagrega en dos actuaciones distintas, aunque íntimamente dependientes; que son, por un lado, el análisis de riesgo y, por otro, la evaluación de impacto.

Señalar con carácter previo que, si bien no todo tratamiento de datos exige una preceptiva evaluación de impacto, en cambio sí se ha de acometer, por el responsable, un análisis de los riesgos a los que está sometido el referido tratamiento, siendo así que, en virtud de dicho análisis, se proponga la adopción de las concretas medidas técnicas u organizativas a implementar.

En el **análisis de riesgos**, se identifican las amenazas más probables y se analizan las vulnerabilidades relacionadas con dichas amenazas. El análisis de riesgos en la protección de datos no aparece citado literalmente ni en el RGPD ni en la LOPDGDD,

pero sí que está implícito en ambas normativas, dejando clara la obligación de llevarlo a cabo siempre que se vayan a realizar actividades de tratamiento de datos personales

En la **evaluación de impacto** se analizan los riesgos que un sistema, producto o servicio pueden suponer para los derechos y libertades de las personas y, tras haber realizado ese análisis, se gestionan esos peligros antes de que se materialicen. Así pues en la evaluación se busca principalmente determinar el impacto que tendría un evento disruptivo en los datos personales a tratar.

Así, el artículo 25 del RGPD establece la obligación de implementar la protección de datos desde el diseño, siendo aplicable a todos los responsables del tratamiento con independencia de su tamaño, el tipo de datos tratados o la naturaleza del tratamiento. En concreto, se les exige que se apliquen las medidas técnicas y organizativas apropiadas "tanto en el momento de determinar los medios de tratamiento como en el propio tratamiento".

Por su parte, el artículo 35 del RGDP establece la obligación de llevar a cabo las Evaluaciones de Impacto en la Protección de Datos (EIPD) en aquellos tratamientos de alto riesgo para los derechos y libertades de las personas. Dicha evaluación debe realizarse antes del tratamiento en los casos que ese tipo de tratamiento utilice nuevas tecnologías, o que por su naturaleza, alcance, contexto o fines, sea probable que entrañe un alto riesgo para los derechos y libertades de las personas físicas.

La evaluación de impacto es un proceso que permite a las organizaciones, en la fase de diseño, valorar la necesidad y proporcionalidad de las operaciones de tratamiento en relación a la finalidad, identificar los riesgos que un sistema, producto o servicio puede implicar para los derechos y libertades de las personas, y, tras haber realizado ese análisis, afrontar y gestionar esos peligros antes de que se materialicen con la elaboración de un plan de acción que incorpore medidas de seguridad y mecanismos que garanticen adecuadamente la protección de los datos personales recabados.

La EIPD y la gestión del riesgo son actividades integradas. Una vez que se toma la decisión de llevar a cabo una EIPD, esta forma parte indivisible de la gestión de riesgos para los derechos y libertades. De esta forma, no es posible ejecutar una EIPD si no existe una gestión de riesgos para los derechos y libertades y no se realiza en el marco de la misma.

La valoración de si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa se atribuye a los responsables y encargados del tratamiento. Para realizar dicha evaluación el responsable del tratamiento recabará el asesoramiento del delegado de protección de datos (artículo 35.2 RGPD y articulo 28.1 LOPDGDD).

El RGPD obliga a las Autoridades de Control a establecer listas orientativas de tratamientos que no requieren EIPD, así como de tratamientos que sí requieren su realización. En consecuencia, pueden consultarse en la página web de la AEPD las listas orientativas de tratamientos que requieren o no requieren EIPD publicadas por la AEPD y aprobadas por el EDPB (*European Data Protection Board*).[1]

Aunque para todos los tratamientos se exige una gestión del riesgo para los derechos y libertades de los interesados según en el artículo 24.1, los tratamientos de alto riesgo tienen como obligación realizar una evaluación de impacto para la protección de datos

1 https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/evaluaciones-de-impacto

(EIPD). Para determinar si hay un alto riesgo hay que comenzar consultando los casos que ya están tasados, como:

• Los casos del artículo 35.3 del RGPD.

• La normativa especial que exige una EIPD para el tratamiento o identifica factores de riesgo.

• Los casos y ejemplos de la guía WP248 "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD)".

•Los casos de la lista aprobada por la AEPD en base al artículo 35.4 del RGPD.

• Los casos del artículo 28.2 de LOPDGDD.

• Los casos del artículo 32.2 del RGPD.

• Los riesgos identificados en el Considerando 75180.

• Los casos y condiciones específicas descritos en las directrices publicadas por el Comité Europeo de Protección de Datos (CEPD) para tratamientos específicos.

• Los casos y condiciones específicas descritos en los códigos de conducta de acuerdo con el artículo 40 y mecanismos de certificación de acuerdo con el artículo 42 del RGPD.

La lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos según artículo 35.4 RGPD se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 de las Directrices WP248 y se considera que será necesario realizar una EIPD en el momento de analizar tratamientos de datos en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD. Cuantos más criterios de los diez incluidos en la lista reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD.

Además, el responsable también podrá llevar a cabo la EIPD cuando lo considere o valore necesario, al ser estas listas orientativas y no restrictivas. Como señala la AEPD "*con independencia de que se trate de un tratamiento obligado o no a la realización de una EIPD, el responsable puede tomar la decisión de efectuarla con el fin de llevar a cabo un análisis más detallado del tratamiento de datos personales en aras de una mayor diligencia a la hora de implementar la responsabilidad proactiva. También son motivos válidos mejorar la calidad de sus productos y servicios, fomentar la cultura de protección de datos en su organización o bien como simple mecanismo para garantizar la confianza de sus clientes*."

Además, debe tenerse en cuenta que, en el ámbito de las administraciones públicas, en el ejercicio de sus competencias, como en este caso analizado, cuando se promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el RGPD, así como la L.O. 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, debe realizarse una evaluación de impacto para la protección de datos en el desarrollo normativo. La AGEPD ha publicado en el mes de junio de 2023 unas orientaciones para su realización.

Para facilitar el análisis de la existencia de un alto riesgo, la AEPD ha puesto a libre disposición guías y herramientas que simplifican su determinación. Si el proceso de

gestionar un alto riesgo no consigue reducirlo hay que consultar a la autoridad de protección de datos. Si no se cumplen los criterios de idoneidad, necesidad y proporcionalidad, o no se ha podido mitigar el alto riesgo, el tratamiento no se podrá llevar a cabo.

Por último debe tenerse en cuenta que si bien la EIPD tiene un carácter a priori, es decir, hay obligación de ejecutarla antes del inicio de las actividades de tratamiento, también es cierto que al ser un proceso integrado dentro del propio proceso de gestión de riesgos para los derechos y libertades y no un estado, su revisión y adaptación se extiende a todas las etapas del ciclo de vida de este.

La AGPD recomienda que, si durante la vida del tratamiento se producen cambios ajenos al responsable, como cambios contextuales o una ampliación no prevista del ámbito/alcance, será necesario actualizar la EIPD y, en su caso, generar un nuevo informe y plan de acción con las medidas de control adicionales que fuera necesario implantar en el marco de la gestión del riesgo antes de continuar con el tratamiento. Además, si no se hubiera realizado la EIPD porque las circunstancias iniciales no obligaban o no lo recomendaban, entonces sería necesario realizar la EIPD desde cero.

5.2 ANÁLISIS

Una vez analizada las obligaciones que suponen la realización de una evaluación de impacto según la normativa actual y, en relación con las actuaciones realizadas por los órganos que constituyen el ámbito subjetivo de esta inspección, tan sólo se tiene constancia de la práctica de EIPD's en el ámbito del SESPA, habiéndose puesto a disposición de esta Inspección las siguientes:

-informe de evaluación de impacto en materia de protección de datos sobre la receta electrónica (e-receta).

-informe de evaluación de impacto en materia de protección de datos sobre los sistemas de Gestión de la asistencia sanitaria a los usuarios instalados en el Servicio Asturiano de Salud del Principado de Asturias (SESPA).

-monitorización de pacientes mediante videocámaras.

Del resto de los tratamientos dependientes de responsables de tratamiento con los que se ha contactado, señalar que, pese a la concurrencia de tratamientos de datos altamente sensibles y de especial protección y alto riesgo para los derechos afectados, lo cierto es que no sólo no se ha informado de la efectiva realización de evaluación de impacto alguna - sin que haya evidencias de su ejercicio-, sino que, de las entrevistas mantenidas, tampoco se tiene constancia de haberse efectuado ningún mínimo análisis de riesgos que pudiera sustentar la idoneidad de oportunas medidas de seguridad implantadas o a implantar.

6 DISEÑO, PROPUESTA Y APLICACIÓN DE MEDIDAS DE SEGURIDAD

6.1 CONTENIDOS

Como ya se había mencionado anteriormente la obligación de gestionar los riesgos va a consistir en seleccionar e implementar las medidas de seguridad más adecuadas para reducir o eliminar los riesgos evaluados, así como establecer mecanismos de control y seguimiento para verificar su eficacia.

A la hora de analizar las medidas de seguridad a aplicar por parte de las Administraciones Públicas, cabe distinguir cuatro aspectos objeto de análisis:

- Deber de confidencialidad en el tratamiento de datos.
- Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
- Brechas de seguridad.
- Medidas de seguridad en el acceso legítimo a datos personales en poder de las administraciones públicas por parte de terceros.

6.1.1 DEBER DE CONFIDENCIALIDAD

Las personas que intervengan en cualquier fase del tratamiento de datos están sujetas al **deber de confidencialidad** y/o, en su caso, secreto profesional (artículo 5 RGPD).

En el ámbito de las administraciones públicas, hemos de destacar la sujeción al **principio de confidencialidad de los empleados públicos** siendo uno de los principios éticos a los que se sujetan estos de acuerdo con lo establecido en el artículo 53.12 del TREBEP ya que se establece que "*guardarán secreto de las materias clasificadas u otras cuya difusión esté prohibida legalmente, y mantendrán la debida discreción sobre aquellos asuntos que conozcan por razón de su cargo, sin que puedan hacer uso de la información obtenida para beneficio propio o de terceras personas, o en perjuicio del interés público*."

En el caso de los funcionarios de la Administración del Principado de Asturias, la Ley 2/2023, de 15 de marzo, de Empleo Público establece en su artículo 142 que regula las faltas disciplinarias, en su apartado 2 que son faltas muy graves:

e) La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función.

f) La negligencia en la custodia de secretos oficiales, declarados así por la ley o clasificados como tales, que sea causa de su publicación o que provoque su difusión o conocimiento indebido.

