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.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 3 establece que las Administraciones Públicas han de asegurar en sus relaciones a través de medios electrónicos la interoperabilidad y seguridad de los sistemas. También el artículo 13 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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, 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, en su 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, que regula el Esquema Nacional de Seguridad, establece, en el artículo 12, 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. Asimismo, 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 adicional séptima recoge que, para la Gerencia Regional de Salud de Castilla y León, en atención a sus especiales funciones y singularidades respecto a su organización y funcionamiento, se podrá establecer una Política de Seguridad de la Información y Protección de Datos propia, resultando de aplicación, en todo caso, a la Gerencia Regional de Salud el Capítulo II del Decreto.

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.

De acuerdo con lo expuesto, el presente decreto regula la Política de Seguridad de la Información y Protección de Datos de la Gerencia Regional de Salud de Castilla y León, conforme a los principios y requisitos mínimos del Decreto 22/2021, de 30 de septiembre, así como a la organización establecida en su capítulo segundo. A tal efecto 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; la persona 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 de la Gerencia Regional de Salud", comprende los 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.

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.

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 ha garantizado 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. También ha sido sometido 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.

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).

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.

En su virtud dictamen, la Junta de Castilla y León, a propuesta del Consejero de Sanidad, de acuerdo con el del Consejo Consultivo de Castilla y León y previa deliberación del Consejo de Gobierno en su reunión de XX de XXXX de 202X.

DISPONE

CAPÍTULO I

Disposiciones Generales

Artículo 1. *Objeto.*

Constituye el objeto del presente decreto, 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, así como su marco organizativo y de gestión.

Artículo 2. *Ámbito de aplicación.*

1. La PSIPD_GRS aprobada mediante el presente decreto se aplicará a todos los sistemas de información y a 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.

2. La obligación de conocer y cumplir la PSIPD_GRS 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.

3. La PSIPD_GRS afectará a toda la información, con independencia del medio en que sea tratada y de su soporte.

4. La aplicación de la PSIPD_GRS se realizará en todos sus términos y condiciones, de acuerdo con el desarrollo normativo previsto en el artículo 21.

Artículo 3. *Definiciones.*

Las expresiones y términos utilizados en el presente decreto tendrán el significado indicado en el glosario de términos incluido en el Anexo IV del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como en las definiciones del artículo 4 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.

Artículo 4*. Marco regulatorio.*

La PSIPD_GRS se regirá, en lo no establecido por el presente decreto, por la normativa citada en el artículo 4 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, normativa sectorial aplicable, así como por la que se encuentre vigente en cada momento en materia de seguridad de la información y protección de datos.

Resultarán igualmente aplicables las normas jurídicas que regulen aspectos relacionados con el tratamiento de la información, tales como las que tengan por objeto la Administración electrónica, el patrimonio documental o la información protegida, entre otras.

Artículo 5. *Principios fundamentales de la Política de Seguridad de la Información y Protección de Datos de la Gerencia Regional de Salud.*

Toda la actividad relacionada con el uso de los activos de información y el tratamiento de datos personales en la Gerencia Regional de Salud se regirá por los principios fundamentales establecidos en el artículo 5 del Decreto 22/2021, de 30 de septiembre.

Artículo 6. *Directrices de la Política de Seguridad de la Información y Protección de Datos de la Gerencia Regional de Salud.*

1. La Gerencia Regional de Salud adoptará en su ámbito de aplicación las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos personales.

2. La PSIPD_GRS se ejecutará aplicando las directrices establecidas en el artículo 6 del Decreto 22/2021, de 30 de septiembre.

CAPÍTULO II

Organización de la Política de Seguridad de la Información y Protección de Datos de la Gerencia Regional de Salud

Artículo 7. *Estructura organizativa.*

1. En el marco de lo establecido en el capítulo II del Decreto 22/2021, de 30 de septiembre, la estructura organizativa encargada de la gestión de PSIPD_GRS de la Gerencia Regional de Salud, atendiendo a sus especiales funciones y singularidades en cuanto a su organización y funcionamiento, está constituida a nivel central y periférico por:

a) El Comité de Seguridad de la Información de la Gerencia Regional de Salud.

b) La Comisión Ejecutiva de Seguridad de la Información de la Gerencia Regional de Salud.

c) Las Comisiones Ejecutivas de Seguridad de la Información de las áreas de salud.

d) Los responsables de la información y del tratamiento de datos personales.

e) Los responsables del servicio.

f) Los encargados del tratamiento.

g) La persona responsable de la seguridad.

h) Los responsables de la seguridad delegados.

i) Los responsables del sistema.

j) Los administradores de seguridad del sistemas o sistemas.

k) El delegado de protección de datos de la Gerencia Regional de Salud.

Artículo 8. *Comité de Seguridad de la Información de la Gerencia Regional de Salud.*

1. El Comité de Seguridad de la Información de la Gerencia Regional de Salud, en adelante CSI_GRS, es el órgano colegiado de impulso, seguimiento y coordinación interna en esta materia en el ámbito del Servicio de Salud de Castilla y León.

2. El CSI_GRS está adscrito a la dirección general de la Gerencia Regional de Salud con competencias en materia de tecnologías de la información y la comunicación.

