MEMORIA DEL PROYECTO DE DECRETO POR EL QUE SE REGULA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS DE LA GERENCIA REGIONAL DE SALUD DE CASTILLA Y LEÓN.

Índice

1. Marco normativo.

1.1 Marco normativo de referencia.

1.1.1. Normativa europea.

Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, en adelante RGPD). El RGPD establece normas relativas a la protección de datos de carácter personal, tanto desde el punto de vista de los derechos de las personas físicas, como de las obligaciones de las personas y entidades que tratan datos de carácter personal, incluidas las Administraciones Públicas.

1.1.2. Normativa estatal.

- Constitución española de 1978 (artículo 18.4), en la interpretación del Tribunal Constitucional, como derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por la que se adapta el ordenamiento jurídico español al RGPD. La disposición adicional primera concreta que en el ámbito del sector público se deben aplicar, en los tratamientos de datos personales, las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Establece en su artículo 13 el derecho de los ciudadanos a la protección de datos de carácter personal y a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Determina, en su artículo 156, que la política de seguridad en la utilización de medios electrónicos se realizará de acuerdo con las prescripciones establecidas en el Esquema Nacional de Seguridad, en el que se establecen los principios básicos y requisitos mínimos que han de garantizar la seguridad de la información tratada.

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que tiene por objeto establecer los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada, garantizando el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos. El artículo 12.2 del citado Real Decreto establece que cada administración pública cuente con una política de seguridad formalmente aprobada por el órgano competente.

1.1.3. Normativa autonómica.

- Estatuto de Autonomía de Castilla y León. Establece en su artículo 12, que la ley garantizará el derecho a la protección de los datos personales contenidos en ficheros dependientes de la Administración autonómica.

- Ley 2/2010, de 11 de marzo, de Derechos de los Ciudadanos en sus relaciones con la Administración de la Comunidad y de Gestión Pública, que establece en su artículo 45, que las actuaciones administrativas a través de medios electrónicos respetarán, en todo caso, la normativa sobre protección de datos de carácter personal.

- Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León que exige, en su artículo 3, que la política de seguridad de los sistemas de la información de la Administración de la Comunidad Autónoma de Castilla y León se desarrolle aplicando el Esquema Nacional de Seguridad.

- Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León, que establece en su artículo 2 (ámbito de aplicación) que los organismos autónomos podrán aprobar su propia política de seguridad de la información y protección de datos si bien en coherencia con el propio decreto y respetando en todo caso su Capítulo II (Organización de la Política de Seguridad de la Información y Protección de Datos). Así mismo, la disposición adicional séptima establece que la Gerencia Regional de Salud de

Castilla y León, en atención a sus especiales funciones y singularidades respecto a su organización y funcionamiento, deberá establecer su propia política de seguridad de la información y protección de datos, conforme a los principios y requisitos mínimos recogidos en este decreto.

1.2 Disposiciones afectadas.

La política de seguridad de la información y protección de datos en el ámbito de la Gerencia Regional de Salud no se encontraba regulada hasta este momento. Por tanto, la aprobación del presente decreto no modifica ni deroga norma alguna.

1.3 Competencia.

1.3.1. Propuesta.

El artículo 26.1.d de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León establece que corresponde a los consejeros preparar y presentar los proyectos de decretos relativos a las cuestiones propias de su consejería. Así mismo, el artículo 7 g) de la Ley 8/2010, de 30 de agosto, de ordenación del sistema de salud de Castilla y León, atribuye a la consejería competente en materia de sanidad el establecimiento de la estructura básica y las características que ha de reunir el sistema de información sanitaria del Sistema de Salud de Castilla y León.

1.3.2. Aprobación.

Los artículos 128 y 129.4 de la Ley 39/2015, de 1 de octubre, atribuyen con carácter general el desarrollo reglamentario de las leyes en el ámbito autonómico a los Consejos de Gobierno respectivos. En la Administración de la Comunidad de Castilla y León este corresponde a la Junta de Castilla y León, que normativamente se expresa a través de decretos (artículos 16.e y 70.1 de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León).

