I. COMUNIDAD DE CASTILLA Y LEÓN

A. DISPOSICIONES GENERALES

CONSEJERÍA DE ECONOMÍA Y HACIENDA

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, establece, en su artículo 13, el derecho de los ciudadanos a la protección y confidencialidad de sus datos y a la seguridad de los mismos cuando figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

En el mismo sentido, la 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 determinan los principios básicos y requisitos mínimos que han de garantizar la seguridad de la información tratada.

El Esquema Nacional de Seguridad, que fue aprobado mediante Real Decreto 3/2010, de 8 de enero, y modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene como finalidad la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el Capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada) y desarrollará una serie de requisitos mínimos.

La Estrategia de Ciberseguridad de la Unión Europea presentada por la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, en diciembre de 2020, tiene como finalidad reforzar la resiliencia colectiva europea contra las ciberamenazas y ayudar a garantizar que todos los ciudadanos y las empresas puedan beneficiarse plenamente de unos servicios y herramientas digitales fiables y de confianza, correspondiendo a las Administraciones Públicas un papel destacado en la custodia de un ciberespacio libre y seguro.

Asimismo, 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, pretende sentar las bases de una normativa de privacidad que se adecue a la nueva realidad tecnológica y social, dando un paso más en la defensa de los derechos de los ciudadanos, en lo que hace referencia a su privacidad.

Por otra parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tiene por objeto, a tenor de lo dispuesto en su artículo 1, adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679, antes mencionado, completando sus disposiciones y garantizando los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución. De igual modo, la disposición adicional primera de esta ley orgánica 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.

En el ámbito autonómico, por lo que se refiere a la política de seguridad de la información, el artículo 3 del Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León, exige, asimismo, que esta se desarrolle aplicando el Esquema Nacional de Seguridad.

En consonancia con esa previsión se dictó la Orden HAC/858/2014, de 30 de septiembre, por la que se aprueba la política de seguridad de la información de la Administración de la Comunidad de Castilla y León. La orden dispone que esta política tiene que ser objeto de una revisión periódica. Esta necesidad de revisión se justifica aún más por el periodo de tiempo transcurrido desde su aprobación, por los cambios normativos que se han producido y por los cambios habidos en las distintas estructuras orgánicas de las diferentes consejerías.

Por lo que atañe a la política de protección de datos personales, el artículo 12 del Estatuto de Autonomía de Castilla y León dispone, en el marco del derecho a una buena Administración, que la ley garantizará a los ciudadanos en sus relaciones con la Administración autonómica, entre otros, el derecho a la protección de datos personales.

El artículo 45 de 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, establece que las actuaciones administrativas a través de medios electrónicos respetarán, en todo caso, la normativa sobre protección de datos de carácter personal.

Por su parte, el Decreto 11/2003, de 23 de enero, por el que se regulan los ficheros de datos de carácter personal susceptibles de tratamiento automatizado de la Administración de la Comunidad de Castilla y León, establece las disposiciones necesarias para garantizar en ese ámbito el cumplimiento de la legislación estatal en la materia. Toda vez que el Reglamento (UE) 2016/679 es aplicable desde el día 25 de mayo de 2018, resulta necesaria la derogación expresa y sustitución de este decreto.

Por tanto, visto que es necesario adaptar ambas políticas a la legislación vigente y a la realidad actual, y dado que están íntimamente ligadas, se considera conveniente aprobar una norma que las regule de manera conjunta y en la que se establezcan claramente las funciones, actividades y responsabilidades implicadas.

El presente decreto responde, tanto en su finalidad y contenido como en el procedimiento de su elaboración, a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. También han sido tenidos en cuenta los principios de accesibilidad, coherencia, y responsabilidad establecidos en la Ley 2/2010, de 11 de marzo.

En este sentido, partiendo de los planteamientos que informan los principios de necesidad, eficiencia y eficacia, y poniéndolos en relación con lo expuesto en los párrafos precedentes, puede afirmarse que este 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. Se considera que este decreto es adecuado para garantizar su consecución evitando cargas administrativas innecesarias o accesorias y racionalizando, en su aplicación, la gestión de los recursos públicos al no implicar incremento del gasto.

Por lo que respecta al cumplimiento del 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 contenido de este decreto 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. El decreto 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 en la elaboración del decreto a través de los mecanismos de consulta previa, audiencia e información pública y petición de los informes correspondientes.

El Decreto 20/2019, de 1 de agosto, por el que se establece la estructura orgánica de la Consejería de Transparencia, Ordenación del Territorio y Acción Exterior, atribuye a esta Consejería las competencias en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales. Por su parte, el Decreto 23/2019, de 1 de agosto, regulador de la estructura orgánica de la Consejería de Fomento y Medio Ambiente, encomienda a esta las competencias en materia de coordinación y ejecución de las medidas que garanticen la seguridad de los sistemas de información.