Y en su apartado 4 son faltas graves:

g) No guardar el debido sigilo respecto de los asuntos que se conozcan por razón del cargo.

Respecto al personal laboral, el V Convenio Colectivo para el personal laboral de la Administración del Principado de Asturias establece en el artículo 50 el régimen disciplinario tipificando como

-faltas graves: *la utilización o difusión indebidas de datos o asuntos de los que se tenga conocimiento por razón del trabajo en el organismo. (*punto 4.11).

-faltas muy graves: *la publicación o utilización indebida de secretos oficiales, así declarados por Ley o clasificados como tales*. (punto 5. 16).

6.1.2 MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS PARA GARANTIZAR UN NIVEL DE SEGURIDAD ADECUADO AL RIESGO

El artículo 32 del RGDP exige la aplicación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

El objetivo principal de la legislación sobre protección de datos es la definición de unas medidas de seguridad, de carácter técnico y organizativo, que pauten el adecuado y seguro tratamiento de los datos personales, que deben incluir, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Estas medidas de seguridad deben atender al riesgo que la entidad identifique, siendo necesario la imposición de más medidas o medidas más robustas cuando el riesgo sea alto, y viceversa.

Además, por tratarse en este caso analizado de entidades del sector público, se deberá atender al Esquema Nacional de Seguridad (ENS) para verificar las medidas que son aplicables de acuerdo a ese marco normativo, siendo extrapolables o aprovechables para la defensa de la privacidad, tal y como se estipula en la disposición adicional primera de la LOPDGDD. [2]

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad viene a sustituir al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, si bien, a fecha actual, se encuentra en el plazo de transitoriedad de veinticuatro meses contados a partir de su entrada en vigor para adecuar los sistemas afectados.

En su artículo 12 establece la obligación de que cada administración pública cuente con una política de seguridad de la información formalmente aprobada por el órgano competente.

Señalar que el principal mandato de la ENS es la aprobación de dicha política de seguridad que consiste "*en el conjunto de directrices que rigen la forma en que una*

[2] *Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.*

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

organización gestiona y protege la información que trata y los servicios que presta" y se establecerá de acuerdo con los principios básicos y se desarrollará aplicando los requisitos mínimos, en proporción a los riesgos identificados en cada sistema. Dentro del instrumento que apruebe dicha política deben incluirse los riesgos que se deriven del tratamiento de datos personales.

6.1.3 BRECHAS DE SEGURIDAD

Los artículos 33 y 34 del RGPD exigen que, en el caso de producirse un incidente, brecha o violación a la seguridad de los datos, se disponga de un previo procedimiento o protocolo de actuación.

Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos. Estas situaciones deben intentar evitarse por los efectos adversos que pueden tener sobre las personas al ser susceptibles de ocasionar daños y perjuicios físicos, materia o inmateriales.

Por ello, la normativa en materia de protección de datos insta, no solo a minimizar el riesgo de que se produzcan, sino también, una vez producido, a una gestión adecuada. En consecuencia, el artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

Asimismo, en el caso de que el responsable considere que no existieran riesgos para los derechos y libertades de las personas físicas también tiene la obligación de documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, permitiendo dicha documentación la autoridad de control verificar el cumplimiento de lo dispuesto en ese artículo.

Finalmente, impone el RGPD, en el artículo 34, la obligación de comunicar al propio interesado sin dilación indebida, por parte del responsable del tratamiento, la violación de la seguridad de sus datos personales que entrañe un alto riesgo para los derechos y libertades de las personas físicas. En todo caso, establece una serie de supuestos en los que no sería necesaria la citada comunicación.

Con el objetivo de ayudar en la obligación de notificar las brechas de datos personales a la autoridad de control, la AEPD ofrece indicaciones en la Guía para la notificación de brechas de datos personales así como otros recursos en su web en el apartado de innovación y tecnología.[3]

Además, la Agencia ha publicado recientemente "Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales", un documento destinado al sector público que aborda la necesidad de gestionar los riesgos derivados del tratamiento de cantidades masivas de datos personales, y su intercambio entre administraciones públicas, tanto para los derechos y libertades de las personas como para la propia sociedad en su conjunto.[4]

[3] Guía para la Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

[4] https://www.aepd.es/es/node/49655

En el documento se insiste en la necesidad de implantar una adecuada política de protección de datos, una cooperación estrecha entre quienes puedan tener atribuidas funciones de gobernanza respecto de tratamientos a los que sean aplicables, incluidas las autoridades de protección de datos y se recomiendan una serie de medidas preventivas, de detección, de respuesta y de revisión y supervisión que se podrían implementar.

Todo ello, teniendo en cuenta que las consecuencias de una brecha masiva de datos personales en el ámbito de las administraciones públicas puede tener un elevado impacto social, por un lado, sobre los derechos fundamentales del individuo y, por otro lado, por el impacto que podría suponer para la garantía del interés público y sus efectos sobre los derechos fundamentales de la propia sociedad, toda vez que las administraciones realizan tratamientos para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos o en el cumplimiento de una obligación legal, que pueden afectar a un gran volumen de población y que la interconexión de infraestructuras para el acceso y el intercambio de datos multiplica la probabilidad de que se materialice una determinada amenaza, más aún si tenemos en cuenta que un incidente puede producir un "efecto dominó", generando quiebras en cadena de las medidas de seguridad en distintos intervinientes.

Advierte la AGPD que "*Los efectos de una brecha masiva pueden generar un gran impacto a nivel social, afectar a las obligaciones de disponibilidad y resiliencia establecidas en el art. 32.1.b del Reglamento General de Protección de Datos (en adelante, RGPD) y, finalmente, pueden generar o ser utilizados para fomentar la desconfianza en los servicios o en la estructura de la Administración del Estado*". De ahí la importancia de estas medidas adicionales a implementar por los múltiples responsables de las Administraciones Públicas que a través de los modelos de interoperabilidad acceden a grandes repositorios de datos.

6.1.4 MEDIDAS DE SEGURIDAD EN EL ACCESO LEGÍTIMO A DATOS PERSONALES EN PODER DE LAS ADMINISTRACIONES PÚBLICAS POR PARTE DE TERCEROS

Ha de tenerse en cuenta que los datos personales recabados por la administración pueden ser tratados o cedidos a entidades privadas, bien a través de convenios de colaboración público-privada, encomiendas, concesiones y contratos por lo que deben incorporarse en los convenios, pliegos de contratación y demás acuerdos las correspondientes cláusulas de confidencialidad.

Respecto a la contratación con terceros que afecta a la materia de protección de datos personales, no debe olvidarse que el cumplimiento por el contratista tanto de la normativa nacional como de la normativa de la Unión Europea en esta materia es una condición especial de ejecución del contrato y tiene el carácter de obligación contractual esencial a los efectos del artículo 211.1 f).

La disposición adicional décimo quinta de la Ley de Contratos del Sector Público (LCSP), que establece la obligación de respetar la normativa de la protección de datos de carácter personal en los contratos que regula dicha ley, también atribuye la condición de encargado del tratamiento al contratista cuando la contratación implique su acceso a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante. Se incluyen además las obligaciones de terceros en el caso de que traten datos personales por cuenta del contratista que tendrá también la consideración de encargado del tratamiento.

La figura del "encargado del tratamiento", recogida en el artículo 28 del RGPD, recae en quien va a realizar un tratamiento, almacenar, procesar datos o información sobre

personas físicas por cuenta y siguiendo las instrucciones del responsable del tratamiento que es quien toma decisiones sobre los fines y los medios en los que los datos son procesados.

La regulación exige que el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Cuando el contratista tenga la consideración de encargado del tratamiento, será necesario que en el contrato o en un documento independiente se incluyan las cláusulas necesarias con objeto de regular este acceso, en los términos y con el contenido previstos en la normativa en materia de protección de datos de carácter personal, y en conformidad con la citada disposición adicional 25 de la LCSP. En particular, se harán constar el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. A su vez, se hará constar si se autoriza que un tercero trate los datos personales por cuenta del contratista.

Cuando finalice la prestación contractual los datos de carácter personal y cualquier apoyo o documento en que consten tienen que ser destruidos o devueltos a la entidad contratante responsable, o al encargado del tratamiento que esta haya designado.

En el supuesto de que la ejecución del contrato no implique el tratamiento de datos personales por parte del contratista, este no está autorizado a hacer ninguna operación sobre datos personales o conjunto de datos personales de las cuales esté enterado de forma accidental o accesoria, y se tiene que abstener de hacer cualquier tratamiento de datos personales no autorizado.

En el supuesto de que, durante la ejecución del contrato, tenga acceso a datos personales, el contratista y su personal están obligados a guardar secreto profesional respecto de estos datos y no podrán utilizar esta información para ninguna finalidad diferente de la derivada de la prestación del servicio.

Esto es, en todo caso, debe garantizarse que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

Por último, hay que recordar que en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, la LOPDGDD ya establece en la disposición adicional primera que las medidas de seguridad se corresponderán con las de la Administración pública de origen y, por lo tanto, se ajustarán al Esquema Nacional de Seguridad.

Señalar que compete, en todo caso, al responsable del tratamiento el asegurarse y garantizar que las personas físicas o jurídicas que, en virtud de contrato o convenio, accedan al tratamiento de datos personales reúnan las condiciones idóneas que garanticen dicho tratamiento con arreglo a las exigencias de la normativa europea y nacional en materia de protección de datos.

6.2 ANÁLISIS

Sobre las medidas de seguridad que se aplican en el ámbito subjetivo de esta inspección, en relación a los cuatro aspectos analizados, se ha constatado lo siguiente:

-Más allá de la normativa en materia de empleo público que establece el deber de confidencialidad en los asuntos que se conozcan en el ejercicio de sus funciones, se

carece de códigos de conducta, circulares o instrucciones dirigidas al personal con indicaciones específicas en esta materia.

-Respecto a las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, como se ha analizado anteriormente, al tratarse de administraciones públicas, en el ámbito del Principado de Asturias, las medidas de seguridad implantadas se corresponden con las previstas en el ENS habiendo sido auditados externamente por AENOR, recibiendo el certificado de conformidad con el Esquema Nacional de Seguridad en cumplimiento de nivel medio (ENS-2019/0009) con renovación bianual, habiéndose realizado la última auditoría en 2021 y estando pendiente la renovación del certificado en el año en curso.