3. El CSI_GRS se someterá en su ámbito de actuación 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.

4. El CSI_GRS ejercerá las siguientes funciones:

a) La dirección y seguimiento de la aplicación de la legislación vigente, normas y estándares aplicables en materia de seguridad de las tecnologías de la información y las comunicaciones.

b) La aprobación de un código de conducta y buenas prácticas en materia de seguridad de la información y protección de datos, así como su seguimiento.

c) Impulsar y promover la divulgación de la Política de Seguridad de la Información y Protección de Datos, así como su cumplimiento y desarrollo normativo.

d) Definir, revisar y modificar tanto la Política de Seguridad de la Información y Protección de Datos, como el cuerpo normativo y documental que la desarrolla

cuando hubiere cambios en las tecnologías de la información y las comunicaciones, cambios normativos o legislativos, o en la organización.

e) La aprobación de las normas de seguridad según lo dispuesto en el artículo 21 de este decreto.

f) Aprobar mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en materia de ciberseguridad.

g) Impulsar nuevas líneas de trabajo en materia de seguridad de las tecnologías de la información y las comunicaciones, que conlleven la mejora continua del sistema de gestión de la seguridad de la información.

h) Gestionar, coordinar y supervisar la seguridad de la información a nivel de organización. En concreto, dirigir las acciones en materia de seguridad de la información de los proyectos cuyo fin sea generar acceso electrónico de la ciudadanía a los servicios de la Gerencia Regional de Salud.

i) Aprobar las medidas correctivas y mejoras derivadas de las auditorías de seguridad y de protección de datos personales, análisis de riesgos, evaluaciones de impacto, diagnósticos de seguridad de la información y hacer seguimiento de su implantación.

j) Aprobar los Planes de continuidad del negocio de la Gerencia Regional de Salud.

k) Aprobar el Plan de Auditoría y el Plan de Formación en materia de seguridad de la información.

l) Promover actividades de concienciación y formación en materia de seguridad de la información para todas las personas afectadas por esta política.

m) Informar regularmente del estado de la seguridad de la información a la Gerencia Regional de Salud.

n) Resolver los conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información.

o) Tomar aquellas decisiones que garanticen la protección de los datos personales, la seguridad de la información y de los servicios prestados por la entidad.

p) Aprobar informes periódicos del estado de la seguridad de la información en la Gerencia Regional de Salud, en colaboración con todas las unidades y centros que la componen, incluyendo entre otras cuestiones, los incidentes más relevantes de cada período.

q) Revisar la información aportada por la persona responsable de la seguridad de la Gerencia Regional de Salud relativa a los incidentes de seguridad.

r) Designar a los administradores de seguridad del sistema o sistemas.

s) Establecer la composición y el régimen de funcionamiento de la Comisión Ejecutiva de Seguridad de la Información de la Gerencia Regional de Salud y de las Comisiones Ejecutivas de Seguridad de la Información de las áreas de salud.

5. El CSI_GRS tendrá la siguiente composición:

a) Presidencia: la persona que ostente el cargo de Director Gerente de la Gerencia Regional de Salud.

b) Vicepresidencia: la persona titular de la dirección general de la Gerencia Regional de Salud con competencias en materia de tecnologías de la información y la comunicación, quien ejercerá la presidencia en caso de vacante, ausencia o enfermedad.

c) Vocalías:

1º. La persona responsable de la seguridad de la Gerencia Regional de Salud.

2º. Un representante de cada una de las direcciones generales de la Gerencia Regional de Salud designado por su titular.

3º. Cuatro representantes de las áreas de salud designados por la dirección general competente en materia de tecnologías de la información y la comunicación, dos pertenecientes al ámbito la atención primaria y dos pertenecientes al ámbito de la atención especializada

6. El delegado de protección de datos de la Gerencia Regional de Salud participará en las reuniones del CSI_GRS, con voz, pero sin voto, cuando vayan a abordarse cuestiones relacionadas con el tratamiento de datos personales, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar en acta su parecer.

7. Ejercerá la secretaria del CSI_GRS, con voz, pero sin voto, un empleado público designado por quien ostente la presidencia.

8. El CSI_GRS aprobará su reglamento interno de organización y funcionamiento, que se acomodará en todo caso a lo dispuesto en el Capítulo IV del Título V de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León; en la subsección 1.ª de la sección 3.ª del Capítulo II del Título preliminar de la Ley 40/2015, de 1 de octubre; en el presente decreto y en las propias normas de funcionamiento que en su caso se aprueben.

9. El CSI_GRS podrá crear grupos de trabajo permanentes para la realización de actividades que se estimen convenientes, tales como la elaboración de estudios, trabajos e informes. Cuando la complejidad de los asuntos a tratar así lo requiera, el CSI_GRS podrá constituir ponencias técnicas, de carácter temporal, para la mejor toma de decisiones.

Artículo 9. *Comisión Ejecutiva de Seguridad de la Información de la Gerencia Regional de Salud.*

1. La Comisión Ejecutiva de Seguridad de la Información, en adelante CESI_GRS, es el órgano colegiado que, bajo la dependencia del CSI_GRS y de acuerdo con las orientaciones y decisiones adoptadas en el mismo, tiene la obligación de velar por la seguridad de la información y los datos personales en sus sistemas de información, para lo cual deberá adoptar cuantas medidas técnicas y organizativas sean necesarias.