La experiencia acumulada en la gestión de las materias indicadas, las referidas modificaciones normativas y los cambios organizativos habidos en estos sectores de la actividad administrativa hacen necesaria la presente norma para configurar una política de seguridad de la información y protección de datos personales acorde con el momento actual.

La Política de Seguridad de la Información y Protección de Datos define el marco de referencia que permite la gestión de la seguridad de la información en los sistemas de la Administración de la Comunidad de Castilla y León y la gestión de los datos personales. Seguridad y gestión entendidas como un proceso integral que incluye todos los elementos técnicos, humanos, materiales y organizativos de los diferentes sistemas de información.

Conforme al artículo 5.c) del Decreto 7/2013, de 14 de febrero, corresponde a la Consejería de Fomento y Medio Ambiente, como consejería competente en la dirección y ejecución de las actuaciones en materia de Administración electrónica, la aprobación de la política de seguridad de la información de la Administración de la Comunidad de Castilla y León, todo ello sin perjuicio de las competencias que en materia de protección de datos corresponden a la Consejería de Transparencia, Ordenación del Territorio y Acción Exterior, y de las especialidades derivadas de la aplicación del Decreto 86/2006, de 7 de diciembre, por el que se designó a la entonces denominada Consejería de Agricultura y Ganadería para actuar como Organismo Pagador de los gastos financiados por el por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

Según lo establecido en el artículo 70.3 de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León, cuando afecte a las competencias de más de una Consejería, los decretos o acuerdos se aprobarán a iniciativa de los consejeros interesados y será propuesto por el de Presidencia y Administración Territorial. Si bien, de acuerdo con la disposición adicional única del Decreto 2/2019, de 16 de julio, del Presidente de la Junta de Castilla y León, de reestructuración de consejerías, las referencias que en la Ley 3/2001, de 3 de julio, se realizan al Consejero de la Presidencia y Administración Territorial, se entenderán efectuadas, al titular de la Consejería de Economía y Hacienda.

En su virtud, la Junta de Castilla y León, a propuesta del Consejero de Economía y Hacienda e iniciativa de los Consejeros de Transparencia, Ordenación del Territorio y Acción Exterior, y de Fomento y Medio Ambiente, de acuerdo con el dictamen del Consejo Consultivo de Castilla y León y previa deliberación del Consejo de Gobierno en su reunión de 30 de septiembre de 2021

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 Protección de Datos de la Administración de la Comunidad de Castilla y León (en adelante, PSIPD), así como su marco organizativo y de gestión.

Artículo 2. Ámbito de aplicación.

1. La PSIPD aprobada mediante el presente decreto será de aplicación 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, sin perjuicio de que dichos organismos y entidades puedan aprobar su propia política de seguridad de la información y protección de datos en coherencia con el presente decreto, del que, en todo caso, les será de aplicación el Capítulo II.

2. La obligación de conocer y cumplir la PSIPD se extiende a todo el personal que acceda, tanto a los sistemas de información, como a la propia información gestionada por la Administración de la Comunidad de Castilla y León, con independencia de la naturaleza de su relación con esta Administración y de su destino o adscripción.

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

4. La aplicación de la PSIPD se realizará en todos sus términos y condiciones, de acuerdo con el desarrollo normativo previsto en el artículo 19.

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 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, 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.

1. Serán de aplicación a la PSIPD las disposiciones en materia de seguridad de la información y protección de datos de carácter personal contenidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público; en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014; en 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; y en el Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León.

2. La información contenida en los sistemas de información del ámbito de la Administración electrónica se encuentra recogida en el Real Decreto 3/2010, de 8 de enero.

3. Al tratamiento de la información que contenga datos de carácter personal le será aplicable el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. 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.

5. Asimismo, formarán parte del marco regulatorio de la PSIPD todos los instrumentos regulados en el Capítulo III.

Artículo 5. Principios fundamentales de la Política de Seguridad de la Información y Protección de Datos.

Toda la actividad relacionada con el uso de los activos de información y el tratamiento de datos personales en la Administración de la Comunidad de Castilla y León se regirá por los siguientes principios fundamentales:

a) Principio de alcance estratégico: La PSIPD contará con el compromiso de todos los niveles directivos de modo que la seguridad de la información y la protección de datos estén integradas y coordinadas con las decisiones estratégicas de la Administración de la Comunidad.

b) Principio de seguridad integral: La seguridad se entenderá como un proceso integral y planificado, constituido por todos los elementos técnicos, humanos, materiales, procedimentales y organizativos relacionados con los sistemas de información, evitando las actuaciones puntuales o tratamientos coyunturales.

c) Principio de ciclo completo y seguridad por defecto: Se contemplarán los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. La seguridad debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Principio de gestión de riesgos: El análisis y la gestión de los riesgos serán parte esencial y permanente del proceso de seguridad. Mediante el análisis de riesgos se detectan los problemas de seguridad y con su correcta gestión se persigue reducirlos a un nivel aceptable mediante la selección e implantación de medidas de seguridad.