En el ámbito del Principado de Asturias la política de seguridad de los sistemas de información está aprobada mediante Resolución de 19 de septiembre de 2014, de la Consejería de Economía y Empleo (BOPA 30-9-2014), conforme a los requisitos en su día fijado en el RD/2010, de 8 de enero, estando en tramitación la adaptación de la política de seguridad de los sistemas de información en la Administración del Principado de Asturias a la nueva regulación.

Para acometer dicha política y llevar a efecto el cumplimiento de este Esquema Nacional, impulsado por la Dirección General de Seguridad y Estrategia Digital (DGSED) dependiente de la Consejería de Presidencia, se crea Comité de estrategia digital y de seguridad de la información del Principado de Asturias (CEDISI), ya que, según la norma de creación[5] " *se consideró fundamental contar con un órgano con capacidad de coordinación y de desarrollo de políticas y estrategias en esta materia y que estaría compuesto por los directivos y los profesionales públicos que conocen el ámbito de trabajo específico de las tecnologías de la Información y aquellos con funciones en materia de seguridad de la información en el Principado de Asturias. Permitirá también adaptar la seguridad TIC corporativa a los requisitos corporativos de la seguridad de la información, adecuándose ésta a las necesidades de protección de los sistemas y racionalizando los costes mediante la aplicación de políticas comunes y estándares*."

Por su parte, en el ámbito del SESPA se crea el Comité de Seguridad de Sistemas de Información de Salud del Principado de Asturias (COSSISPA)[6] configurado como un grupo de trabajo con funciones de asesoramiento y apoyo, adscrito a la Dirección General con competencias en sistemas de información sanitaria de la Consejería competente en materia de sanidad que "*tiene como finalidad servir de marco de reunión de los responsables del tratamiento de datos personales y de seguridad con el Delegado de Protección de Datos para el desarrollo e implantación de las medidas establecidas por la normativa sobre protección de datos personales, así como para la definición de estrategias coordinadas de seguridad en el ámbito del Servicio de Salud, incluidas sus Áreas Sanitarias."*

-Sobre la existencia de brechas de seguridad, de acuerdo con las entrevistas realizadas, se ha tenido conocimiento de, al menos, una brecha de seguridad de cierta

[5] Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público (BOPA 27-VII-2018).

Decreto 68/2020, de 17 de septiembre, de primera modificación del Decreto 37/2018, de 18 de julio (BOPA 5-X-2020).

6 Resolución de 14 de noviembre de 2018, de la Consejería de Sanidad, por la que se crean el Comité de Seguridad de Sistemas de Información de Salud del Principado de Asturias (COSSISPA) y los Comités de Seguridad de Sistemas de Información de Salud de las Áreas Sanitarias (BOPA 4-XII-2018).

entidad recientemente comunicada a la AEPD sin que exista, más allá de la ayuda mencionada de la Agencia con las publicaciones en su web, constancia de un protocolo, guía o modelo de comunicación ni procedimiento de gestión de incidentes en la materia, ni de valoración del riesgo para determinar la procedencia o no de comunicación al interesado, ni tampoco de un inventario de incidencias que permita extraer lecciones aprendidas de la revisión de las situaciones sucedidas y la valoración de la eficacia de las acciones correctivas, en su caso.

-En relación con las medidas de seguridad en el acceso legítimo a datos personales en poder de la administración por parte de terceros, se constata que en alguno de los convenios de colaboración de la Administración del Principado de Asturias con entidades, asociaciones de carácter privado recientemente publicados se incluye en el convenio un apartado relativo a la protección de datos en el que las partes se sujetan respecto al intercambio de información a los principios de confidencialidad, integridad, disponibilidad, información y transparencia, responsabilidad y deber de secreto profesional en el marco del cumplimiento de la normativa en la materia.

Examinados algunos convenios de colaboración público-privada que implican el manejo de datos en materias sensibles, como salud, servicios sociales o información de los contribuyentes se constata que se incluyen cláusulas relativas al carácter de reservados y secretos de los datos que son objeto de cesión y tratamiento, al deber de confidencialidad y al compromiso de las parte del cumplimiento de la normativa en materia de protección de datos personales así como a la adopción de todas aquellas medidas a su disposición según el estado de la tecnología para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los mismos.

No obstante, más allá de los compromisos genéricos de sujeción a la normativa en vigor, se aprecia una falta de definición clara de los roles que desempeña cada una de las entidades así como de concreción en las obligaciones de cada una de las partes

Todas estas condiciones y requisitos se ha comprobado que se incluyen en algunos modelos de pliegos de cláusulas administrativas particulares a las que se incorporan modelo de contrato de encargado del tratamiento de datos que se incorpora al contrato que se formalice entre las partes.

Sin embargo, no se ha podido acreditar que se incluyen en todos los casos ni que en la ejecución del contrato exista un control o supervisión de su cumplimiento más allá de la que la que proactivamente pueda realizar el responsable del contrato. Tampoco se suelen exigir mayores garantías como auditorías favorables, certificaciones, etc.

En este sentido, con carácter general no se acredita que se tenga en cuenta el Esquema Nacional de Seguridad para la transmisión de medidas de acuerdo al nivel de seguridad del adecuado servicio.

7 SUJECIÓN DE LAS ACTIVIDADES DE TRATAMIENTO DE DATOS A UNA PREVISIÓN Y GESTIÓN LLEVADA A CABO DESDE LA PRIVACIDAD

7.1 CONTENIDOS

Como se ha expuesto, es **tratamiento** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Por lo tanto, cualquier tipo de acción que se realice sobre un dato personal se considera tratamiento de datos personales, tanto si es tratamiento automatizado de datos personales como no automatizado, siempre que después se incluyan en un fichero o archivo estructurado al que se pueda tener acceso.

El RGPD establece en su artículo 5 los siguientes principios que es necesario tener en cuenta en la definición y práctica de cualquier tratamiento:

1. Licitud, lealtad y transparencia.
2. Limitación de la finalidad.
3. Minimización de datos.
4. Exactitud.
5. Limitación del plazo de conservación.
6. Trazabilidad.
7. Integridad y confidencialidad.

Por su parte, el apartado 2 del artículo 25 del RGPD establece que:

"*El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*"

Esto es, el RGPD exige del responsable una configuración por defecto de los tratamientos que sea respetuosa con los principios de protección de datos, abogando por un procesamiento mínimamente intrusivo:

- mínima cantidad de datos personales,
- mínima extensión del tratamiento,
- mínimo plazo de conservación
- mínima accesibilidad a datos personales.

Todo ello, además, sin que sea necesaria la intervención del interesado para garantizar que estos mínimos están establecidos.

Para su cumplimiento se requiere la práctica de una serie de actuaciones, como son, entre otras:

-Fijar criterios de recogida limitados a la finalidad que persigue el tratamiento.

-Acometer un tratamiento sólo si la finalidad de éste no pudiera lograrse razonablemente por otros medios.

-Adoptar todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos.

-Restringir los accesos a los datos personales a las partes implicadas en los tratamientos atendiendo al principio de mínimo conocimiento "need to know" , el cual ha de garantizar que cada persona de la organización acceda a lo que necesita saber, ni más ni menos, para lo cual, según la función que realicen, se deben crear perfiles

de acceso diferenciados. Este análisis se deberá realizar para cada una de las fases del tratamiento.

-Definir plazos estrictos de conservación y establecer mecanismos operativos que garanticen su cumplimiento. La destrucción segura y garantizada de la información al final de su ciclo de vida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

Junto a lo expuesto, los tratamientos de datos personales están legalmente sujetos a los principios de visibilidad y transparencia, exigiéndose de los responsables su fomento adoptando una serie de medidas tales como, entre otras:

-Hacer públicas las políticas de privacidad y protección de datos que rigen el funcionamiento de la organización.

-Desarrollar y publicar cláusulas de información concisas, claras e inteligibles, que sean fácilmente accesibles y que permitan a los interesados comprender el alcance del tratamiento de sus datos, los riesgos a los que pueden verse expuestos, así como el modo de hacer valer sus derechos en materia de protección de datos.

7.2 ANÁLISIS

De lo observado en el contenido publicado de los Registros de Actividades de Tratamiento, así como de la información recabada en las entrevistas mantenidas, cabe sostener que no existe constancia de una actividad explícita, previa y programada tendente a observar el cumplimiento de los principios recogidos en el artículo 5 del RGPD, comprensivos de un tratamiento mínimamente intrusivo.

Así, no se ha puesto de manifiesto, ni facilitado la aprobación de criterios expresos y documentados con arreglo a los cuales se lleve a cabo la recogida y tratamiento de datos que garanticen en todo caso y en función de la sensibilidad de los datos y del tratamiento, un procesamiento mínimo intrusivo.

Igualmente, respecto al plazo de conservación, se advierte una generalizada e indiscriminada remisión a la normativa en materia de gestión documental[7], sin distinguir en función de las diferentes fases del tratamiento y sin existir mecanismos implantados que garanticen la limitación temporal de su conservación, careciéndose de plazos programados para su revisión periódica.

Tampoco se documentan ningún tipo de medidas a través de las cuales se garantice la exactitud e integridad de los datos recogidos y tratados a través de las distintas fases que integran el ciclo de dicho tratamiento, existiendo almacenamiento de datos que se contradicen entre sí.

[7] Ley del Principado de Asturias 1/2001, de 6 de marzo, de Patrimonio Cultural.

Resolución de 22 de marzo de 2016, de la Consejería de Presidencia y Participación Ciudadana, por la que se aprueba la Política de Gestión de Documentos del Principado de Asturias

8 GARANTÍA DEL EJERCICIO DE DERECHOS

8.1 CONTENIDOS

La normativa vigente en esta materia precisamente tiene por objetivo principal proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. Los tratamientos de datos personales se rigen por los principios generales de la protección de datos recogidos en el artículo 5 del RGPD y en el artículo 4 LOPDGDD.

El capítulo III del Reglamento recoge todos los derechos que corresponden a los interesados en relación al tratamiento de sus datos personales, exigibles ante el responsable del tratamiento, siendo los siguientes:

-**derecho de acceso:** derecho a obtener confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a una serie de información recogida en el artículo 15 del RGPD.

-**derecho de rectificación:** derecho a obtener sin dilación indebida la rectificación de los datos personales inexactos que le conciernan o a que se completen los datos personales que sean incompletos.