2. Necesidad y oportunidad de la norma.

2.1 Motivación de la necesidad y oportunidad.

El Servicio de Salud de Castilla y León, denominado Gerencia Regional de Salud, es un organismo autónomo adscrito a la Consejería competente en materia de sanidad, dotado de personalidad jurídica, patrimonio y tesorería propios, y con plena capacidad de obrar para el cumplimiento de sus fines. Su finalidad es ejercer las competencias de administración y

gestión de servicios, prestaciones y programas públicos sanitarios de carácter asistencial y de atención a la salud de la Comunidad de Castilla y León y aquellos otros que le encomiende la Administración de la Comunidad Autónoma conforme a los objetivos y principios de la Ley 8/2010, de 30 de agosto, de ordenación del sistema de salud de Castilla y León.

En atención a sus especiales funciones, la Gerencia Regional de Salud cuenta con singularidades en su organización y funcionamiento. A tal efecto dispone de una estructura territorial y funcional diferente de la correspondiente a la Administración General de la Comunidad, de la que forman parte todos los centros e instituciones sanitarios y en la que se integra la actividad asistencial correspondiente a los diferentes niveles asistenciales.

Así mismo hay que poner de manifiesto que la información que recaba la Gerencia Regional de Salud de Castilla y León en sus sistemas de información es un activo esencial para el ejercicio de sus competencias. No obstante, si bien su gestión mediante las nuevas tecnologías es altamente beneficiosa, en este entorno tanto la seguridad de la información como la responsabilidad asociada a la protección de los datos personales resultan imperativas.

Esta imperatividad resulta de lo establecido en el artículo 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, según el cual las Administraciones Públicas han de asegurar en sus relaciones a través de medios electrónicos la interoperabilidad y seguridad de los sistemas. También del artículo 13 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que recoge el derecho de las personas en sus relaciones con las Administraciones Públicas a la protección de datos personales, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones. Y por último de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por la que se adapta al ordenamiento jurídico español el 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, cuyo artículo 1 garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución y cuya disposición adicional primera establece que en los tratamientos de datos personales realizados en el ámbito del sector público se deben

aplicar las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

El Real Decreto 311/2022, de 3 de mayo, regula el Esquema Nacional de Seguridad. En el apartado primero de su artículo 12 establece que la política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. Y en el apartado segundo señala que cada órgano o entidad con personalidad jurídica propia del sector público deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

Para dar cumplimiento a las exigencias mencionadas, la Junta de Castilla y León ha aprobado el Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León. Dicha norma regula el marco organizativo y de gestión aplicable a todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sean responsables los órganos de la Administración General de la Comunidad de Castilla y León, así como sus organismos autónomos y entes públicos de derecho privado cuando ejerzan potestades administrativas. No obstante, el apartado primero del artículo 2 establece la posibilidad de que dichos organismos y entidades puedan aprobar su propia política de seguridad de la información y protección de datos, siempre que esta sea coherente con el decreto y se aplique su capítulo segundo (“Organización de la Política de Seguridad de la Información y Protección de Datos”). En coherencia con el precepto mencionado, la disposición final séptima otorga un plazo de seis meses a la Gerencia Regional de Salud de Castilla y León, en atención a sus especiales funciones y singularidades respecto a su organización y funcionamiento, para establecer su propia política de seguridad de la información y protección de datos.

4.1. Objetivo del proyecto.

El objetivo del presente decreto es desarrollar la política de seguridad de la información y protección de datos de la Gerencia Regional de Salud de Castilla y León, en cumplimiento del mandato previsto en la disposición final séptima del Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León y respetando el marco organizativo establecido en su Capítulo II.

4.2. Principios de buena regulación y calidad normativa.

El decreto responde, tanto en su finalidad y contenido como en el procedimiento de su elaboración, a los principios de buena regulación establecidos tanto en el artículo 129 de la Ley 39/2015, de 1 de octubre, como en el artículo 42 de la Ley 2/2010, de 11 de marzo.

En relación con los principios de necesidad, eficiencia y eficacia, puede afirmarse que el decreto sirve al interés general, identificando el problema público que se pretende resolver, que es dotar de seguridad las relaciones electrónicas entre ciudadanos y Administración, con pleno respeto a la legislación en materia de protección de datos. No impone cargas administrativas innecesarias o accesorias y contribuye a la racionalización de la gestión de los recursos públicos al no implicar incremento del gasto.