e) Principio de proporcionalidad: El establecimiento de medidas de protección, detección y recuperación será proporcional, en sus costes económicos y operativos, a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Principio de responsabilidad diferenciada: En los sistemas de información se diferenciarán el responsable de la información, el responsable del servicio, el responsable del sistema y el responsable de la seguridad. En ningún caso podrán recaer en una misma persona las responsabilidades de seguridad y del sistema.

g) Principio de responsabilidad proactiva: El responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de la información se hace conforme a la normativa española y europea en la materia.

h) Principio de legitimación en el tratamiento de datos personales: Solo se tratarán los datos de carácter personal cuando dicho tratamiento esté legitimado en alguna de las causas previstas en el Reglamento (UE) 2016/679.

i) Principio de licitud, lealtad y transparencia: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.

j) Principio de limitación de la finalidad: Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

k) Principio de minimización de datos: Los datos tratados serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que sean tratados.

l) Principios de integridad y calidad: Se garantizará el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y, en su caso, actualización.

m) Principio de limitación del plazo de conservación: Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que pudieran derivarse de su tratamiento.

Los datos podrán conservarse durante periodos más largos cuando sean tratados exclusivamente con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos de acuerdo con lo establecido en el Reglamento (UE) 2016/679. El tratamiento para estos fines se realizará con las medidas técnicas y organizativas adecuadas, respetando particularmente el principio de minimización de los datos personales, así como, cuando sea posible, su anonimización. En esta modalidad de tratamiento será a su vez de aplicación lo dispuesto en la normativa sobre archivos y documentación.

n) Principio de confidencialidad: Quienes intervengan en el tratamiento estarán obligados a guardar el deber de secreto, incluso después de haber finalizado el proceso de tratamiento.

ñ) Principio de profesionalidad: La seguridad de los sistemas estará implantada, atendida, revisada y auditada por personal cualificado y formado, que participará en todas las fases del ciclo de vida de los sistemas.

o) Principio de prevención, disponibilidad y recuperación: Se desarrollarán planes de acción y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. Se asegurará el nivel de disponibilidad requerido para los activos y recuperación ante cualquier contingencia.

p) Principio de revisión periódica: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuarlas a la constante evolución de los riesgos y promover así una mejora continua.

q) Principio de exactitud: Los datos personales serán exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Artículo 6. Directrices de la Política de Seguridad de la Información y Protección de Datos.

Se adoptarán 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. La PSIPD se ejecutará aplicando las siguientes directrices:

a) Líneas de defensa: Los sistemas de información dispondrán de una estrategia de protección constituida por múltiples capas de seguridad.

b) Seguridad física: Los activos de información se emplazarán en áreas seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad. Los sistemas y los activos de información ubicados en dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

c) Controles de acceso: El acceso a la información estará debidamente controlado y limitado a las personas usuarias, procesos y dispositivos autorizados. A tal fin se implantarán los mecanismos de identificación y autenticación adecuados para cada activo.

d) Gestión de activos de información: Los activos de información se inventariarán y categorizarán. Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

e) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que, debidamente autorizada, acceda a los activos de información conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

f) Registro de actividad: La actividad realizada por las personas usuarias deberá ser registrada al objeto de verificar y auditar el buen uso de la información, siempre con plenas garantías a la intimidad y dignidad personal, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

   La monitorización deberá realizarse motivando su necesidad y aplicando el principio de proporcionalidad, eligiendo la medida menos invasiva.

g) Gestión de incidentes de seguridad: Los procedimientos de gestión permitirán identificar, registrar y dar una efectiva y pronta respuesta a los incidentes de seguridad.

h) Protección de las comunicaciones: La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, sin perjuicio de las actuaciones realizadas con fines de registro de actividad.

i) Especificaciones de seguridad: El desarrollo y mantenimiento de los sistemas de información irán acompañados de las especificaciones de seguridad y de los correspondientes procedimientos de control.

j) Adquisición de productos de seguridad de las tecnologías de la información y comunicaciones: Se optará, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, por aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

CAPÍTULO II

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

Artículo 7. Marco organizativo.

El marco organizativo para la gestión de la PSIPD está constituido por:

a) La consejería competente en materia de seguridad de la información, a través del centro directivo que tenga atribuida dicha materia.

b) La consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales, a través del centro directivo que tenga atribuida dicha materia.

c) El Comité de Seguridad de la Información.

d) Los responsables de la información.

e) Los responsables del tratamiento.

f) Los encargados del tratamiento.

g) Los responsables del servicio.

h) Los responsables de la seguridad.

i) Los responsables del sistema.

j) Los delegados de protección de datos.

Artículo 8. La consejería competente en materia de seguridad de la información.

Corresponde a la consejería competente en materia de seguridad de la información, a través del centro directivo que tenga atribuida dicha materia, el ejercicio de las facultades relativas a la seguridad de la información y de los datos personales que le atribuye la normativa reguladora de su estructura orgánica.