-**derecho de supresión ("al olvido"):** derecho a obtener sin dilación indebida la supresión de los datos personales que le conciernan cuando concurra alguna de las circunstancias enumeradas en el artículo 17 del Reglamento tales como que hayan dejado de ser necesarios para los fines que fueron recogidos, la retirada del consentimiento prestado, hayan sido tratados ilícitamente, etc. Además, en determinados supuestos, es posible ampliar este derecho a la supresión de todo enlace a los datos, o las copias o réplicas de estos, esto es, el derecho al olvido.

-**derecho de limitación:** derecho a obtener la limitación del tratamiento de los datos mediante la suspensión cuando se impugne la exactitud de los datos durante el plazo que permita al responsable su verificación o cuando se haya ejercido la oposición al tratamiento de los datos en base en base al interés legítimo o misión de interés público, mientras el responsable verifica si estos motivos prevalecen sobre los del interesado.

También incluye el derecho a solicitar la conservación de los datos cuando el tratamiento sea ilícito y el interesado se haya opuesto a la supresión de sus datos solicitando la limitación de su uso o cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

-**derecho de portabilidad:** derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento, cuando el tratamiento se efectúe por medios automatizados siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable.

-**derecho de oposición:** derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en una misión de interés público o en el interés

legítimo o cuando tenga como finalidad la mercadotecnia directa el incluida la elaboración de perfiles sobre la base de dichas disposiciones.

El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

-derecho de no ser objeto de decisiones individualizadas automatizadas: derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, con las excepciones de aplicación que recoge el artículo 22 del RGPD.

-derecho de información: el responsable del tratamiento debe satisfacer el derecho de los interesados a ser informados acerca del tratamiento de los datos, de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo (artículos 12, 13 y 14 RGPD; artículo 11 LOPDGDD).

Para dar cumplimiento a este derecho, la AEPD recomienda que esta información se facilite por capas o niveles de manera que se disponga de una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos personales y se remita el resto, en un medio más adecuado para su presentación, compresión y, si se desea, archivo. En el caso de que los datos personales no hayan sido obtenidos directamente del interesado, además de la información básica recogida en el artículo 13, se debe añadir en la información básica de la primera capa, la fuente o procedencia de los datos y en la información adicional de la segunda capa, la información detallada del origen de los datos, incluso si proceden de fuentes de acceso público la categoría de datos que se traten.

Finalmente, el ejercicio de esos derechos debe quedar garantizado, por parte del responsable del tratamiento, mediante la atención de las solicitudes de ejercicio de derechos de los interesados, en tiempo y forma (artículos 15 a 22 RGPD; artículos 12 a 18 LOPDGDD).

8.2 ANÁLISIS

La adaptación a la obligación de proporcionar la información mediante capas o niveles y ajustarse a los requisitos de la nueva normativa y las recomendaciones de las autoridades de protección de datos, dio lugar en esta Administración a que se elaborasen unas instrucciones cuyo objeto era orientar acerca de las mejores prácticas para dar cumplimiento a la obligación de informar a los interesados mediante la normalización de los formularios electrónicos competencia del Servicio de Procesos Administrativos y que son accesibles a través de la sede electrónica (https://sede.asturias.es).

El documento de fecha 3 de mayo de 2018 denominado "Instrucciones para usuarios: Adaptación de los formularios electrónicos normalizados al Reglamento General de Protección de Datos", accesible en la intranet del Principado, permite realizar la adaptación de los formularios a las nuevas exigencias legales, recogiendo la información por capas, como así se hace en la mayoría de los casos.

En consecuencia, con carácter general, se realizado la citada adaptación de los formularios si bien se ha detectado todavía que algunos delos publicados en la web están desactualizados figurando referencias a la normativa anterior recogida en la LO 15/1999.

En algunos casos, la información proporcionada adolece de los mismos defectos observados en los registros de tratamiento de datos publicados que corresponden a los procedimientos a que se vinculan los formularios: falta de información sobre el delegado de protección de datos, incumplimiento del principio de minimización de datos, incorrección en la elección de la base jurídica del tratamiento, ambigüedad en los destinatarios, falta de concreción de los plazos de conservación o de las medidas de seguridad implementadas, designación como encargado de tratamiento al Centro de Gestión de Servicios Informáticos (CGSI), etc.

Además, en el ámbito de la Administración del Principado de Asturias está a disposición de los ciudadanos un formulario normalizado denominado "DECO0022T01 - Reconocimiento del derecho a la protección de datos personales de las personas físicas: Formulario para poder ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición de las personas físicas con respecto a sus datos personales relacionados con las decisiones individuales automatizadas." [8]

Desde su aprobación, sólo han entrado 7 solicitudes, 3 en el 2020, 2 en 2021 y 2 en 2022 en el ámbito Consejerías. (4 a Presidencia, 1 a Hacienda, 1 a Educación y otra a Ciencia, Innovación y Universidad).

Asimismo, se ha dado de alta un procedimiento en SITE dentro del grupo de procedimientos "declaraciones y comunicaciones de los interesados" pero hasta el momento no se han tramitado por esta vía, por lo que es difícil de comprobar la respuesta que se ha llevado a cabo por cada uno de los responsables de tratamiento a los que se han dirigido las solicitudes.

Sin embargo, en el caso del SESPA, se ha implementado un procedimiento para el ejercicio de estos derechos desde el 2022, centralizado en servicios centrales, contando con un registro de dichas solicitudes que, hasta este momento, ha tramitado la solicitud del ejercicio de sus derechos de un total de 129 interesados.

También cuentan con el registro de información sobre la trazabilidad de los accesos a las historias clínicas teniendo en cuenta que la información relativa a la asistencia sanitaria que recibe la persona reclamante por parte de la red pública de salud es "información pública" a efectos del artículo 2.b de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTC), que establece, como criterio general, que el derecho de acceso a la información pública sólo puede ser denegado o restringido por las causas expresamente establecidas por las leyes (artículo 20 y ss. LTC).

Precisamente, la desatención al ejercicio al derecho de acceso a la historia clínica de un residente en el organismo autónomo ERA adscrito a la Consejería de Derechos Sociales por parte de su hija, dio lugar a que la AGPD sancionase con apercibimiento a la Consejería por una infracción del artículo 58.2 del RGPD, tipificada en el artículo 83.6 del RGPD, y en el artículo 72.1 m) de la LOPDGDD (expte. nº PS/00175/2021). Esto es, se sancionó por haber incumplido lo dispuesto en una resolución dictada por la AGPD en la que se acordaba estimar la admisión a trámite de la reclamación presentada por la recurrente instando a la Consejería para que remitiese a la parte reclamante

[8] https://sede.asturias.es/-/dboid-62690000128800831075 73?redirect=%2Fbuscador%3F_pa_sede_buscadorgeneral_web_portlet_mini_BuscadorGeneralMiniPortlet_formDate%3D1687866621598%26p_r_p_searchText%3DDECO0022T01%26p_auth%3D

certificación en la que hiciese constar haber atendido el derecho de acceso ejercido por ésta o denegado motivadamente indicando las causas por las que no procediese atender su petición.

9 ELABORACIÓN, LLEVANZA Y ACTUALIZACIÓN DEL REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO Y PUBLICIDAD ACTIVA DEL INVENTARIO DE ACTIVIDADES DE TRATAMIENTO

9.1 CONTENIDOS

Dentro de las obligaciones de documentación contempladas en la normativa sobre protección de datos, se encuentra la llevanza y actualización, por parte de los responsables y encargados, de un **Registro de las actividades de tratamiento** bajo su propia responsabilidad.

La finalidad de este registro se basa en el principio de responsabilidad proactiva, y requiere que las organizaciones analicen qué datos personales tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo, siendo una herramienta que permite tener una perspectiva general de todas las actividades de tratamiento de datos que la organización está llevando a cabo.

Dicha obligación corresponde tanto al responsable del tratamiento como el encargado, estando exentas de configurar este registro de actividades las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Los registros, por norma general, deben estar elaborados en soportes que permitan un acceso rápido y seguro, permitiendo actualizar la información contenida cuando sea necesario.

El contenido del Registro de Actividades de Tratamiento constituye una información mínima exigible. Este registro podría integrarse y formar parte de los catálogos de procesos que ya existiesen en la entidad, incluyendo toda la información que el responsable considere necesaria para proteger los derechos y libertades de las personas físicas y poder demostrar cumplimiento atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los posibles orígenes de los riesgos que dicho tratamiento pudiera suponer para los interesados. El registro podría incluir aspectos que faciliten la aplicación efectiva de la responsabilidad proactiva como: análisis de riesgos para los derechos y libertades realizados, la descripción sistemática del tratamiento, los sistemas de información sobre los que se apoya, la descripción de la identidad de los encargados del tratamiento, las garantías previstas para llevar a cabo transferencias internacionales de datos, información de contacto de las personas o los departamentos de la organización que se encuentran implicados en las operaciones de tratamiento, etc.

Responsables y encargados tienen obligación de colaborar con la autoridad de control competente y, por tanto, de poner a disposición de esta, previa solicitud, los registros de actividades de tratamiento cuando sean requeridos para supervisar las operaciones de tratamiento.

Junto con la elaboración, llevanza y actualización del registro de actividades de tratamiento, las administraciones públicas (entre otros sujetos) han de hacer público el **Inventario de sus actividades de tratamiento** de manera que sea accesible por

medios electrónicos (Art. 31.2 LOPDGDD) donde se incluya, para cada actividad de tratamiento:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- la base jurídica del tratamiento;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad. En dicha descripción general debe evitarse cualquier información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad. Se recomienda contar con el Responsable de Seguridad o CISO (*Chief Information Security Officer*) con carácter previo a la publicación de dicha descripción general o, en su caso, utilizar una referencia general a los estándares de seguridad utilizados.

9.2 ANÁLISIS

Examinadas las páginas web de los sujetos analizados se advierte lo siguiente:

-Aparecen con la denominación de Registros de Actividades de tratamiento los relativos a las diez consejerías, así como los del Ente Público de Servicios Tributarios, SEPEPA y SESPA.