2. La CESI_GRS ejercerá las siguientes funciones:

   a) Coordinar la implantación de las medidas de seguridad adoptadas por el Comité de Seguridad de la Información de la Gerencia Regional de Salud.

   b) Promover y difundir normas, procedimientos e instrucciones técnicas.

   c) Proponer Programas de Concienciación y Formación en Seguridad de la Información para ser aprobados en el CSI_GRS.

   d) Proponer al CSI_GRS medidas correctivas y mejoras, derivadas de las auditorías de seguridad de la información y protección de datos personales, análisis de

riesgos y evaluaciones de impacto, así como hacer el seguimiento de su implantación.

e) Recabar la información necesaria de las unidades correspondientes, para certificar el cumplimiento de medidas de seguridad gestionadas por otros.

f) Proponer los Planes de continuidad del negocio para su aprobación por el CSI_GRS.

g) Proponer Planes de Auditoria para su aprobación por el CSI_GRS.

3. El CSI_GRS establecerá la composición y el régimen de organización y funcionamiento de la CESI_GRS.

En todo caso serán miembros de la CESI_GRS, un representante de la dirección general competente en materia de tecnologías de la información y la comunicación la persona responsable de la seguridad de la Gerencia Regional de Salud y las personas responsables del sistema de la Gerencia Regional de Salud.

Artículo 10. *Comisiones Ejecutivas de Seguridad de la Información de las áreas de salud.*

1. En cada área de salud existirá una Comisión Ejecutiva de Seguridad de la Información del área de salud, en adelante CESI_ASA. La CESI_ASA es el órgano colegiado que, bajo la dependencia el CSI_GRS y de acuerdo con las orientaciones y decisiones adoptadas en el mismo, tiene la obligación de velar por la seguridad de la información y los datos personales en sus sistemas de información, para lo cual deberá adoptar cuantas medidas técnicas y organizativas sean necesarias.

2. Las CESI_ASA ejercerán las siguientes funciones:

a) Aplicar la política y las medidas de seguridad de la información y apoyar las decisiones adoptadas por el CSI_GRS.

b) Promover la mejora continua de la seguridad de la información.

c) Promover los proyectos de seguridad relacionados con los procedimientos exigidos por la normativa vigente.

d) Delimitar las responsabilidades de todas las personas involucradas y coordinar los esfuerzos de los grupos de trabajo.

e) Proponer, al CSI_GRS, medidas correctivas y mejoras derivadas de las auditorias de seguridad y protección de datos personales, análisis de riesgos, evaluaciones de impacto, diagnósticos de seguridad de la Información y hacer el seguimiento de su implantación.

f) Recabar la información necesaria de las unidades correspondientes, para certificar el cumplimiento de medidas de seguridad gestionadas por otros.

g) Proponer los Planes de continuidad del negocio para su aprobación por el CSI_GRS.

h) Impulsar los programas de Concienciación y los Planes de formación en protección de datos personales y seguridad de la información, aprobados por el CSI_GRS.

3. El CSI_GRS establecerá la composición, organización y funcionamiento de las CESI_ASA.

En todo caso serán miembros cada la CESI_ASA los responsables de la información y del tratamiento, los responsables de seguridad delegados y los responsables de los sistemas de cada área de salud.

Artículo 11. *Los responsables de la información y el tratamiento de datos personales.*

1. De conformidad con el artículo 11 el Decreto 22/2021, de 30 de septiembre, las personas titulares de las direcciones generales de la Gerencia Regional de Salud serán los responsables de la información tratada en el ámbito de su competencia.

2. Asimismo, las personas titulares de las direcciones generales de la Gerencia Regional de Salud serán responsables del tratamiento de datos personales a los efectos del Reglamento (UE) 2016/679.

3. La persona que ostente el cargo de Director económico, presupuestario y financiero de la Gerencia Regional de Salud será, en su ámbito competencial, la persona responsable de la información y del tratamiento de datos personales.

4. Las personas que ostenten el cargo de Gerente de las distintas gerencias en que se organizan las áreas de salud, serán, en el ámbito competencial de su respectiva gerencia, los responsables de la información y del tratamiento de datos personales.

5. En el supuesto de competencias, procedimientos y/o proyectos compartidos entre distintos centros directivos será responsable del tratamiento la persona que ostente el cargo de Director Gerente de la Gerencia Regional de Salud, que decidirá efectivamente sobre la finalidad de la actividad de tratamiento y sobre los elementos esenciales de los medios para realizarla, tales como la determinación de las categorías de datos a tratar, el periodo de conservación, la procedencia de los datos, las personas que tratarán los datos y los destinatarios de estos.

6. En su respectivo ámbito competencial, los responsables de la información y del tratamiento de datos personales ejercerán, además de las funciones previstas en el artículo 11.3 del Decreto 22/2022, de 30 de septiembre, las siguientes:

a) Valorar el impacto que un incidente de seguridad podría tener sobre la información y los servicios.

b) Asumir la responsabilidad acerca del uso que se haga de los datos personales y de la información manejada dentro de su ámbito, así como de cualquier error o negligencia que desemboque en un incidente de seguridad que afecte a varias o todas las dimensiones de seguridad relevantes, especialmente a la confidencialidad y a la integridad.

c) Llevar a cabo de forma periódica el análisis de riesgos de las actividades de tratamiento y, realizar una evaluación del impacto cuando el tratamiento suponga un alto riesgo para los derechos y libertades de las personas.

d) Realizar la consulta previa a la AEPD cuando, tras la ejecución de la evaluación de impacto, se identifiquen riesgos que no se pueden evitar o mitigar suficientemente.