Artículo 9. La consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales.

Corresponde a la consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales, a través del centro directivo que tenga atribuida dicha materia, el ejercicio de las facultades relativas al cumplimiento y desarrollo normativo en materia de protección de datos personales que le atribuye la normativa reguladora de su estructura orgánica.

Artículo 10. El Comité de Seguridad de la Información.

1. El Comité de Seguridad de la Información (en adelante, CSI) es el órgano colegiado de impulso, seguimiento y coordinación interna en esta materia en el ámbito de la Administración de la Comunidad de Castilla y León.

2. El CSI está adscrito a la consejería competente en materia de seguridad de la información.

3. El CSI actuará en el ámbito del cumplimiento de las medidas a las que se refiere el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, de 5 de diciembre y su normativa de desarrollo, así como el Real Decreto 3/2010, de 8 de enero.

4. Al CSI le corresponden las siguientes funciones:

a) Promover la divulgación de la PSIPD.

b) Velar por la disponibilidad de los recursos necesarios para el desarrollo de la PSIPD.

c) Coordinar la actividad de las diferentes consejerías, organismos, entidades, y unidades administrativas de la Administración de la Comunidad de Castilla y León en materia de seguridad de la información.

d) Coordinar la actividad de los diferentes responsables a los que se refiere el marco organizativo de la presente PSIPD, así como resolver los posibles conflictos que puedan surgir entre cualquiera de ellos, sin perjuicio de las atribuciones que corresponden a la consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales.

e) Promover la coordinación, cooperación y colaboración con otras Administraciones Públicas en materia de seguridad de la información y protección de datos personales.

f) Informar las normas de seguridad a las que se hace referencia en el artículo 19.2.

g) Aprobar el plan de formación y concienciación en materia de seguridad de la información.

h) Aprobar el plan director de seguridad de la Administración de la Comunidad de Castilla y León.

i) Aprobar un informe anual de seguimiento de la PSIPD dentro del primer trimestre de cada año, referido al ejercicio anterior.

j) Impulsar el desarrollo y la revisión regular de la PSIPD.

k) Promover la mejora continua en la gestión de la seguridad de la información.

l) Adoptar los acuerdos necesarios para el desarrollo de los fines del presente decreto.

5. El CSI tendrá la siguiente composición:

a) Presidencia, que será ostentada por la persona titular de la secretaría general de la consejería con competencia en materia de seguridad de la información, y que contará con voto de calidad.

b) Vicepresidencia, que será ostentada por la persona titular del centro directivo con competencia en materia de seguridad de la información, quien ejercerá la presidencia en caso de vacante, ausencia o enfermedad.

c) La persona que ocupe la jefatura del servicio competente en materia de seguridad de la información.

d) La persona que ocupe la jefatura del servicio competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales.

e) Vocalías: Los responsables de la seguridad.

Un representante del grupo de trabajo de delegados de protección de datos, designado por este, participará, con voz pero sin voto, en las reuniones en que vayan a ser tratadas cuestiones relacionadas con la protección de datos personales o cuando se requiera.

6. Ejercerá la secretaría del CSI, con voz pero sin voto, un empleado público designado por quien ostente la presidencia.

7. La organización y funcionamiento del CSI se acomodarán 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.

Las convocatorias de las sesiones del CSI se realizarán por medios electrónicos. El desarrollo de sus sesiones podrá realizarse de forma presencial o a distancia, conforme a lo señalado en el artículo 17 de la Ley 40/2015, de 1 de octubre.

Se reunirá, con carácter ordinario, con una frecuencia mínima de dos veces al año y, con carácter extraordinario, cuando lo decida la presidencia. Los grupos de trabajo previstos en los artículos 16 y 18 podrán solicitar la convocatoria.

Para la válida constitución del CSI se requerirá la asistencia de las personas que ostenten la presidencia y la secretaría, o en su caso, de quienes les suplan, y la de la mitad, al menos, de sus miembros.

A las reuniones del CSI podrá asistir personal técnico, cuando así lo decida la presidencia, bien por propia iniciativa o a petición de cualquier miembro del Comité.

8. El CSI 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 podrá constituir ponencias técnicas, de carácter temporal, para la mejor toma de decisiones.

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

1. La persona titular de cada centro directivo de las diferentes consejerías, organismos autónomos y entes públicos de derecho privado será el responsable de la información tratada en el ámbito de sus competencias.

2. Las personas titulares de los centros directivos serán asimismo responsables del tratamiento de datos personales, a los efectos previstos en el Reglamento (UE) 2016/679.

