INFORME

Asunto: PROYECTO DE DECRETO POR EL QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS DE LA GERENCIA REGIONAL DE SALUD DE CASTILLA Y LEÓN.

Por el Servicio de Evaluación, Normativa y Procedimiento se remite el "Proyecto de Decreto por el que se aprueba la política de seguridad de la información y protección de datos de la Gerencia Regional De Salud de Castilla y León", para emitir informe preceptivo de acuerdo con lo dispuesto en el artículo 4.2 b) de la Ley 6/2003, de 3 de abril, reguladora de la Asistencia Jurídica a la Comunidad de Castilla y León, y en el artículo 3.3. b) del Decreto 17/1996, de 1 de febrero, de organización y funcionamiento de los Servicios Jurídicos de la Comunidad de Castilla y León.

Acompaña al Proyecto de Decreto la Memoria Justificativa conforme a lo dispuesto en los artículos 75 y 76 de la Ley 3/2001, de 3 de julio.

Vista 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 ; el Real Decreto 311/2022, de 3 de mayo, que regula 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; la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; y demás normativa aplicable, esta Asesoría jurídica informa:

El presente proyecto de decreto responde al mandato contenido en la disposición adicional séptima del Decreto 22/2021, de 30 de septiembre, en la que se recoge que, la Gerencia Regional de Salud de Castilla y León, en atención a sus especiales funciones y singularidades respecto a su organización y funcionamiento, aprobará su propia política de seguridad de la información y protección de datos, conforme a los principios y requisitos mínimos recogidos en el Decreto. En todo caso, resultará de aplicación a la Gerencia Regional de Salud el Capítulo II del citado Decreto.

El proyecto de decreto se estructura en cuatro capítulos, a los que siguen tres disposiciones adicionales, una disposición derogatoria y dos disposiciones finales.

- El Capítulo I, "Disposiciones Generales" recoge:

El objeto que es la aprobación de la Política de Seguridad de la Información y de Protección de Datos (en adelante, PSIPD_GRS), en el ámbito de la Gerencia Regional de Salud de Castilla y León, su marco organizativo y de gestión.

El ámbito de aplicación son todos los sistemas de información y todas las actividades de tratamiento de datos personales de los que sean responsables la Gerencia Regional de Salud de Castilla y León, así como sus centros y organismos adscritos a ella; afectará a toda la información, con independencia del medio en que sea tratada y de su soporte.

Se extiende a todo el personal que acceda, tanto a los sistemas de información, como a la propia información gestionada por la Gerencia Regional de Salud de Castilla y León, con independencia de la naturaleza de su relación con esta Administración y de su destino o adscripción.

La normativa aplicable a la PSIPD_GRS además de la recogida expresamente en el texto es la normativa citada en el artículo 4 del Decreto 22/2021, de 30 de septiembre; remitiéndose a los principios fundamentales y las directrices recogidas en los artículos 5 y 6 del Decreto 22/2021, de 30 de septiembre, como propios de la PSIPD_GRS.

- El Capítulo II "Organización de la Política de Seguridad de la Información y Protección de Datos de la Gerencia Regional de Salud".

Recoge la estructura organizativa encargada de la gestión de PSIPD_GRS de la Gerencia Regional de Salud, a nivel central y periférico, atendiendo a sus especiales funciones y singularidades en cuanto a su organización y funcionamiento.

Forman parte de la estructura organizativa: el Comité de Seguridad de la Información; la Comisión Ejecutiva de Seguridad de la Información; las Comisiones Ejecutivas de las áreas de salud; los responsables de la información y del tratamiento de datos personales; los responsables del servicio; los encargados del tratamiento; la persona responsable de la seguridad de la Gerencia Regional de Salud y los responsables de la seguridad delegados; los responsables del sistema; los administradores de seguridad; y el delegado de protección de datos de la Gerencia Regional de Salud.

El Comité de Seguridad de la Información de la Gerencia Regional de Salud es el órgano colegiado de impulso, seguimiento y coordinación interna en esta materia en el ámbito del Servicio de Salud de Castilla y León. En su actuación se somete a las directrices de los organismos de seguridad de la información y protección de datos de acuerdo con lo dispuesto por el Decreto 22/2021, de 30 de septiembre. Recoge sus funciones, su composición, con indicación del ejercicio de la presidencia y la secretaría y remitiendo para su regulación a las disposiciones que para los órganos colegiados se contiene en la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León y a la Ley 40/2015, de 1 de octubre.

Para el resto de los órganos colegiados se limita a determinar su ámbito de actuación y funciones, siendo el Comité de Seguridad de la Información de la Gerencia el encargado de determinar su composición y el régimen de organización y funcionamiento.

En cuanto a los distintos "responsables" que recoge añade nuevas funciones a las atribuidas en el Decreto 22/2021, de 30 de septiembre, al que se remite.

En el artículo 16 se crea la figura de los administradores de seguridad, que no está contemplada en el Decreto 22/2021, de 30 de septiembre, para asegurar la correcta implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información. La designación de los administradores de seguridad se hará por el Comité de Seguridad de la Información de la Gerencia Regional de Salud, por decisión

propia o a propuesta de la Gerencia Regional de Salud y los centros y organismos adscritos a ella, cada uno dentro de su ámbito de actuación.

No se determina en el texto el alcance de esta propuesta de nombramiento si es vinculante o no para el Comité de Seguridad de la Información de la Gerencia Regional de Salud, **lo cual ha de ser precisado**, máxime, cuando en el párrafo 3 señala que las funciones del administrador de seguridad podrían recaer en la misma persona para todos los sistemas de información que entran en el ámbito de actuación del responsable del sistema, o se podrán designar administradores de seguridad para cada sistema de información, dependiendo de la complejidad, distribución, separación física de sus elementos o número de usuarios, y en el siguiente que si no se designa un administrador de seguridad, este rol podrá coincidir con el rol del responsable del sistema.

Se prevé que se creen grupos de trabajo e incluye un mecanismo de resolución de conflictos.

Se remite a la obligatoriedad de la existencia del delegado de protección de datos de la Gerencia Regional de Salud exigida en el Decreto 22/2021, de 30 de septiembre y al artículo 39 del Reglamento (UE) 2016/67 para el ejercicio de su funciones.

- El Capítulo III, dedicado al "Desarrollo de la Política de Seguridad de la Información y Protección de Datos", desarrolla la estructura documental y normativa y 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", viene a regular 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:

Primera establece 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.

Segunda señala el mecanismo para la designación de las personas responsables.

Tercera, fija la constitución de los órganos colegiados de seguridad de la información.

En la disposición derogatoria se dejan sin efecto todas las disposiciones de igual o inferior rango que se opongan al decreto; las disposiciones finales, la primera habilita a la persona titular de la Consejería de Sanidad para dictar disposiciones y actos necesarios para el desarrollo y ejecución del presente decreto y en la segunda se establece la fecha de entrada en vigor.

A la vista de lo anterior y sin perjuicio de la precisión que ha de realizarse en el artículo 16, el proyecto de decreto por el que se aprueba la política de seguridad de la información y protección de datos de la Gerencia Regional De Salud de Castilla y León se
ajusta a la normativa específica aplicable en la materia.

Es cuanto procede informar

EXCMO. SR. CONSEJERO DE SANIDAD

Junta de Castilla y León. Asesoría Jurídica. Consejería de Sanidad