7. Cuando se establezca colaboraciones con terceros ajenos a la Gerencia Regional de Salud, de naturaleza pública o privada, considerados también responsables del tratamiento, se requerirá la formalización del debido acuerdo de corresponsabilidad, con arreglo al artículo 26 del Reglamento (UE) 2016/679.

8. En los casos en que exista corresponsabilidad del tratamiento se establecerá un único punto de contacto para los interesados, sin perjuicio de que estos puedan ejercer sus derechos ante cualquiera de los corresponsables.

Artículo 12. *Los responsables del servicio.*

De conformidad con el artículo 12 el Decreto 22/2021, de 30 de septiembre, las personas titulares de las direcciones técnicas y de los servicios o unidades administrativas equivalentes que gestionen cada procedimiento, proyecto o actuación, tendrán la consideración de responsable del servicio. Corresponde a los responsables del servicio determinar las características y los requisitos de seguridad de los servicios a prestar dentro de su ámbito.

Artículo 13. *Responsable de la seguridad de la Gerencia Regional de Salud.*

1. De conformidad con el artículo 13 el Decreto 22/2021, de 30 de septiembre, la persona que ostente el cargo de Director Gerente de la Gerencia Regional de Salud designará una persona responsable de la seguridad de la Gerencia Regional de Salud jerárquicamente independiente de la persona responsable del sistema. La designación se realizará previa propuesta de la persona titular de la dirección general competente en materia de seguridad de la información y podrá recaer en la persona titular del servicio o unidad equivalente encargada de la seguridad de la información en el ámbito de la Gerencia Regional de Salud.

2. La persona responsable de la seguridad de la Gerencia Regional de Salud, cuyo ámbito de actuación comprende todos los sistemas de información de la Gerencia Regional de Salud, ejercerá, además de las funciones previstas en el artículo 13.2 del Decreto 22/2022, de 30 de septiembre, las siguientes:

a) Dirigir y coordinar la respuesta a los incidentes de seguridad, junto con otras unidades de la Gerencia Regional de Salud, analizando y proponiendo salvaguardas que prevengan incidentes futuros.

b) Elaborar informes periódicos del estado de la seguridad de la información, para el Comité de Seguridad de la Información o para la Comisión Ejecutiva correspondiente, que incluyan los incidentes más relevantes de cada período.

c) Recoger los requisitos de protección de datos que sean fijados por la persona responsable o encargado del tratamiento contando con el asesoramiento del delegado de protección de datos de la Gerencia Regional de Salud.

d) Determinar la categoría de los sistemas de información de la Gerencia Regional de Salud en función de la valoración realizada por los responsables de la información y de los servicios.

e) Seleccionar las medidas de seguridad apropiadas, incluso medidas adicionales, y supervisar su implantación para garantizar que se satisfacen los requisitos de seguridad.

f) Elaborar, en coordinación con la persona responsable del sistema, los planes de mejora de la seguridad de los sistemas de información.

g) Validar los Planes de Continuidad elaborados por la persona responsable del sistema y aprobados por el Comité de Seguridad de la Información.

h) Registrar, gestionar y solucionar incidentes de seguridad, en colaboración con la persona responsable del sistema.

i) Designar a los responsables de la seguridad delegados, a propuesta de los responsables de la información de las gerencias dependientes de la Gerencia Regional de Salud.

j) Dirigir y coordinar la seguridad de la información con los responsables de la seguridad delegados.

k) Constituir grupos de trabajo con los responsables de la seguridad delegados cuando lo estime necesario.

3. Asimismo, la persona responsable de la seguridad de la Gerencia Regional de Salud se constituye como único punto de contacto y coordinación técnica con la autoridad competente, conforme a lo previsto en el apartado 3 del artículo 16 del Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información.

4. En el ejercicio de sus funciones la persona responsable de la seguridad de la Gerencia Regional de Salud podrá recabar el asesoramiento, si fuera necesario, de los servicios jurídicos de la Administración de la Comunidad de Castilla y León, a través de los cauces correspondientes y conforme a su normativa reguladora y de los servicios técnicos de la propia Gerencia Regional en particular, los servicios con competencias en materia de tecnologías de la información y las comunicaciones.

Artículo 14. *Los responsables de la seguridad delegados*.

1. Con el fin de asegurar el carácter transversal de la seguridad de la información, la persona responsable de la seguridad de la Gerencia Regional de Salud designará una persona responsable de la seguridad delegada para cada Gerencia en que se organice el área de salud, previa propuesta del Gerente de quien dependa.

2. Cada responsable de la seguridad delegado mantendrá una dependencia funcional directa de la persona responsable de seguridad de la Gerencia Regional de Salud, a quien reportará y su ámbito de actuación se limitará a los sistemas de información que sean competencia de la Gerencia a la que pertenece.