3. A los responsables de la información y del tratamiento de datos personales les corresponden las siguientes funciones dentro de su ámbito de competencia:

a) Velar por una adecuada gestión de la seguridad de la información.

b) Decidir sobre la finalidad, contenido y uso de la información.

c) Determinar las categorías, niveles y medidas de seguridad aplicables a los sistemas de información, dentro del marco establecido en los Anexos I y II del Real Decreto 3/2010, de 8 de enero.

d) Aprobar las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas. Entre ellas se incluirán las medidas necesarias para poder demostrar que el tratamiento es conforme a lo establecido en el Reglamento (UE) 2016/679.

e) Mantener y actualizar el registro de actividades de tratamiento de datos personales en el ámbito de sus competencias y comunicarlo al delegado de protección de datos.

f) Cumplir el deber de información, de acuerdo con el principio de transparencia y teniendo en cuenta los criterios que se establezcan.

g) Garantizar el cumplimiento del deber de confidencialidad y de las demás obligaciones relacionadas con los derechos de las personas interesadas en materia de protección de datos personales.

h) Realizar las evaluaciones de impacto de protección de datos preceptivas, cuando el tratamiento entrañe alto riesgo para los derechos y las libertades de las personas, con el asesoramiento del delegado de protección de datos y los responsables de la seguridad y de los sistemas.

i) Notificar las violaciones de la seguridad de los datos que pudieran producirse a la Agencia Española de Protección de Datos, según dispone la normativa aplicable.

j) Seleccionar, en su caso, encargados de tratamiento que ofrezcan garantías suficientes, transmitirles las obligaciones que les competen y verificar su cumplimiento.

k) Responder a los requerimientos que les envíe el delegado de protección de datos en relación con los tratamientos de datos que gestiona en su ámbito de actuación.

l) Cualquier otra que les atribuya la normativa básica aplicable en materia de seguridad de la información y protección de datos personales.

4. En los supuestos de competencias o procedimientos administrativos compartidos, será responsable del tratamiento la persona titular del centro directivo que decida 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.

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.

La persona titular del servicio o unidad administrativa equivalente que gestione cada procedimiento o actuación administrativa y en cuyo ámbito se lleve a cabo el tratamiento de la información, tendrá 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. Los responsables de la seguridad.

1. La persona titular de la secretaría general de cada consejería, o de los órganos equivalentes de cada organismo autónomo o ente público de derecho privado, designará un responsable de la seguridad jerárquicamente independiente del responsable del sistema.

El ámbito de actuación de cada responsable de la seguridad se limitará a los sistemas de información que sean competencia de la consejería, organismo autónomo o entidad de derecho privado a la que pertenezca.

2. A los responsables de la seguridad les corresponden las siguientes funciones:

a) Promover la seguridad de la información manejada.

b) Adoptar las decisiones necesarias para satisfacer los requisitos de seguridad definidos por los responsables de la información y los responsables del servicio, ejerciendo las funciones en materia de análisis y gestión de riesgos que le atribuyen el Anexo II del Real Decreto 3/2010, de 8 de enero, y el artículo 21.

c) Impulsar la elaboración de normas de seguridad de la información.

d) Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

e) Determinar los criterios de acceso de las personas a los sistemas de información.

f) Poner en conocimiento del delegado de protección de datos y del responsable de la información y del servicio las violaciones de seguridad que se produzcan.

g) Informar periódicamente al centro directivo competente en materia de seguridad de la información de la actividad desarrollada en su ámbito de actuación.

h) Proporcionar y validar la información requerida en su ámbito competencial, a efectos de elaborar el Informe del Estado de Seguridad a que hace referencia el Esquema Nacional de Seguridad.

i) Promover auditorías periódicas para verificar el grado de conformidad de los sistemas de información con las prescripciones del Esquema Nacional de Seguridad.

j) Adoptar medidas de mejora en la gestión de la seguridad de la información.

k) Validar los Procedimientos Operativos de Seguridad.

En el ejercicio de sus funciones el responsable de la seguridad 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; de los servicios técnicos de la propia consejería; del servicio de seguridad de la información, y de los servicios comunes de informática y comunicaciones de la Administración de la Comunidad.

Artículo 14. Los responsables del sistema.

1. En cada consejería, organismo autónomo o ente público de derecho privado habrá un responsable del sistema, que será la persona titular del servicio o unidad administrativa equivalente con competencias en materia de informática.

2. También serán responsables del sistema, en su propio ámbito de actuación, las personas titulares de los servicios o unidades administrativas competentes en materia de servicios corporativos de informática y de comunicaciones.

3. Los responsables del sistema tendrán las siguientes funciones:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información, en coordinación con los servicios o unidades administrativas competentes en materia de servicios corporativos de informática y de comunicaciones, de acuerdo con lo establecido en el Anexo II del Real Decreto 3/2010, de 8 de enero, y en el artículo 21 del presente decreto.

b) Informar al responsable de la seguridad sobre las anomalías observadas en la aplicación de las normas y procedimientos de seguridad.

c) Notificar incidentes de seguridad de la información.

d) Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecian deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por el responsable de la información, debe ser acordada con los responsables de los servicios afectados y con el responsable de la seguridad.

e) Monitorizar el estado de la seguridad del sistema, dando cuenta al responsable de la seguridad.