-Varios de dichos registros no están actualizados (algunos de ellos tienen fecha de actualización de mayo de 2022)

-Respecto al contenido:

- No se cumplimenta el contenido legal mínimo en todos los casos.
- La categorización de los tratamientos es heterogénea, agrupándose en ocasiones por procedimientos concretos y en otros por categorías procedimentales genéricas. En los supuestos en los que se acude a la agrupación por procedimientos concretos se advierte que los incluidos en el correspondiente Registro no se corresponden, en ocasiones, con la totalidad de los ejecutados por la consejería, organismo o ente.
- Incorrectas identificaciones de las bases de legitimación, invocando en varias ocasiones el consentimiento como causa única en aquellos tratamientos que responden al ejercicio de obligaciones legales o ejercicio de poderes públicos.
- Respecto a la descripción de las categorías de datos personales, éstas denotan ausencia de aplicación de los principios de minimización.
- Incorrecta identificación de los encargados del tratamiento.

- Genérica remisión a los plazos contenidos en el Cuadro General de Conservación de Documentos Administrativos del Principado de Asturias, plazos que atienden a la satisfacción de finalidades distintas de las propias de la protección de datos personales.
- Respecto al delegado de protección de datos, la información se limita a la aportación de un correo electrónico.

10 CONTROLES DE CUMPLIMIENTO

10.1 CONTENIDOS

Como establece el principio de responsabilidad proactiva en el artículo 24.1 del RGPD, las medidas y garantías implementadas han de estar documentadas y recoger la información suficiente para permitir, de forma satisfactoria y demostrable, acreditar el cumplimiento del RGPD. Esta documentación ha de permitir la trazabilidad de las decisiones tomadas y de las comprobaciones realizadas siguiendo los principios de minimización antes señalados.

A efectos meramente orientativos cabe identificar los siguientes controles básicos que cabría tomar en consideración para determinar la adaptación del tratamiento a la normativa reguladora. Se trataría, en todo caso, de una serie de verificaciones que deberían considerarse circunscritas a auditorias integradas en el marco propio de la protección de datos. Así:

1.- Comprobar que está disponible en la entidad responsable la documentación necesaria para aplicar la política de protección de datos de forma objetiva; en particular, la definición de roles y obligaciones de los miembros de la organización, la política de control de accesos, la política de información y cualquier otra documentación significativa.

2.- Comprobar que la entidad tiene implementados procedimientos que garanticen el cumplimiento de las políticas anteriores y que están operativos.

3.- Comprobar que está disponible la información básica relativa al tratamiento, en particular, sobre la naturaleza, el ámbito, el contexto y los fines, así como el análisis de proporcionalidad y necesidad.

4.- Tener documentado un análisis del tratamiento y comprobar que el análisis de tratamiento se ha descompuesto en fases e identificar para cada fase las operaciones, la implementación organizativa y técnica, los datos personales y los intervinientes internos y externos

5.- Comprobar que el ciclo de vida de los datos está ajustado a los casos de uso.

6. Comprobar que el responsable no obliga al usuario a aceptar un tratamiento más intrusivo (mayor cantidad de datos o una mayor extensión en las operaciones) como condición para acceder a un servicio.

7.- Comprobar que se han implementado medidas de seguridad.

8.- Comprobar la posibilidad de revocar elecciones en cualquier momento con la misma facilidad con la que fueron seleccionadas.

En consecuencia, sería importante que se procediese con una supervisión rutinaria y habitual de las prestaciones que se realicen a nivel de seguridad de la información y obligaciones en materia de protección de datos personales, con el objetivo de confirmar o auditar que se han respetado todas las medidas acordadas. No llevar a

cabo un mínimo seguimiento en este sentido podría provocar el incumplimiento contractual y legal del encargado del tratamiento sin que fuera detectado por parte de la entidad, con el correspondiente impacto que podría suponer.

10.2 ANÁLISIS

A excepción del SESPA en que sí se documentan la existencia de auditorías externas, el resto de las consejerías y organismos analizados carecen de actuaciones de control documentadas, exponiendo en las entrevistas realizadas la ausencia de su realización.

Todo ello al margen de los controles de seguimiento y comprobación que se llevan a cabo en el marco de las políticas de seguridad de la información, que si bien –como se ha expuesto- están íntimamente interrelacionadas con las de la protección de datos, responden a una finalidad y regulación diferenciadas.

11 IMPLEMENTACIÓN DE LA ESTRUCTURA ORGANIZATIVA Y COMPETENCIAL PARA LA PROTECCIÓN DE DATOS PERSONALES, CON ESPECIAL REFERENCIA A LA ASUNCIÓN DE LAS FUNCIONES LEGALMENTE ATRIBUIDAS A LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS

11.1 CONTENIDOS

La reiterada obligación impuesta por el RGPD en orden a la adopción de medidas técnicas y organizativas apropiadas, que posibiliten el cumplimiento del mismo, determina la necesidad de aprobar políticas internas en materia de protección de datos personales que configuren las medidas con las que se cumplan, en particular, los principios de protección de datos desde el diseño y por defecto.

Uno de los contenidos oportunos de dichas políticas internas ha de estar orientado a la configuración organizativa de las distintas unidades administrativas responsables e intervinientes activos en la gestión de los respectivos tratamientos de datos que se lleven a cabo.

Es por ello que se estima necesario regular, en el ámbito de las administraciones públicas, la organización competencial que se estime adecuada para una diligente gestión de los tratamientos de datos personales así como de su protección.

Así, se debe acometer, en primer término, una atribución orgánica de la competencia relativa a la gestión de esta materia, residenciando las competencias en una determinada consejería o estructura orgánica. Dicha atribución puede hacerse coincidir, si así se estima oportuno, con la propia de la gestión y organización de la seguridad de la información, al ser ambas (seguridad de la información y protección de datos) íntimamente dependientes.

Asimismo, con independencia de que cada consejería y, en su caso, organismo o ente, estén individualmente obligados al cumplimiento de la normativa en la materia, resulta necesario acometer una política de protección de datos que, siendo de aplicación a la administración general y, en su caso, organismos, dote de coherencia, dirección, coordinación, eficacia y supervisión a toda la gestión de tratamientos de datos imputables a la organización. Se trata, en todo caso, de dar cumplimiento con ello al principio de responsabilidad proactiva. A tal efecto el RGPD establece, en su artículo 24, como obligaciones generales la aplicación de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento. Entre las medidas mencionadas se incluirá la aplicación de las oportunas políticas de protección de datos. Cabe, asimismo, extender el alcance de la

política de protección de datos a las previsiones y requisitos del Esquema Nacional de Seguridad bajo la consideración que esta última forma parte de la seguridad de la información, lo que se desprende de la inclusión de ambas materias en el derecho de la ciudadanía a que refiere el artículo 13 h) de la Ley 39/2015, de 1 de octubre.

El RGPD recoge la necesidad de establecer claramente el mapa de intervinientes en todo tratamiento de datos, al objeto de determinar con acierto la atribución de responsabilidades de acuerdo con la citada norma. Por tanto, cualquier actividad que conlleve el tratamiento de datos personales será atribuible a algún sujeto que cumpla los requisitos de las distintas categorías que ofrece el RGPD.

En efecto, se estima imprescindible en orden a la satisfacción del principio de responsabilidad proactiva, diseñar una política de protección de datos en la que, entre otros aspectos, se definan y delimiten las distintas responsabilidades orgánicas que intervienen en la gestión de la protección de datos, distinguiendo entre:

1.- Aquellos a los que se atribuyen funciones de coordinación y dirección de las actuaciones relativas al cumplimiento de las obligaciones legales en materia de protección de datos personales:

·Consejería/s competente/s u otros órganos directivos

·Unidades de coordinación e informe.

2.- Aquellos que intervienen en la implementación:

·Responsable y corresponsable del tratamiento.

·Encargados del tratamiento.

3.- Aquellos que intervienen en la asistencia activa y/o la supervisión:

·Delegado/s de protección de datos.

·Unidades organizativas de gestión de servicios comunes.

En efecto, junto a los perfiles de obligada existencia legal – responsable, encargado y delegado- se pueden arbitrar figuras potestativas que conformen la estructura funcional con responsabilidades en la materia, como pueden ser las unidades de coordinación e informe, que pueden adoptar la forma de órgano colegiado, con una conformación multisectorial y con adscripción funcional a la consejería competente en materia de protección de datos y a los que se pueden atribuir funciones de coordinación e informe preceptivo en relación con la adopción de planes, proyectos e iniciativas en la materia o en la resolución de conflictos intersectoriales.

En cualquier caso, respecto a los perfiles de existencia obligatoria, si bien las funciones propias de los responsables, encargados y delegados de protección de datos están legalmente definidas, tanto en la normativa europea como en la nacional, resulta necesario determinar la configuración orgánica de dichas figuras, a fin de evitar disfunciones en dicha atribución en función de las respectivas consejerías, organismos y entidades.

En efecto, la atribución orgánica de la condición de **responsable del tratamiento** puede recaer, bien en las consejerías, o bien en órganos directivos distintos, si así se estima oportuno y teniendo en cuenta en todo caso la atribución competencial propia o delegada con la que se delimiten los fines y modos del tratamiento. Pero en cualquier caso resulta necesaria la conformación de criterio uniforme al respecto para toda la administración a fin de evitar la dispersión, carente de justificación, que se aprecia en muchas ocasiones en la identificación de los respectivos responsables del tratamiento

que va desde los titulares de las consejerías hasta niveles orgánicos de jefaturas de servicio o sección.

Junto a esta figura, el RGPD define en su artículo 26, el **corresponsable del tratamiento** determinando el régimen jurídico a que debe someterse:

"1. *Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados*".

El RGPD define en su artículo 4.8) la figura del **encargado del tratamiento** o encargado como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*".

También resulta imprescindible determinar las condiciones jurídicas que configure el estatuto funcional del delegado de protección de datos, que ostenta por imperativo normativo europeo de unas especiales condiciones legales de garantías legales para su desempeño, además de desarrollar una función de supervisión en la gestión de la protección de datos por parte de cualquier órgano incluidos los directivos y también todas las unidades administrativas.

La función del delegado de protección de datos será la de prestar al responsable la asistencia y asesoramiento necesarios en el proceso de adopción de las medidas y supervisar que las mismas se han adoptado y se llevan a la práctica. Es decir, el delegado de protección de datos asesora al responsable y controla el cumplimiento de las obligaciones establecidas por la normativa de protección de datos de carácter personal.