Por lo que respecta al principio de proporcionalidad, existe un equilibrio entre los impactos previsibles de la norma y las medidas que se adoptan para conseguir el objetivo del desarrollo de una política de seguridad de la información y de protección de datos. El decreto contiene la regulación imprescindible para atender al fin que lo justifica, que es la creación de las condiciones de confianza necesarias en el uso de los medios electrónicos, mediante la aplicación de las medidas que garanticen la seguridad de los sistemas, las comunicaciones, los servicios electrónicos y el cumplimiento de las obligaciones establecidas en la normativa vigente en materia de protección de datos personales. Además, no hay alternativa posible a la regulación, ya que la disposición final séptima del Decreto 22/2021, de 30 de septiembre, obliga a la Gerencia Regional de Salud a desarrollar su propia política de seguridad de la información y protección de datos.

El decreto es también coherente con el resto del ordenamiento jurídico. Además de estar en consonancia con las normas citadas, también lo está con la Ley 2/2010, de 11 de marzo, de Derechos de los Ciudadanos en sus relaciones con la Administración de la Comunidad de Castilla y León y de Gestión Pública; con el Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León; y con la Ley 8/2003, de 8 de abril sobre derechos y deberes de las personas en relación con la salud, que contempla el derecho a la protección de la confidencialidad e intimidad.

El principio de accesibilidad se satisface mediante el uso de una redacción sencilla e inteligible, pero a su vez rigurosa.

En cumplimiento del principio de responsabilidad, se establecen y definen los distintos roles para hacer efectiva la seguridad de la información y la protección de los datos personales.

El decreto también cumple con el principio de seguridad jurídica, al ser coherente con el resto del ordenamiento jurídico autonómico, nacional y de la Unión Europea, generando un marco regulatorio que define el ámbito de aplicación, el marco organizativo y los instrumentos para desarrollar su contenido. Define también las medidas a adoptar y las funciones atribuidas a cada órgano competente en materia de seguridad de la información y de protección de datos personales, facilitando su actuación y la toma de decisiones.

El principio de transparencia se garantiza mediante la publicación en el Portal de Gobierno Abierto de la Junta de Castilla y León de los mecanismos de consulta previa y participación ciudadana, así como mediante el sometimiento al trámite de audiencia y al informe preceptivo de los correspondientes órganos y organismos. Por último, toda la tramitación se hará pública en la Huella Normativa de la web corporativa.

3. Estructura y contenido de la norma.

El Decreto consta de veintinueve artículos, estructurados en cuatro capítulos, tres disposiciones adicionales, una disposición derogatoria y dos disposiciones finales.

El Capítulo I, “Disposiciones Generales”, señala el objeto y ámbito de aplicación, la misión de la Gerencia Regional de Salud, interpretación de las definiciones, el marco regulatorio aplicable y los principios fundamentales que rigen la política de seguridad de la información y protección de datos.

El Capítulo II “Organización de la Política de Seguridad de la Información y Protección de Datos”, comprende los artículos 7 a 20, que establecen la estructura organizativa, compuesta por: el Comité de Seguridad de la Información; la Comisión Ejecutiva de Seguridad de la Información; las Comisiones Ejecutivas de las Gerencias de Asistencia Sanitaria, Gerencias de Atención Especializada y Gerencias de Atención Primaria; los responsables de la información y del tratamiento de datos personales; los responsables del servicio; el responsable de la seguridad de la Gerencia Regional de Salud y los responsables de la seguridad delegados; los responsables del sistema; responsables delegados y grupos de trabajo; y el delegado de protección de datos de la Gerencia Regional de Salud. También incluye un mecanismo de resolución de conflictos.

El Capítulo III, “Desarrollo de la Política de Seguridad de la Información y Protección de Datos”, artículos 21 y 22, está dedicado a la estructura documental y normativa y a la gestión y coordinación de la política de seguridad de la información y protección de datos.

El Capítulo IV “Gestión de la Política de Seguridad de la Información y Protección de Datos”, artículos 23 a 29 regulan, la obligación de realizar análisis de riesgos y evaluaciones de impacto de protección de datos, así como la gestión de los riesgos de seguridad de la información; uso de medios digitales por las personas empleadas públicas; auditoría de seguridad; notificación de violaciones de seguridad de los datos personales; registro de actividades de tratamiento; formación y concienciación; y obligaciones profesionales.