3. A la persona responsable de la seguridad delegada, corresponden las siguientes funciones:

a) Identificar los sistemas de información de su centro, mantener el inventario actualizado de los mismos y categorizarlos en colaboración con los recursos de la Gerencia Regional de Salud.

b) Ser el punto de contacto único con la persona responsable de la seguridad de la Gerencia Regional de Salud y el delegado de protección de datos de la Gerencia Regional de Salud para cualquier actuación en el ámbito de la seguridad de la información y protección de datos.

c) Coordinar y mantener la seguridad de la información y la protección de los datos personales dentro de su ámbito.

d) Aplicar la normativa de seguridad transversal y específica de su ámbito, debiendo notificar esta última al responsable de la seguridad de la Gerencia Regional de Salud.

e) Informar periódicamente al responsable de la seguridad de la Gerencia Regional de Salud sobre la actividad desarrollada dentro de su ámbito, y cuando las circunstancias lo requieran.

f) Notificar al responsable de la seguridad de la Gerencia Regional de Salud la adquisición o implantación de nuevos productos y servicios para su autorización previa.

g) Informar periódicamente al Gerente del que dependa, del estado de la seguridad de la información y siempre que las circunstancias lo requieran.

h) Atender los requerimientos de la persona responsable de la seguridad de la Gerencia Regional de Salud dentro un plazo máximo de diez hábiles.

i) Promover la concienciación y formación dentro de su ámbito, de acuerdo con los planes de formación corporativos. Detectar y recibir las necesidades formativas.

j) Contactar con el delegado de protección de datos de la Gerencia Regional de Salud para actuaciones relacionadas con su centro.

k) Apoyar en la gestión de incidentes de seguridad.

l) Analizar los riesgos a los que los sistemas de información estén expuestos, formalizar y firmar la “Declaración de Aplicabilidad” relativa a los sistemas propios.

m) Colaborar en tareas de inspección mediante la realización de análisis de riesgos, auditorías y controles periódicos.

n) Analizar los informes de auditoría.

o) Participar en la categorización de los sistemas de información en función de las valoraciones realizadas por los responsables de la información y colaborar en seleccionar medidas de seguridad apropiadas.

p) Elaborar, junto con la persona responsable del sistema, los planes de mejora de seguridad de los sistemas de información.

q) Trasladar los criterios de acceso a los sistemas de información en consonancia con las normas de la Gerencia Regional de Salud.

r) Analizar periódicamente los riesgos a los que los sistemas de información propios de su ámbito están expuestos e informar de los mismos al responsable de la seguridad de la Gerencia Regional de Salud.

s) Participar en los grupos de trabajo que puedan ser constituidos por la persona responsable de seguridad de la Gerencia Regional de Salud.

t) Aquellas otras funciones que se establezcan por delegación.

Artículo 15. *Los responsables del sistema.*

1. De conformidad con el artículo 14 del Decreto 22/2021, de 30 de septiembre, son responsables del sistema de la Gerencia Regional de Salud, la persona titular del servicio con competencias en materia de tecnologías de la información y la persona titular del servicio con competencias en materia de comunicaciones.

2. Son responsables del sistema en el ámbito periférico, la persona titular del servicio con competencias en materia de informática de cada Gerencia en que se organice el área de salud, dentro de su propio ámbito de actuación.

3. Los responsables del sistema ejercerán dentro de su ámbito de competencias, además de las funciones previstas en el artículo 14.2 del Decreto 22/2021, de 30 de septiembre, las siguientes:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y sistema de gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Velar por la implementación de las medidas de seguridad en función de la categorización de los sistemas y su integración dentro del marco general de seguridad.

d) Adoptar las medidas correctoras adecuadas que garanticen la seguridad de los sistemas de información.

e) Verificar trimestralmente, las personas usuarias autorizadas para acceder a los sistemas de información, dejando constancia de dicha revisión.

f) Autorizar, registrar y controlar las entradas y salidas de soportes dejando constancia.

g) Registrar, gestionar, notificar y solucionar incidencias, en colaboración con la persona responsable de la seguridad de la Gerencia Regional de Salud y responsables de la seguridad delegados, según su ámbito de actuación

h) Elaborar informes respecto a las actuaciones realizadas en su ámbito de responsabilidad, con la periodicidad que se establezca.

i) Colaborar, reportar y atender los requerimientos de información de la persona responsable de la seguridad.

Artículo 16. *Los administradores de seguridad del sistema o sistemas.*

1. Con el fin de asegurar la correcta implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información, el CSI_GRS designará administradores de seguridad 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.

2. El administrador de seguridad reportará al responsable del sistema y ejercerá, dentro de su ámbito de actuación, las siguientes funciones:

a) Garantizar la implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

b) Monitorizar la gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

c) Controlar la gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

d) Validar la aplicación de los procedimientos operativos de seguridad.

e) Afianzar que los controles de seguridad establecidos son adecuadamente observados.

f) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

h) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

i) Informar al responsable de la seguridad o al responsable del sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

3. 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.

4. En los casos en que no se designe un administrador de seguridad, este rol podrá coincidir con el rol del responsable del sistema.

Artículo 17. *Responsables delegados.*

Además de lo previsto en el artículo 15 en relación con los responsables de la seguridad delegados, podrán nombrarse por los responsables de la información y del servicio cuantos responsables delegados consideren necesarios para el eficaz desempeño de sus atribuciones, en función de la complejidad, especificidad, distribución, volumen o número de personas usuarias de los sistemas de información gestionados.

Los responsables del sistema de la Gerencia Regional de Salud, en concreto la persona titular del servicio con competencias en materia de tecnologías de la información y la persona titular del servicio con competencias en materia de comunicaciones podrán también nombrar responsables delegados para el desempeño de sus atribuciones.