La figura del delegado de protección de datos adquiere una destacada importancia en el RGPD (artículos 37 a 39) y así lo recoge la LOPDGDD, que parte del principio del carácter obligatorio en los supuestos que determina, pudiendo estar o no integrado en la organización del responsable o encargado y ser, tanto una persona física, como una persona jurídica.

Si bien es cierto que puede recaer en un órgano colegiado, dada la redacción literal de la ley, dicho órgano ha de tener personalidad jurídica (persona jurídica), no pudiendo, en consecuencia, atribuirse dicha condición y funciones a órganos colegiados que carezcan de la misma.

Asimismo, se exige en todo caso, que la designación y funciones no recaiga en personas (físicas o jurídicas) que tenga atribuidas funciones que conlleven un conflicto de intereses al tener que ejecutarse de manera simultánea a las que son legalmente propias de la figura del DPD. En todo caso, el carácter asesor y supervisor del DPD, impide que se puedan implicar la intervención directa en la toma de decisiones referidas a los fines y medios del tratamiento, ya que afectaría a su independencia e implicarían la existencia de un conflicto de intereses. De este modo, la necesaria independencia del DPD y la necesidad de evitar los conflictos de intereses impide asignarle responsabilidades directas en un ámbito que va a tener que supervisar y en el que estaría sujeto a instrucciones de otros órganos.

La ausencia de conflicto de intereses está estrechamente ligada al requisito de actuar de manera independiente. Aunque los DPD puedan tener otras funciones, solamente podrán confiárseles otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso (Directrices sobre los delegados de protección de datos adoptadas por el Grupo de Trabajo sobre Protección de Datos del Artículo 29).

El documento elaborado por la Agencia Española de Protección de Datos denominado "El delegado de protección de datos en las Administraciones Públicas" añade lo siguiente:

"*El RGPD prevé que el DPD podrá desarrollar su actividad a tiempo completo o a tiempo parcial y también que podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. En órganos, organismos o entes de gran tamaño en que exista un único DPD lo habitual será que desempeñe sus funciones a tiempo completo. Es, incluso, posible que el DPD formalmente nombrado esté respaldado por una unidad específicamente dedicada a la protección de datos. El DPD actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos.* "

De lo anterior se extrae que, al margen de la fórmula adoptada para su nombramiento, la designación del delegado de protección de datos ha de responder a las exigencias derivadas del principio de independencia en el desarrollo de su actividad, **debiendo garantizarse que el desempeño de sus funciones y cometidos no den lugar a conflicto de intereses.**

El artículo 36.2 de la LOPDGDD establece lo siguiente:

"2. *Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses."*

En definitiva, si bien la Sección 4 del Capítulo IV, del RGPD -artículos 37 a 39-, contempla para los DPD amplias posibilidades en cuanto a su nombramiento y encuadre en la organización de las entidades a las que se refiere su designación, no es menos cierto que dicha autonomía debe conciliarse con las exigencias derivadas del principio de independencia del delegado, debiendo garantizarse que el ejercicio de sus funciones no dé lugar situaciones de incompatibilidad, ni a conflicto de intereses.

Por otro lado, y en cuanto a la **configuración orgánica de la figura del delegado de protección de datos**, señalar que el artículo 37, apartado 2, del RGPD permite a un grupo empresarial designar un único DPD, siempre que este "sea fácilmente accesible desde cada establecimiento". Según el Grupo de Trabajo Sobre Protección de Datos del artículo 29, la noción de accesibilidad se refiere a las tareas del DPD como punto de contacto con respecto a los interesados y a la autoridad de control, pero también internamente dentro de la organización. Esto es, se podrá designar un único DPD para varios organismos públicos, pero la decisión de nombrar un único delegado o varios ha de venir determinada por la estructura organizativa y el tamaño de la entidad, así como por la naturaleza, sensibilidad y el volumen de datos a tratar.

Como solución organizativa intermedia entre un único o varios delegados, algunas administraciones optan por una denominada "gestión sectorial de la protección de datos", mediante la figura de los delegados adjuntos, respecto de los cuales el DPD ejerce la supervisión funcional de sus actuaciones.

Así mismo es necesario tener en cuenta que, en función del tamaño y la estructura de la organización, puede ser necesario establecer un equipo de DPD (un DPD y su personal). En esos casos, deben delimitarse con claridad la estructura interna del equipo y las tareas y responsabilidades de cada uno de sus miembros. Se trata ésta de una decisión organizativa que ha de tenerse muy presente a fin de dar cumplimiento a la obligación que pesa sobre el responsable del tratamiento de dotar al delegado de los medios personales y materiales necesarios para el ejercicio de sus funciones con independencia y autonomía.

Prosiguiendo con el aspecto organizativo, y por lo que a la adscripción orgánica del DPD se refiere, señalar que la misma se tiene que compadecer con las notas de independencia y autonomía en el ejercicio de sus funciones; y por otra parte, la íntima interdependencia entre las políticas de protección de datos y las políticas de seguridad de la información aconsejan que se tome en cuenta los beneficios de una misma adscripción orgánica para ambas, esto es, residenciando en una misma consejería la atribución de ambas competencias.

Por lo que a las **exigencias de idoneidad** se refiere en orden al desempeño de las funciones, el artículo 37, apartado 5, del RGPD establece que el delegado de protección de datos "*será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39*". El considerando 97 dispone que el nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos que se realicen y de la protección exigida para los datos personales tratados.

Esto es, si bien el nivel de conocimientos requerido no está definido estrictamente, debe ser acorde con la sensibilidad, complejidad y cantidad de los datos que una organización trata. Asimismo, ha de atenderse al conocimiento de la organización del responsable y de las operaciones de tratamiento que se llevan a cabo y en el caso de una autoridad u organismo público, el DPD debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización.

Finalmente, señalar que el artículo 37, apartado 7, del RGPD requiere que el responsable o el encargado del tratamiento publique los datos de contacto del DPD y los comunique a las correspondientes autoridades de control. El objetivo de dichos requisitos es garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades de control puedan contactar de forma fácil y directa con el DPD, sin tener que contactar con ninguna otra parte de la organización.

Como una buena práctica, el Grupo de Trabajo del artículo 29 recomienda también que las organizaciones informen a sus empleados del nombre y datos de contacto del DPD. Por ejemplo, el nombre y los datos de contacto del DPD podrían publicarse internamente en la intranet de la organización, en el directorio telefónico interno y en el organigrama.

Concluyendo, en síntesis, respecto al delegado de protección de datos, ha de tenerse presente las siguientes notas.

- Su nombramiento es obligatorio para las administraciones públicas.
- Puede estar integrado o no en la organización.

- Puede ser persona física o jurídica, con lo que si bien puede recaer en un órgano colegiado, éste ha de estar dotado de personalidad jurídica.
- Puede tener una dedicación exclusiva o compartida con el ejercicio de otras funciones, pero siempre y cuando entre éstas y las propias del delegado no haya riesgo de conflicto de intereses.
- Su configuración orgánica puede ser la de un único delegado para todas la administración y sus organismos, varios, o incluso acudirse a la figura de los delegados adjuntos. Para ello ha de valorarse el tamaño de la organización, el volumen, naturaleza y sensibilidad de los datos a tratar.
- Su adscripción orgánica ha de garantizar la independencia y autonomía en el ejercicio de sus funciones, siendo oportuno valorar la adscripción única de las políticas de protección de datos y las de seguridad de la información.
- Su nombramiento, así como sus datos de contacto, han de comunicarse a la Autoridad de Control, siendo recomendable la puesta en conocimiento de dicha información a todo el personal de la administración.

11.2 ANÁLISIS

Examinados los respectivos decretos de estructuras orgánicas vigentes, se advierte ausencia de atribución competencial a ninguna de las consejerías en orden a la asunción de funciones en materia de dirección, impulso, coordinación de la protección de datos en el conjunto de la administración autonómica.

Tampoco se advierte atribución competencial en dicha materia en relación con los respectivos ámbitos competenciales de los organismos autónomos o consejerías, a excepción de la Consejería de Salud, cuyo Decreto 83/2019, de 30 de agosto atribuye en su artículo 3.e) al Servicio de Asuntos Generales y régimen Presupuestario, adscrito a la Secretaría General Técnica, las funciones relativas a "*La gestión del registro de las actividades de tratamiento efectuadas por los órganos de la Consejería, de conformidad con el artículo 30 del 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 y por el que se deroga la Directiva 95/46/CE.*"

Por su parte, la Relación de Puestos de Trabajo adscritos a la Consejería de Educación contempla un puesto de Técnico Asesor adscrito a la Secretaría General Técnica a la que se atribuye el "*Desarrollar, promover la ejecución, supervisar y controlar las medidas técnicas necesarias para el adecuado tratamiento de los datos de carácter personal en el ámbito educativo conforme a la legislación sectorial aplicable*".

Asimismo, según lo dispuesto en el artículo 32.2, apartado b), del Convenio Colectivo del personal laboral de la Entidad Pública 112 Asturias (BOPA 08/08/2007), se establece el complemento específico que retribuye la responsabilidad de coordinar y controlar las medidas de seguridad aplicables a los ficheros que contenga datos de carácter personal y protegidos por la Ley Orgánica 15/1999, de 12 de diciembre, de protección de datos de carácter personal, en la actualidad Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Se advierte, en definitiva, una ausencia competencial de las funciones relativas a la protección de datos personales, tanto de carácter transversal (competencias residenciadas en una determinada consejería y de general aplicación) como de naturaleza sectorial (referenciadas al respectivo ámbito subjetivo de aplicación de las diferentes consejerías organismos y entidades).

Se carece de una política documentada de protección de datos en la que, entre otros aspectos, se contemplen e identifiquen las referencias organizativas que asuman las

figuras de existencia obligatoria establecidas en el RGPD, en especial por lo que se refiere a la uniformidad en la identificación de los responsables de tratamientos, siendo así que dicha atribución se lleva a cabo de manera heterogénea, incluso, dentro de las propias consejerías y organismos. Así, en unos casos se identifican como tales a los máximos órganos de gobierno (consejerías, gerencias, etc.) llegando a coexistir con responsables que se residencian en direcciones generales así como en jefaturas de servicio y hasta de sección. Siendo así que, conforme a la Ley 8/1991, de 30 de julio, de Organización de la Administración del Principado de Asturias, tanto los servicios como las secciones son unidades administrativas que carecen de funciones decisorias, y por ende, de competencias para decidir la finalidad y medios de los tratamientos que, en su caso, gestionen.