Artículo 15. Responsables delegados.

Los responsables de la información, los responsables del servicio y los responsables de la seguridad podrán designar 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 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 16. Grupos de trabajo.

1. Los responsables definidos en los artículos 11 a 14 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 17. Los delegados de protección de datos.

1. Existirá un delegado de protección de datos en cada una de las consejerías, así como en cada uno de los organismos autónomos y entes públicos de derecho privado.

No obstante, podrá designarse un único delegado de protección de datos para una consejería y para todas o alguna de las entidades institucionales que dependan o estén vinculadas a ella.

2. Los delegados de protección de datos serán designados por las personas titulares de las consejerías, u órganos equivalentes de las entidades institucionales, entre personas que reúnan la cualificación profesional exigida por el artículo 37.5 del Reglamento (UE) 2016/679, acreditada por los mecanismos establecidos en el artículo 35 de la Ley Orgánica 3/2018, de 5 de diciembre, y de conformidad con lo establecido en la normativa reguladora en materia de función pública a este respecto.

Las personas titulares de las secretarías generales de las consejerías u órganos equivalentes de las entidades institucionales comunicarán las designaciones, así como las modificaciones, a la Agencia Española de Protección de Datos, en el plazo de diez días desde que se produzcan, y al centro directivo competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales.

3. Los delegados de protección de datos llevarán 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 establezca la normativa estatal y de la Comunidad.

4. En el desempeño de sus funciones, los delegados de protección de datos tendrán 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.

Artículo 18. Grupo de trabajo de delegados de protección de datos.

1. Se crea el grupo de trabajo de delegados de protección de datos, que estará integrado por quienes ostenten esa condición en el ámbito de la Administración de la Comunidad de Castilla y León.

2. El grupo de trabajo contará con el apoyo de la consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales.

3. El grupo de trabajo realizará las siguientes actuaciones:

a) Formular recomendaciones para la adaptación de la normativa de la Comunidad en el ámbito de la protección de datos.

b) Realizar propuestas para normalizar y homogeneizar metodologías, criterios y documentos sobre protección de datos personales.

c) Coordinar actuaciones para facilitar la labor de supervisión que corresponde a los delegados de protección de datos en el cumplimiento del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018, de 5 de diciembre, así como de otras disposiciones en materia de protección de datos de carácter personal.

d) Proponer el diseño de la formación del personal a los responsables de tratamiento y a los órganos competentes en materia de formación.

4. A las reuniones del grupo de trabajo asistirá la persona que ostente la jefatura del servicio con competencias en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales.

CAPÍTULO III

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

Artículo 19. Instrumentos de desarrollo de la Política de Seguridad de la Información y Protección de Datos.

1. La PSIPD se desarrollará por medio de:

a) Normas de seguridad de la información.

b) Procedimientos generales de seguridad.

c) Procedimientos operativos de seguridad.

d) Guías técnicas de seguridad.

e) Otros instrumentos.

2. Las normas de seguridad, de obligado cumplimiento para todas las consejerías y organismos incluidos en el ámbito de aplicación de la presente Política de Seguridad de la Información y Protección de Datos, serán aprobadas por la persona titular de la consejería competente en materia de seguridad de la información, estableciéndose en ellas las directrices y principios generales aplicables a los siguientes aspectos de la seguridad de la información:

a) Gestión de la Política de Seguridad de la Información.

b) Organización de la seguridad y responsabilidades.

c) Seguridad ligada al personal.

d) Clasificación y control de activos.

e) Control de accesos y gestión de claves.

f) Seguridad física y del entorno.

g) Seguridad operacional.

h) Seguridad de las comunicaciones.

i) Adquisición, desarrollo y mantenimiento de sistemas.

j) Gestión de incidentes de seguridad.

k) Gestión de la continuidad del negocio.

l) 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 en el plazo de diez días desde su aprobación, salvo que por el nivel de confidencialidad o por la naturaleza de la información deba limitarse su difusión.

3. Los procedimientos generales de seguridad serán aprobados por la persona titular del centro directivo con competencia en materia de seguridad de la información, y en ellos se establecerán las metodologías, contenidos mínimos y responsables de la elaboración de los procedimientos operativos.

4. Los procedimientos operativos de seguridad, en los que se concretarán de forma detallada las acciones a desarrollar en un proceso crítico relacionado con la seguridad, serán aprobados por el órgano o unidad administrativa con competencias en la materia sobre la que se desarrolla el documento, previa validación del responsable de la seguridad previsto en el artículo 13.

5. Las guías técnicas de seguridad, de carácter meramente informativo, constituyen una ayuda a las personas usuarias para aplicar de forma correcta las medidas de seguridad. Su aprobación corresponde al responsable de la seguridad.