En cuanto a las tres disposiciones adicionales, la primera regula la aplicación de los principios y previsiones de la Política de Seguridad de la Información y Protección de Datos de la Gerencia Regional de Salud por los Comités de Ética de la Investigación adscritos a la Consejería de Sanidad. La segunda señala el mecanismo para la designación de las personas responsables. Por último, la tercera, regula la constitución de los órganos colegiados de seguridad de la información.

En las disposiciones derogatoria y finales se dejan sin efecto todas las disposiciones de igual o inferior rango que se opongan al decreto, se contempla una habilitación normativa a favor de la persona titular de la Consejería de Sanidad y se establece la fecha de entrada en vigor.

4. Evaluación de impactos.

4.1. Evaluación de impacto normativo.

El Decreto 43/2010, de 7 de octubre, por el que se aprueban determinadas medidas de mejora en la calidad normativa de la Administración de la Comunidad de Castilla y León, establece en su artículo 4 que estarán sometidos a evaluación de impacto normativo los proyectos de disposiciones administrativas de carácter general que deban ser aprobados por la Junta de Castilla y León relacionados con la política socioeconómica y que, de acuerdo con lo dispuesto en el artículo 3.1ª) de la Ley 13/1990, de 28 de noviembre, del Consejo Económico y Social, deban ser sometidos preceptivamente a informe previo de este órgano.

La presente norma no está relacionada con la política socioeconómica y por tanto no procede someterla a evaluación de impacto normativo.

4.2. Evaluación de impacto administrativo.

El Decreto 43/2010, de 7 de octubre, en sus artículos 5 y 6, exige un estudio de impacto administrativo en la elaboración de aquellas disposiciones de carácter general que regulen nuevos procedimientos o que modifiquen preceptos relativos a procedimientos administrativos ya existentes o que aprueben aplicaciones de administración electrónica.

La presente norma no regula ni modifica procedimientos, puesto que éstos se contienen en la normativa estatal vigente. Contiene, sin embargo, fórmulas que plausiblemente favorecerán la coordinación y la homogeneización en la gestión de dichos procedimientos, por lo que cabe esperar un impacto positivo.

4.3. Evaluación de impacto en la infancia, la adolescencia y la familia.

La Constitución Española de 1978 al enumerar, en el capítulo III del Título I, los principios rectores de la política social y económica, hace mención, en primer lugar, a la obligación de los poderes públicos de asegurar la protección social, económica y jurídica de la familia y dentro de esta, con carácter singular, la de los menores.

La Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil, en su artículo 22 quinquies establece que las memorias del análisis de impacto normativo que deben acompañar a los anteproyectos de ley y a los proyectos de reglamentos incluirán el impacto de la normativa en la infancia y en la adolescencia.

La Ley Orgánica 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León establece en su artículo 70.10 la competencia exclusiva de la Comunidad de Castilla y León en materia de asistencia social, servicios sociales y desarrollo comunitario, promoción y atención a la infancia, y protección y tutela de menores.

Ello ha dado lugar a la Ley 14/2002, de 25 de julio, de promoción, atención y protección a la infancia en Castilla y León, la cual prescribe que en todas las actuaciones dirigidas a la población menor de edad, cualesquiera que sean su naturaleza y alcance, la planificación, la integralidad en la acción, la coordinación a partir de una asignación de competencias que resulta directa expresión del principio de corresponsabilidad, y la participación y la colaboración social, son predicadas con especial énfasis.

Por último, la disposición adicional décima de la Ley 40/2003, de 18 de noviembre, de Protección a las Familias Numerosa, establece que las memorias de análisis de impacto

normativo que deben acompañar a los anteproyectos de ley y a los proyectos de reglamentos incluirán el impacto de la normativa en la familia.

La regulación de la política de seguridad de la información y protección de datos de la Gerencia Regional de Salud no tiene un impacto específico sobre las políticas públicas destinadas a los colectivos mencionados.

4.4. Evaluación de impacto sobre la discapacidad.

El artículo 71 de la Ley 2/2013, de 15 de mayo, de igualdad de oportunidades de personas con discapacidad, establece que en la memoria que acompaña a los proyectos de decreto se deberá hacer mención al impacto de discapacidad.

La regulación de la política de seguridad de la información y protección de datos de la Gerencia Regional de Salud no tiene un impacto específico sobre la política de igualdad de oportunidades de las personas con discapacidad.