Los responsables delegados estarán sujetos a las mismas responsabilidades que los responsables titulares, conservando estos últimos en todo caso la responsabilidad final sobre las actuaciones realizadas.

Artículo 18. *Grupos de trabajo.*

1. Los responsables definidos en los artículos 12 a 15 podrán constituir un grupo de trabajo específico para cada modalidad de responsable.

2. Las reuniones de los grupos de trabajo podrán celebrarse por medios electrónicos.

Artículo 19. *Resolución de conflictos.*

1. Los conflictos entre las diferentes personas, unidades y órganos responsables que componen la estructura organizativa de la política de la PSIPD_GRS serán resueltos por el superior jerárquico común, que podrá elevar consulta previa al CSI_GRS. En caso de conflicto prevalecerán las decisiones del CSI_GRS.

2. En la resolución de estos conflictos prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos personales.

Artículo 20. *El delegado de protección de datos de la Gerencia Regional de Salud.*

1. En los términos previstos en el Decreto 22/2021, de 30 de septiembre, existirá una persona delegada de protección de datos en la Gerencia Regional de Salud con las responsabilidades y funciones recogidas en la citada norma.

2. El delegado de protección de datos llevará a cabo las funciones establecidas en el artículo 39 del Reglamento (UE) 2016/679, de conformidad con lo que este dispone y con lo que establece la normativa estatal y de la Comunidad.

3. En el desempeño de sus funciones, el delegado de protección de datos tendrá acceso a los datos personales y operaciones de tratamiento, no pudiendo, el responsable o el encargado del tratamiento oponer a este acceso la existencia de cualquier deber de confidencialidad o secreto.

4. La Gerencia Regional de Salud nombrará un único delegado de protección de datos para toda la organización, órgano unipersonal, cuyo nombramiento será comunicado a la Agencia Española de Protección de Datos, y a la propia organización, con competencias en la Gerencia Regional de Salud, las gerencias, los organismos y los centros que dependen o están vinculados con ella.

CAPÍTULO III

Desarrollo de la Política de Seguridad de la Información y Protección de Datos

Artículo 21. *Estructura documental y normativa.*

1. El cuerpo documental de la Gerencia Regional de Salud sobre seguridad de la información se desarrollará en cuatro niveles por ámbito de aplicación, nivel de detalle técnico y de obligado cumplimiento, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior.

2. Los niveles de desarrollo documental son los siguientes:

a) Primer nivel. Política de Seguridad de la Información.

Está constituido por el presente decreto y es de obligado cumplimiento, al amparo de lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

b) Segundo nivel. Normas de seguridad de la información.

Las normas de seguridad uniformizan el uso de aspectos concretos del sistema e indican el uso correcto y las responsabilidades de las personas usuarias.

Son de obligado cumplimiento, según lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y se formalizarán mediante aprobación del CSI_GRS.

Las normas de seguridad desarrollarán, entre otros, los siguientes aspectos:

- Protección de datos personales.
- Organización de la seguridad y responsabilidades.
- Seguridad ligada a las personas que trabajan o prestan sus servicios en la organización.
- Clasificación y control de activos.
- Control de accesos y gestión de claves.
- Seguridad física y del entorno.
- Gestión de operación y comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad.
- Gestión de la continuidad del negocio.
- Conformidad legal.

Cada uno de estos aspectos de la seguridad podrá ser desarrollado en una o varias normas de seguridad.

Las normas de seguridad serán publicadas en la intranet del portal corporativo de la Gerencia regional de Salud, en el plazo de 10 días desde su aprobación, salvo que por el nivel de confidencialidad o por la naturaleza de la información deba limitarse su difusión.

c) Tercer nivel. Procedimientos operativos de seguridad.

Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos operativos de seguridad dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado, y recaerá en la persona titular de la dirección general competente en la materia sobre la que se desarrolla el

procedimiento, previa validación por parte de la persona responsable de la seguridad de la Gerencia Regional de Salud.

d) Cuarto nivel. Guías técnicas de seguridad e instrucciones técnicas.

Las guías técnicas de seguridad y las instrucciones técnicas tienen como objetivo proporcionar las recomendaciones y pasos a seguir por los usuarios, para la correcta implantación de medidas de seguridad sobre la infraestructura tecnológica que soporta la información y servicios de la organización.

Su aprobación corresponde a la persona responsable de la seguridad de la. Gerencia Regional de Salud.

3. El CSI_GRS establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo documental con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política.

4. Además de las normas, procedimientos y guías de seguridad, la estructura documental de la Gerencia Regional de Salud podrá incluir otros documentos tales como informes técnicos, registros, evidencias, que son documentos de carácter técnico en los que se recogen el resultado y las conclusiones de un estudio y o de una evaluación, registros de actividad o alertas de seguridad.

Artículo 22. *Gestión y coordinación de la Política de Seguridad.*

1. La gestión de la seguridad se llevará a cabo de manera diferenciada por cada figura implicada.

2. La coordinación entre las diferentes figuras implicadas deberá tener en cuenta que:

a) La persona responsable de la seguridad de la Gerencia Regional de Salud reportará, al CSI_GRS, así como al CESI_GRS, los temas que afecten a la seguridad de la información.