Se evidencia, también, ausencia de identificación de corresponsables del tratamiento y ello, pese a existir una previa identificación de distintos responsables que confluyen en una misma consejería y organismo y que tratan datos interrelacionados, por la, a su vez, interdependencia de los procedimientos administrativos y servicios a proveer.

Se carece de modelos referenciales que uniformicen los términos en los que se recojan las exigencias mínimas en relación con el tratamiento de datos a llevar a cabo por parte de los encargados, ya asuman tal condición mediante contrato, convenio, encomienda u otra fórmula jurídica.

En relación con otras figuras, de configuración voluntaria, tales como órganos de coordinación e informe, o de apoyo o referencia a la gestión, señalar la ausencia al respecto de las mismas, el citado previamente COSSISPA para el ámbito del Servicio de Salud del Principado de Asturias.

Por lo que se refiere a la figura del delegado de Protección de Datos, procede señalar lo siguiente:

Consultada la Sede Electrónica de la Agencia de Protección de Datos, en el apartado relativo a las consultas sobre la lista de delegados de protección de datos comunicados a la misma, por lo que a la Administración del Principado de Asturias se refiere, se relacionan a continuación los delegados comunicados y que lo son por las siguientes consejerías u organismos:

- Consejería de Sanidad.
- Servicio de Salud del principado de Asturias.
- Consorcio de aguas de Asturias.
- Gestión de Infraestructuras Sanitarias de Asturias, SAU.
- Instituto de Desarrollo Económico del Principado de Asturias.
- Consorcio de Transportes de Asturias.
- Sociedad pública de gestión y promoción turística y cultura del Principado de Asturias.
- Fundación para el fomento en Asturias de la investigación científica aplicada y la tecnología.

Consultada la página de transparencia del Principado de Asturias, no se identifica ningún delegado de protección de datos que extienda sus funciones a la Administración del Principado en su conjunto.

Aparecen, bajo la identificación de delegados de protección de datos las siguientes designaciones:

- Consejería de Derechos Sociales y Bienestar:

"*Datos de contacto del Delegado de Protección de Datos en la Consejería: Comité para la protección de datos de carácter personal de la Consejería de Servicios y Derechos Sociales.*"

El Comité es creado por Resolución de la Consejería de 30 de abril de 2019 (BOPA de 7 de junio) y está presidido por la persona titular de la Secretaría General Técnica e integrado por personal adscrito a los diferentes órganos directivos de la Consejería.

- Consejería de Hacienda:

"*Datos de contacto del Delegado de Protección de Datos en la Consejería: Comité para la protección de datos de carácter personal de la Consejería de Hacienda.*"

El Comité es creado por Resolución de la Consejería de 25 de septiembre de 2019 y está presidido por la persona titular de la Secretaría General Técnica e integrado por personal adscrito a los diferentes órganos directivos de la Consejería.

- Consejería de Industria, Empleo y Promoción Económica:

"*Datos de contacto del Delegado de Protección de Datos en la Consejería: Comité para la protección de datos de carácter personal de la Consejería de Industria, Empleo y Promoción Económica* "

El Comité es creado por Resolución de la Consejería de 27 de julio de 2020 (BOPA 4 de agosto) y está presidido por la persona titular de la Secretaría General Técnica e integrado por personal adscrito a los diferentes órganos directivos de la Consejería.

- Consejería de Desarrollo Rural y Recursos Naturales:

"*Datos de contacto del Delegado de Protección de Datos en la Consejería: Secretaría General Técnica de la Consejería de* Desarrollo Rural y Recursos Naturales."

- Consejería de Presidencia:

"*Datos de contacto del Delegado de Protección de Datos en la Consejería: Secretaría General Técnica de la Consejería de Presidencia*".

- Consejería de Administración Autonómica, Medio Ambiente y Cambio Climático:

"*Datos de contacto del Delegado de Protección de Datos en la Consejería: Secretaría General Técnica de la Consejería de* Administración Autonómica, Medio Ambiente y Cambio Climático. (Resolución del titular de la Consejería de 19 de diciembre de 2022, BOPA 4 de enero de 2023).

- Consejería de Ciencia, Innovación y Universidad: dpd-ciencia@asturias.org

No aparecen, en cambio, la designación del delegado de protección de datos de la Consejería de Sanidad, pese a existir y haber sido comunicada a la AGPD, y que recae en un funcionario que compatibiliza dichas funciones con las propias de su puesto adscrito al Servicio de Inspección de Servicios y Centros Sanitarios. Tampoco se identifica la designación de dicha figura en el SESPA, pese a haber sido igualmente comunicada a la AGPD y que recae en la Secretaría General de dicha entidad.

No existe información alguna respecto al ejercicio de las funciones propias del delegado en relación con el resto de organismos, ni de las Consejerías de Educación y la de Cultura, Política Lingüística y Turismo, las cuales carecen de designación alguna en tal sentido.

En relación con lo expuesto, proceden, en síntesis, las siguientes consideraciones:

- Ausencia de la figura de un único delegado de protección de datos que desempeñe las funciones, legalmente atribuidas, al ámbito subjetivo de toda la administración autonómica, habiéndose optado por la designación individual de dicha figura por las respectivas consejerías u organismos.
- Concurrencia de conflicto de intereses en la atribución de las funciones del delegado de protección de datos a las respectivas secretarías generales técnicas de las distintas consejerías u organismos, dada la simultaneidad entre estas funciones y las de responsable de distintos tratamientos (personal, contratación, presupuestaria, etc.). Ello determina la improcedencia legal de dichos nombramientos con arreglo a la normativa en materia de protección de datos.
- Carencia de personalidad jurídica de los órganos o comités a los que se atribuyen las funciones del delegado de protección de datos, siendo así que su naturaleza de órgano instrumental les dota más bien de las características propias de órganos de coordinación, informe y asesoramiento especializado, no respondiendo por ello a la figura del delegado configurada legalmente.
- Ausencia de ejercicio de las funciones propias del delegado de protección de datos con respecto a varias consejerías y la mayoría de los organismos adscritos.

12 OTROS ASPECTOS COMPLEMENTARIOS

En este apartado se recogen las evidencias de si la administración realiza acciones de concienciación, sensibilización o formación sobre la protección de datos.

En materia de formación, se ha de partir de los datos publicados en su web por el Instituto Asturiano de Administración Pública "Adolfo Posada" (IAAP) como órgano competente para la investigación, estudio, información, enseñanza y difusión de las materias de la Administración Pública del Principado de Asturias, y en relación con el personal al servicio de la Comunidad Autónoma, como responsable de la organización de cursos de formación y perfeccionamiento del mismo para su permanente actualización y, en su caso, reciclaje o promoción en la carrera administrativa, con especial atención a la formación del personal directivo.

Desde la entrada en vigor del RGPD en 2018, se ofertaron cursos sobre las novedades del Reglamento Europeo (UE) de Protección de Datos para gestores o la introducción al Nuevo Reglamento Europeo (UE) de Protección de Datos.

En cada semestre a partir de esa fecha se vienen ofertando cursos de carácter general sobre la normativa en materia de protección de datos (para subgrupos A1 y A2 y otro para subgrupos C1 y C2), cursos de análisis de casos prácticos en materia de protección de datos en administración general y específicos en el ámbito educativo, sanitario, sociosanitario, servicios sociales, o referidos a la relación del derecho a la protección de datos con otros derechos como el de acceso a la información, la confidencialidad o la transparencia.

Asimismo, se ofertan cursos más específicos en atención a las peculiaridades del sector si bien no con la asiduidad de los anteriores, como por ejemplo, la aplicación práctica de la protección de datos en el ámbito local, la protección de datos en la Administración de Justicia, en el ámbito deportivo, en bibliotecas, archivos y centros de documentación, en la gestión de recursos humanos, en la contratación pública, en la gestión y control de las subvenciones, en las relaciones laborales, en el ámbito estadístico, procedimiento administrativo o derecho penal o bien dedicados a un personal en concreto como protocolos de atención al usuario y protección de datos en la información telefónica y/o presencial en el IAAP o al personal de la inspección educativa.

También se han realizado actividades formativas sobre cuestiones más concretas de la aplicación de la normativa como la introducción al análisis de riesgos en la protección de datos personales, la cancelación de datos y derecho al olvido en la normativa de protección de datos, la seguridad de la información, la normativa y aplicación del Esquema Nacional de Seguridad (ENS) o la Investigación y la Interoperabilidad en Informática Sanitaria.

En relación a la difusión de la información, accediendo al portal del empleado, en "para tu trabajo" figura un apartado sobre "protección de datos" que incluye subapartados con documentos pdf explicativos de la protección de datos, del marco normativo, los principios de la protección de datos, las medidas de responsabilidad activa, el deber de información, los derechos de los afectado, la hora de ruta para la adaptación de la Administración del Principado de Asturias al Reglamento General de Protección de Datos y una guía sobre protección de datos.[9]

En el ámbito sanitario, debido a la sensibilidad de los datos protegidos, hay una mayor concienciación de la protección de los datos manejados ya sea con medidas de difusión a través de las sesiones clínicas o bien por la medida disuasoria que supone la repercusión mediática de imposición de penas en el orden penal a personal sanitario por acceso indebido a datos de salud.

13 CONCLUSIONES

A continuación, se sintetizan las conclusiones, ya efectuadas a lo largo de este informe derivadas del análisis expuesto y que son las siguientes:

PRIMERA.- Si bien las comunidades autónomas pueden asumir competencias de desarrollo normativo de la legislación estatal en materia de protección de datos dictada al amparo del artículo 149.1.1, la Comunidad Autónoma Principado de Asturias no se ha dotado de normativa legislativa ni reglamentaria que acometa dicho desarrollo.

SEGUNDA.- Carencia de diseño organizativo y competencial en materia de protección de datos, sin atribución orgánica expresa a ningún centro directivo que asuma la coordinación de su implantación y el seguimiento del cumplimiento de la normativa reguladora de la materia, en el ámbito de la Administración del Principado de Asturias, sus organismos y entes adscritos.

TERCERA.- Ausencia de una política de protección de datos documentada, vinculada a la política de seguridad de la información, en la que, entre otros aspectos, se contemplen e identifiquen las referencias organizativas que asuman las figuras de

[9] https://intranet.asturias.es/group/intranet/general/-/categories/240930

existencia obligatoria establecidas en el RGPD, en especial por lo que se refiere a la uniformidad en la identificación de los responsables de tratamientos, siendo así que dicha atribución se lleva a cabo de manera heterogénea, incluso, dentro de las propias consejerías, organismos y entidades públicas.