6. Forman parte de los instrumentos de desarrollo de la PSIPD los acuerdos adoptados por el CSI.

Así mismo, los órganos y unidades administrativas a las que resulta de aplicación la presente PSIPD, en el ámbito de sus respectivas competencias y responsabilidades, podrán elaborar otros documentos tales como informes técnicos, instrucciones, registros, evidencias, etc.

Artículo 20. Gestión de documentos relativos a la Política de Seguridad de la Información y Protección de Datos.

Corresponde a la consejería competente en materia de seguridad de la información la gestión documental de las normas, procedimientos generales, procedimientos operativos y guías técnicas de seguridad, definiendo su estructura, categorización, trazabilidad y requisitos de acceso, sin perjuicio de las facultades atribuidas al CSI.

CAPÍTULO IV

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

Artículo 21. Gestión de riesgos.

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 3/2010, de 8 de enero.

2. Cuando la información contenga datos de carácter personal 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. Este análisis deberá realizarse de forma periódica y en todo caso una vez cada dos años.

3. Para cada tipo de riesgo se utilizarán las metodologías de análisis y gestión de riesgos que resulten más apropiadas.

4. Los 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.

5. Corresponde al responsable de la seguridad la selección de las medidas de seguridad a aplicar.

6. 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, el responsable del tratamiento deberá realizar antes del mismo una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales.

El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos al realizar la evaluación de impacto relativa a la protección de datos.

7. El responsable de la seguridad y el responsable del sistema de cada consejería aprobarán conjuntamente un plan de gestión de riesgos para su ámbito de competencia, en coordinación con los servicios corporativos de informática y de comunicaciones.

Artículo 22. Uso de medios digitales.

1. Los medios digitales puestos a disposición del personal empleado público se destinarán exclusivamente al cumplimento de sus obligaciones laborales o estatutarias.

2. Respetando el derecho a la intimidad de los trabajadores, la protección de los datos personales y el secreto de las comunicaciones, la Administración de la Comunidad podrá acceder a los contenidos de los medios digitales de titularidad pública, incluidas las comunicaciones que estén cifradas, para garantizar la integridad 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 a la información deben ser idóneas, necesarias y proporcionales.

Artículo 23. 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 el responsable de la seguridad de la información y por el delegado de protección de datos.

Artículo 24. Notificaciones de violaciones de seguridad de los datos personales.

La consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales adoptará las medidas necesarias para garantizar que los responsables de tratamiento realicen la notificación a la Agencia Española de Protección de Datos de las violaciones de seguridad de los datos de carácter personal, de conformidad con el procedimiento previsto en el artículo 33 del Reglamento (UE) 2016/679.

Así mismo, será la encargada de adoptar las medidas pertinentes para que los responsables de tratamiento notifiquen a los interesados afectados las violaciones de seguridad de los datos de carácter personal, de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679.

Artículo 25. Registro de las actividades de tratamiento.

1. La consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales establecerá los criterios para la elaboración del registro de las actividades de tratamiento de datos de carácter personal, una vez oídas las recomendaciones efectuadas por el grupo de trabajo de delegados de protección de datos.

2. El responsable del tratamiento en el ámbito de sus competencias llevará y mantendrá actualizado el registro de actividades de tratamiento de datos de carácter personal, 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.

El 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 Administración de la Comunidad de Castilla y León hará público un inventario de sus actividades de tratamiento accesible a través del Portal de Gobierno Abierto. Para ello, cada responsable de tratamiento comunicará, a través de las personas titulares de las secretarías generales u órganos equivalentes, al centro directivo competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos, la información necesaria para su formación, en el modelo que este establezca.

Artículo 26. Formación y concienciación.

Se desarrollarán actividades formativas específicas orientadas a la formación y concienciación del personal empleado público en materia de seguridad de la información y protección de datos personales, que tendrán en cuenta los planes y recomendaciones propuestos por el CSI y el grupo de trabajo de delegados de protección de datos.

La Escuela de Administración Pública de Castilla y León, a propuesta de las consejerías competentes en materia de seguridad de la información y de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales, incluirá en sus planes acciones formativas relativas a dichas materias, de acuerdo con las disponibilidades presupuestarias y conforme a la programación y planificación de la Escuela.

Artículo 27. Obligaciones del personal.

1. El personal de la Administración de la Comunidad deberá colaborar en la implementación de la PSIPD y cumplir lo previsto en los instrumentos que la desarrollan.

2. Dicho personal cumplirá las obligaciones establecidas en la normativa de protección de datos personales y en particular las siguientes:

a) Acceder a los datos personales solo cuando tenga autorización, en virtud de las funciones o tareas asignadas, y guardar el deber de confidencialidad.

b) Utilizar los datos únicamente para los fines para los cuales han sido recabados.

c) No divulgar las contraseñas de acceso a los sistemas y aplicaciones informáticas que contengan datos de carácter personal, y custodiar con diligencia los documentos en soporte papel que los contengan.

d) Solicitar las autorizaciones o realizar las consultas necesarias para grabar en dispositivos portátiles o tratar fuera de las dependencias administrativas datos de carácter personal.

e) No utilizar con fines distintos a los propios del servicio los medios digitales puestos a su disposición.