Las personas responsables de la seguridad delegados reportarán a la CESI_ASA correspondiente, determinada por su ámbito competencial, los temas que afecten a la seguridad de la información. Asimismo, reportarán al responsable de la seguridad de la Gerencia Regional de Salud.

En concreto, se informará acerca de las siguientes cuestiones:

1º. Las decisiones e incidentes en materia de seguridad que afecten a la información y al servicio de la Gerencia Regional de Salud, en particular, de lo relativo al riesgo residual y a las desviaciones de riesgo respecto de los márgenes aprobados como asumibles.

2º. Resumen consolidado de las actuaciones llevadas a cabo en materia de seguridad de la información.

3º. Resumen consolidado de las actuaciones llevadas a cabo en relación con los incidentes que afecten seguridad de la información y la protección de los datos personales.

4º. Estado de la seguridad del sistema, en particular, del riesgo residual al que el sistema está expuesto.

b) La CESI_GRS y las CESI_ASA reportarán al CSI_GRS.

c) Las personas responsables del sistema reportarán a la persona responsable de la seguridad correspondiente sobre las actuaciones en materia de seguridad dentro del ámbito de su competencia, y le informará acerca de las siguientes cuestiones:

1º. Las incidencias relativas a la información y servicios que le competen.

2º. Las actuaciones en materia de seguridad, en particular, en lo relativo a decisiones de arquitectura del sistema, así como de cualquier decisión relevante que afecte a la protección de datos personales.

3º. El resumen consolidado de incidentes de seguridad que hubieren tenido lugar.

4º. El resumen de la eficacia de las medidas de protección implantadas.

d) Las personas designadas como administradores de seguridad reportarán a la persona responsable del sistema correspondiente sobre la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información dentro del ámbito de su competencia, y le informarán de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad del sistema.

CAPÍTULO IV

Gestión de la Política de Seguridad de la Información y Protección de Datos

Artículo 23. *Análisis de riesgos, evaluación de impacto en la protección de datos y gestión de riesgos de seguridad de la información.*

1. El proceso de gestión de riesgos de seguridad de la información deberá realizarse de manera continua sobre todos los sistemas de información sujetos a la presente PSIPD, conforme a las directrices establecidas en el Real Decreto 311/2022, de 3 de mayo.

2. Cuando la información contenga datos personales también se llevará a cabo un análisis de riesgos con el fin de identificar, evaluar y tratar las amenazas para los derechos y libertades de las personas físicas con respecto a las actividades de tratamiento.

3. Este análisis de riesgos deberá realizarse de forma periódica y en todo caso, al menos, una vez cada dos años.

4. Para cada tipo de riesgo se utilizarán las metodologías de análisis y gestión de riesgos que resulten más apropiadas, siguiendo a lo establecido en la normativa vigente en materia de seguridad de la información y protección de datos personales, así como a las indicaciones de la Agencia Española de Protección de Datos y demás autoridades competentes al respecto.

5. Las personas responsables de la información y del servicio son los encargados de establecer los requisitos de la información y los servicios en materia de seguridad y, en consecuencia, de aceptar los riesgos residuales.

6. Corresponde al responsable de la seguridad de la Gerencia Regional de Salud la selección de las medidas de seguridad a aplicar.

7. Cuando del análisis de riesgos realizado resulte probable que el tratamiento supone un riesgo significativo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del Reglamento (UE) 2016/679, la persona responsable del tratamiento recabará el asesoramiento de la persona delegada de protección de datos

de la Gerencia Regional de Salud y deberá realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

8. La persona responsable de seguridad de la Gerencia Regional de Salud, los responsables de seguridad delegados y los responsables del sistema correspondientes, aprobarán conjuntamente un plan de gestión de riesgos para su ámbito de competencia.

Artículo 24. *Uso de medios digitales.*

Los medios digitales puestos a disposición de las personas empleadas públicas se destinarán exclusivamente al cumplimento de las obligaciones laborales o estatutarias.

Con pleno respeto del derecho a la intimidad de las personas trabajadoras, la protección de los datos personales y el secreto de las comunicaciones, la Gerencia Regional de Salud podrá acceder a los contenidos derivados del uso de los medios digitales de su titularidad, incluidas las comunicaciones que estén cifradas, para garantizar la integridad de los medios digitales y la continuidad en la prestación de los servicios públicos. Con la misma finalidad, dichos contenidos podrán ser capturados y almacenados para su análisis posterior.

En todo caso, las medidas adoptadas para acceder la información deben ser idóneas, necesarias y proporcionales.

Artículo 25. *Auditoría de seguridad.*

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos de la presente política, del Esquema Nacional de Seguridad o de cualquier otra norma que así lo requiera.

Con carácter extraordinario, se realizará dicha auditoría cuando existan cambios sustanciales en la información tratada o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves.

2. Las auditorías serán supervisadas por la persona responsable de seguridad de la Gerencia Regional de Salud y por el delegado de protección de datos. La persona

responsable de seguridad delegado analizará el resultado de las auditorías correspondientes a su ámbito de actuación.

Artículo 26. *Notificaciones de violaciones de seguridad de los datos personales.*

En relación con la notificación de violaciones de seguridad de datos personales, se aplicará lo dispuesto en el artículo 24 del Decreto 20/2021, de 30 de septiembre.