CUARTA.- Respecto a la figura del delegado de protección de datos, cuya existencia es obligatoria en las administraciones públicas, se advierte:

- Ausencia de la figura de un único delegado de protección de datos que desempeñe las funciones, legalmente atribuidas, al ámbito subjetivo de toda la administración autonómica, habiéndose optado por la designación individual de dicha figura por las respectivas consejerías u organismos, los cuales – en los casos en que se produce designación- han optado – a excepción de la Consejería de Salud- por una doble vía alternativa: asignación de funciones bien a las respectivas secretarías generales técnicas, bien a un comités integrados por personal adscrito a las mismas.

- Concurrencia de conflicto de intereses en la atribución de las funciones del delegado de protección de datos a las respectivas secretarías generales técnicas de las distintas consejerías u organismos, dada la simultaneidad entre estas funciones y las de responsable de distintos tratamientos (personal, contratación, presupuestaria, etc). Ello determina la improcedencia legal de dichos nombramientos con arreglo a la normativa en materia de protección de datos.

- Carencia de personalidad jurídica de los órganos o comités a los que se atribuyen las funciones del delegado de protección de datos, siendo así que su naturaleza de órgano instrumental les dota más bien de las características propias de órganos de coordinación, informe y asesoramiento especializado, no respondiendo por ello a la figura del delegado configurada legalmente.

- Ausencia de ejercicio de las funciones propias del delegado de protección de datos con respecto a varias consejerías y la mayoría de los organismos adscritos.

QUINTA.- Generalizado incumplimiento de la normativa en materia de protección de datos por parte de los respectivos responsables de los tratamientos, que se materializa en los siguientes aspectos:

- Gestión de los tratamientos de datos personales careciendo de un diseño preventivo mediante el enfoque de riesgos. A excepción del SESPA, tanto las consejerías como los organismos y entidades analizadas carecen de gestión documental que acredite la realización de identificación de riesgos ni de evaluaciones de impacto en los distintos tratamientos que acometen.

- Carencia de gestión documentada comprensiva de las medidas de seguridad adoptadas en atención a los riesgos concurrentes que, como se ha expuesto, no se determinan ni evalúan. Tampoco existen planes ni protocolos preventivos de actuación ante eventuales brechas de seguridad, así como de instrucciones sobre cómo realizar la comunicación a la autoridad de control o realizar la valoración de la procedencia de la comunicación al interesado sin que haya constancia de un inventario de la gestión de incidencias.

Si bien se incorporan cláusulas de confidencialidad en los convenios de colaboración, contratos y otros instrumentos jurídicos que impliquen acceso a datos personales por terceros o , en su caso, el tratamiento de éstos, se constata la ausencia de una definición clara de las responsabilidades concretas de cada una de las partes, sin que haya evidencia de controles o supervisión por parte del responsable del tratamiento en relación con cumplimiento de las mismas así como falta de exigencia de mayores

garantías tales como auditorías o certificaciones acreditativas del cumplimiento o adecuación a las medidas del ENS.

- Gestión de los tratamientos de datos personales sin una previa configuración de procedimientos que, diseñada por defecto y con respeto a la privacidad, garantice que éstos sean mínimamente intrusivos tanto en la recogida de datos, como en la discriminación de los distintos ciclos de vida del tratamiento.

- Inexistencia, a excepción del SESPA, de auditorías o actuaciones de control documentadas.

- Deficiente configuración de los inventarios de actividades de tratamiento, apreciándose las siguientes disfunciones:

  - ✓ Incumplimiento del contenido legal mínimo en algunos casos.
  - ✓ Heterogénea categorización de los tratamientos, agrupándose en ocasiones por categorías procedimentales genéricas y, en otros, por procedimientos concretos siendo así que en estos últimos se advierte que los incluidos en el correspondiente Registro no se corresponden, en ocasiones, con la totalidad de los ejecutados por la consejería, organismo o entidad.
  - ✓ Incorrectas identificaciones de las bases de legitimación, invocando en varias ocasiones el consentimiento como causa única en aquellos tratamientos que responden al ejercicio de obligaciones legales o ejercicio de poderes públicos.
  - ✓ Ausencia de aplicación de los principios de minimización en la descripción de las categorías de datos personales.
  - ✓ Incorrecta identificación de los encargados del tratamiento.
  - ✓ Genérica remisión a los plazos contenidos en el Cuadro General de Conservación de Documentos Administrativos del Principado de Asturias, plazos que atienden a la satisfacción de finalidades distintas de las propias de la protección de datos personales.
  - ✓ Respecto al delegado de protección de datos, la información se limita a la aportación de un correo electrónico.

- Respecto al ejercicio de derechos, si bien hay una adecuación a la obligación de proporcionar la información mediante capas o niveles a través de la normalización de los formularios electrónicos, no obstante, no se acredita la existencia de medidas de control o seguimiento para garantizar ni la homogeneidad y correcta aplicación de las instrucciones de adecuación publicadas ni la actualización existiendo aún algunos formularios con referencias a la normativa anterior. Asimismo, en algunos casos, la información que se proporciona en los formularios, basada en la contenida en el registro de tratamiento de datos, adolece de los mismos defectos o imprecisiones de éstos.

A excepción del SESPA, no hay constancia de la llevanza, por parte de los responsables de tratamiento, de un registro de solicitudes del ejercicio de derechos ni de los resultados de su tramitación.

SEXTA.- Respecto a la política de seguridad de la información, directamente relacionada con la política de protección de datos, esta es asumida por la Dirección General de Seguridad y Estrategia Digital (DGSED) dependiente de la Consejería de Presidencia de la política de seguridad de la información, contando con el impulso del Comité de estrategia digital y de seguridad de la información del Principado de Asturias (CEDISI) y con el apoyo, para el ámbito de los sistemas de información de salud, del Comité de Seguridad de Sistemas de Información de Salud del Principado de Asturias (COSSISPA).

Se acredita una adecuación de los sistemas de información de la Administración del Principado de Asturias y su sector público a las medidas de seguridad previstas en el Esquema Nacional de Seguridad, en su nivel medio, de acuerdo con la certificación obtenida mediante auditoría externa.

SÉPTIMA.- Respecto a medidas complementarias que puedan crear una cultura de la protección de datos entre los empleados de la organización, se constata:

- La incorporación con carácter ordinario en los planes de formación de cursos de carácter generalista en materia de protección de datos así como de cursos más específicos en atención a las peculiaridades del sector o la sensibilidad de los datos tratados como ocurre en el ámbito educativo, sanitario, sociosanitario o el de los servicios sociales. No obstante, de la duración y el contenido de estos se deduce la ausencia de una oferta formativa que permita obtener una verdadera especialización en la materia.

- La inclusión en el portal del empleado de información de carácter general sobre protección de datos, estando publicados una serie de documentos pdf explicativos de las principales exigencias y requisitos que implica el cumplimiento de la normativa en la materia.

14 RECOMENDACIONES

Como consecuencia de las citadas conclusiones, se realizan una serie de recomendaciones que permitan una adecuada adaptación de esta administración a la normativa en materia de protección de datos:

PRIMERA.- Atribuir a una determinada consejería, a través de los decretos de estructura orgánica, el ejercicio de las funciones que en materia de dirección, impulso, y coordinación del cumplimiento de la normativa en materia de protección de datos, resulten aplicables a toda la organización. En dicha atribución se ha de valorar la conveniencia, en su caso, de residenciar dichas funciones conjuntamente con las inherentes a la seguridad de la información.

SEGUNDA.- Aprobar una política documentada de protección de datos personales, debiendo valorarse la integración de la misma en la política de seguridad de la información aplicable a la organización en su conjunto.

En todo caso, dicha política ha de contemplar las referencias organizativas que asuman las figuras de existencia obligatoria establecidas en el RGPD, en especial por lo que se refiere a la creación de la figura del delegado de protección de datos, sin que la misma pueda hacerse coincidir con las secretarías generales técnicas ni con órganos carentes de personalidad jurídica con funciones deliberantes y decisivas. En el diseño organizativo de esta figura ha de valorarse especialmente lo siguiente:

- La singularidad y vulnerabilidad, así como el elevado volumen de los datos personales de carácter sanitario aconseja la creación de un delegado específico para dicho ámbito, que pueda extender su ámbito competencial tanto al Servicio de Salud como a la propia Consejería.

- La singularidad y vulnerabilidad de los datos personales de carácter educativo, así como de contenido social determinan la necesidad de acometer una opción organizativa entre la creación de sendos delegados para dichos ámbitos u optar por una gestión sectorial a través de las figuras de los delegados adjuntos.

- Dada la estructura y configuración de la Administración del Principado de Asturias, así como de sus organismos y entidades adscritos, ello aconseja la dedicación plena a las funciones de delegado por parte de quien o quienes sean designados, así como la puesta a disposición de los medios materiales y, especialmente, personales que garanticen su independencia y el ejercicio de sus funciones.

De todo lo cual se informa, sin perjuicio de criterio mejor fundado en Derecho, a los efectos del artículo 7 de la Ley del Principado de Asturias 11/2018, de 16 de noviembre, de la Inspección General de Servicios.

Inspectora de Servicios

Inspectora de Servicios

DILIGENCIA PARA HACER CONSTAR QUE EN EL EXPEDIENTE INSP/2023/624 (ESTUDIO DE LAS POLÍTICAS DE PROTECCIÓN DE DATOS, EN ESPECIAL, DE LOS DATOS DE MAYOR SENSIBILIDAD / PLAN ANUAL 2023 DE LA INSPECCION GENERAL DE SERVICIOS), NO SE HAN FORMULADO CONSIDERACIONES AL INFORME PROVISIONAL EN EL ASUNTO CITADO POR LO QUE LA INSPECCION GENERAL DE SERVICIOS SE HA RATIFICADO EN EL MISMO Y SE HA ELEVADO A INFORME DEFINITIVO (ARTÍCULOS 7.3 Y 8.3 E) DE LA LEY DEL PRINCIPADO DE ASTURIAS 11/2018, DE 16 DE NOVIEMBRE, DE LA INSPECCION GENERAL DE SERVICIOS).

Oviedo, a la fecha de la firma digital

EL INSPECTOR GENERAL DE SERVICIOS

[redacted]