DISPOSICIONES ADICIONALES

Primera. Constitución del Comité de Seguridad de la Información.

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

Segunda. Designaciones.

1. Los responsables de la 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.

2. En el mismo plazo cada consejería remitirá al centro directivo competente en materia de seguridad de la información una relación de responsables de la información, del servicio y del sistema.

Tercera. No incremento del gasto público.

La aplicación de las previsiones contenidas en este decreto no supondrá incremento del gasto público, al ser atendidas con los medios materiales y humanos personales de que dispone la Administración de la Comunidad.

Cuarta. Plan de formación y concienciación y planes de gestión de riesgos.

Los planes a los que se refieren la letra g) del artículo 10.4 y el artículo 21.7 deberán aprobarse en el plazo de nueve meses a contar desde el día siguiente a la entrada en vigor de este decreto.

Quinta. Formularios para el ejercicio de derechos.

En el plazo de tres meses desde la entrada en vigor de este decreto, el centro directivo con competencias en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales pondrá a disposición de los ciudadanos en la sede electrónica el formulario o formularios de tramitación electrónica oportunos para el ejercicio de los derechos de protección de datos que les corresponden.

Sexta. Política de seguridad de la información del Organismo Pagador de la Comunidad de Castilla y León.

1. La Consejería de Agricultura, Ganadería y Desarrollo Rural como Organismo Pagador de la Comunidad de Castilla y León, designada por el Decreto 86/2006, de 7 de diciembre, dispondrá de una organización de la seguridad de los sistemas de información y una política de seguridad de la información propias, pero imbricadas y coordinadas en todo momento con la PSIPD, en aplicación de las disposiciones comunitarias que afectan al Organismo Pagador en lo que se refiere a la autorización de los organismos pagadores y otros órganos y la liquidación de cuentas del FEAGA y del FEADER.

2. El desarrollo y las modificaciones posteriores en materia de política de seguridad que afecten al Organismo Pagador serán realizadas por el director de este organismo, conforme a las competencias que le confiere la normativa citada anteriormente. No obstante, esta política de seguridad de la información y sus modificaciones serán previamente comunicadas por el Organismo Pagador al centro directivo competente en materia de seguridad de la información, que emitirá informe previo.

Séptima. Política de seguridad de la información y protección de datos de la Gerencia Regional de Salud de Castilla y León.

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, en el plazo de seis meses a contar desde el día siguiente a la entrada en vigor del presente decreto, su propia política de seguridad de la información y protección de datos, conforme a los principios y requisitos mínimos recogidos en este decreto.

En todo caso, resultará de aplicación a la Gerencia Regional de Salud el Capítulo II del presente decreto.

Octava. No discriminación por razón de género.

En aquellos casos en los que en este decreto se utilizan sustantivos de género masculino para referirse a personas, debe entenderse que se emplean de forma genérica con independencia del sexo de las personas mencionadas, con estricta igualdad a todos los efectos.

DISPOSICIÓN TRANSITORIA

Aplicación de la presente Política de Seguridad de la Información y Protección de Datos a la Gerencia Regional de Salud.

Este decreto resultará de aplicación a la Gerencia Regional de Salud de Castilla y León entre la fecha de su entrada en vigor y la de su propia política de seguridad de la información y protección de datos, conforme a lo señalado en la disposición adicional séptima.

DISPOSICIÓN DEROGATORIA

Derogación normativa.

Quedan derogadas todas las disposiciones de igual o inferior rango que se opongan a este decreto y, en concreto las siguientes normas:

– El Decreto 11/2003, de 23 de enero, por el que se regulan los ficheros de datos de carácter personal susceptibles de tratamiento automatizado, de la Administración de la Comunidad de Castilla y León.

– La Orden HAC/858/2014, de 30 de septiembre, por la que se aprueba la política de seguridad de la información de la Administración de la Comunidad de Castilla y León.

DISPOSICIONES FINALES

Primera. Habilitación normativa.

Se autoriza a las personas titulares de la consejería competente en materia de seguridad de la información y de la consejería competente en materia de coordinación y seguimiento del cumplimiento de la normativa de protección de datos personales a dictar cuantas disposiciones sean precisas para el desarrollo y aplicación del presente decreto.

Segunda. Entrada en vigor.

El presente decreto entrará en vigor a los veinte días de su publicación en el Boletín Oficial de Castilla y León.

Valladolid, 30 de septiembre de 2021.

El Presidente de la Junta
de Castilla y León,
Fdo.: Alfonso Fernández Mañueco

El Consejero
de Economía y Hacienda,
Fdo.: Carlos Fernández Carriedo

CV: BOCYL-D-04102021-1