Artículo 27. *Registro de las actividades de tratamiento.*

1. La Gerencia Regional de Salud elaborará un registro de actividades de tratamiento de datos personales, conforme a los criterios que establezca la consejería competente en materia de protección de datos, una vez oídas las recomendaciones efectuadas por el delegado de protección de datos de la Gerencia Regional de Salud.

2. La persona responsable del tratamiento en el ámbito de sus competencias llevará y mantendrá actualizado el registro de actividades de tratamiento de datos personales, que incluirá la información a la que se refiere el artículo 30 del Reglamento (UE) 2016/679, y se documentará de acuerdo con los criterios a que se refiere el apartado 1 de este artículo.

La persona responsable del tratamiento comunicará al delegado de protección de datos el registro de las actividades de tratamiento de datos que gestiona en su ámbito de actuación, así como sus modificaciones, en el plazo de diez días desde que se produzcan.

3. La Gerencia Regional de Salud hará público el inventario de sus actividades de tratamiento accesible a través del Portal de Transparencia de SACYL. Para ello, cada responsable de tratamiento comunicará al delegado de protección de datos de la Gerencia Regional de Salud, la información necesaria para su formación, en el modelo que este establezca.

Artículo 28. *Formación y concienciación.*

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de todas las personas que presten servicios en la Gerencia Regional de Salud, así como a la difusión entre las mismas de la PSIPD y de su desarrollo normativo, pudiendo, en algún caso, recabar la colaboración de entidades encargadas de coordinar las acciones de seguridad de la información en los organismos públicos.

2. A estos efectos, deberán incluirse actividades formativas en materia de seguridad de la información y protección de datos personales, dentro de los Planes de Formación de la Gerencia Regional de Salud.

Artículo 29. *Obligaciones profesionales.*

1. Todas las personas que presten servicios en la Gerencia Regional de Salud, como usuarias de los sistemas de información bajo su responsabilidad, cumplirán con las siguientes obligaciones:

a) Conocer y cumplir la PSIPD_GRS y demás normativa de seguridad derivada de ella.

b) Conocer y cumplir los códigos de conducta y buenas prácticas en materia de seguridad de la información y protección de datos, que sean adoptados por la Gerencia Regional de Salud.

c) Cumplir con las obligaciones establecidas en la normativa de protección de datos personales y tratar los datos siguiendo las instrucciones de la persona responsable del tratamiento.

d) Colaborar en la implementación, mejora de los principios y requisitos en materia de protección de datos y seguridad de la información, con el fin de evitar y aminorar los riesgos a los que se encuentra expuesta la información y los datos personales.

2. El CSI_GRS será el responsable de asegurar que la PSIPD sea conocida por todas las personas usuarias de los sistemas de información de la Gerencia Regional de Salud.

Adicionalmente, la publicación de la presente PSIPD_GRS se llevará a cabo en el portal web corporativo de la organización para una amplia y efectiva difusión de la misma.

3. Todas las unidades y órganos de la Gerencia Regional de Salud de Castilla y León prestarán su colaboración en las actuaciones de implementación de la PSIPD_GRS aprobada en este decreto.

DISPOSICIONES ADICIONALES

Primera*. Comités de Ética de la Investigación.*

1. Los Comités de Ética de la Investigación, acreditados y adscritos a la Consejería de Sanidad de la Comunidad de Castilla y León, también deberán aplicar los principios y previsiones de la PSIPD_GRS.

2. La Gerencia Regional de Salud y los Comités de Ética de la Investigación colaborarán e informarán con el fin de cumplir con la normativa vigente aplicable en materia de protección de datos y de investigación, mediante la coordinación y evaluación conjunta de los proyectos de investigación, por parte de las personas delegadas de protección de datos de cada organismo, o persona experta, en el caso de los Comités de Ética de la Investigación.

Asimismo, la persona delegada de protección de datos de la Gerencia Regional de Salud, en el ejercicio de sus funciones, podrá requerir al Comité de Ética de la Investigación, cuanta información sea necesaria acerca de los tratamientos de datos responsabilidad de la Gerencia Regional de Salud.

Segunda. *Designación de las personas responsables.*

Los responsables de seguridad serán designados, en caso de no estarlo, en el plazo máximo de tres meses a contar desde el día siguiente a la entrada en vigor del presente decreto.

En el mismo plazo cada centro directivo remitirá una relación de los responsables de la información, del servicio y del sistema a la dirección general de la Gerencia Regional de Salud con competencias en materia de tecnologías de la información y la comunicación.

Tercera. *Constitución de los órganos colegiados de seguridad de la Información.*

En el plazo de dos meses a contar desde el día siguiente a la entrada en vigor del presente decreto se celebrará la sesión constitutiva del CSI_GRS.

En dicha sesión se aprobará la composición y el régimen de organización y funcionamiento de la CESI_GRS y de las CESI_ASA.

DISPOSICIÓN DEROGATORIA

Derogación normativa.

Quedan derogadas todas las disposiciones de igual o inferior rango que se opongan a este Decreto.

DISPOSICIONES FINALES

Primera. *Habilitación normativa.*

Se faculta a la persona titular de la Consejería competente en materia de sanidad para dictar las disposiciones y actos necesarios para el desarrollo y ejecución del presente Decreto.

Segunda. *Entrada en vigor.*

El presente Decreto entrará en vigor el mismo día de su publicación en el “Boletín Oficial de Castilla y León”.