4.5. Evaluación de impacto de género.

4.5.1. Fundamentación y objeto del informe.

4.5.1.1. Contexto normativo.

La emisión del presente informe se sustenta en el artículo 3 de la Ley 1/2003, de 3 de marzo, de igualdad de oportunidades entre hombres y mujeres en Castilla y León, y en el artículo 14 de la Ley Orgánica 14/2007, de 30 de noviembre, que modifica el Estatuto de Autonomía de Castilla y León, que incluyen entre los principios que informan la actuación administrativa el de la transversalidad en la aplicación de la perspectiva de género en las fases de planificación, ejecución y evaluación de las políticas de la Administración Autonómica.

La Ley 1/2011, de 1 de marzo, de Evaluación de Impacto de Género en Castilla y León, con la finalidad de garantizar que la igualdad entre hombres y mujeres y la transversalidad de género estén presentes en todas las políticas públicas, establece la obligación de realizar con carácter preceptivo un informe de evaluación de impacto de género en todos los procedimientos de elaboración de nomas con rango de Ley y demás disposiciones administrativas de carácter general, que se elaborará de acuerdo con las pautas metodológicas establecidas por la Junta de Castilla y León.

El Decreto 43/2010, de 7 de octubre, por el que se aprueban determinadas medidas de mejora en la calidad normativa de la Administración de la Comunidad de Castilla y León,

incluye la evaluación del impacto de género en la memoria que acompaña a los anteproyectos de ley y proyectos de disposiciones de carácter general.

Por último, la Orden ADM/1835/2010, de 15 de diciembre, por la que se aprueba la Guía metodológica de mejora de la calidad normativa, en aplicación del decreto mencionado contiene las pautas orientativas para la elaboración de los informes de evaluación de impacto de género. Todo ello de acuerdo con la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva entre mujeres y hombres, que configura la igualdad de trato entre mujeres y hombres como un principio informador del ordenamiento jurídico. En su artículo 15, bajo el epígrafe transversalidad del principio de igualdad, impone a la Administración la obligación de integrar el principio de igualdad entre mujeres y hombres, de forma activa, en la adopción de sus disposiciones normativas.

4.5.1.2. Objeto del informe.

Respondiendo a los anteriores requerimientos normativos se elabora el presente informe con el objeto de evaluar el efecto potencial que el Decreto de política de seguridad de la información y protección de datos de la Gerencia Regional de Salud, tiene sobre el género.

4.5.2. La pertinencia de género de la norma.

El objeto de la norma es regular la política de seguridad de la información y protección de datos de la Gerencia Regional de Salud y en concreto, definir su organización, desarrollo y gestión.

Este objeto no afecta de manera directa ni indirecta a mujeres u hombres de manera diferenciada, no incide en el logro de la igualdad, por lo que se concluye que no existe pertinencia de género de la norma, entendiendo que esta norma no tiene incidencia en lo que se refiere al género.

El destinatario de la norma es la Gerencia Regional de Salud, que podrá y deberá tener en cuenta en el despliegue de la política la perspectiva de género, procurando la adecuada representación de ambos géneros en los puestos de responsabilidad que se determinan.

En la redacción del decreto se ha procurado utilizar un lenguaje no sexista e inclusivo, huyendo del abuso del masculino genérico y sustituyéndolo por términos genéricos reales y por el desdoblamiento (uso de los dos géneros gramaticales).

4.6. Evaluación de impacto en la sostenibilidad y la lucha y adaptación contra el cambio climático.

El Acuerdo 64/2016, de 13 de octubre, por el que se aprueban medidas de desarrollo sostenible en la Comunidad de Castilla y León, establece entre las medidas destinadas a integrar la sostenibilidad y el cambio climático en los procesos de toma de decisiones, la obligación de incorporar en las memorias de los proyectos de decreto un análisis de su contribución a la sostenibilidad y a la lucha y adaptación contra el cambio climático.

El contenido de la norma no tiene impacto sobre la sostenibilidad y la lucha y adaptación contra el cambio climático.

5. Memoria económica.

La aprobación de esta norma no genera ningún gasto, no siendo necesaria financiación alguna para su desarrollo e implementación, ni produciendo efecto alguno en la economía. La aplicación de las previsiones contenidas en ella será atendida con los medios humanos y materiales de que dispone la Administración de la Comunidad. Por tanto, no procede realizar memoria económica.