Versión 1ª (19 de diciembre de 2022)

PROYECTO DE DECRETO XX/2023, de XX, del Gobierno de Aragón, por el que se aprueban las Políticas de Protección de Datos Personales y de Seguridad de la Información de la Administración pública de la Comunidad Autónoma de Aragón.

ÍNDICE

Artículo 39. Funcionamiento del pleno y de las subcomisiones.
Artículo 40. Medios.
Disposición adicional primera. Definiciones técnicas y su actualización.
Disposición adicional segunda. Régimen jurídico de los comités y grupos de trabajo.
Disposición derogatoria única. Derogación normativa.
Disposición final primera. Habilitación de desarrollo.
Disposición final segunda. Entrada en vigor.
ANEXO Definiciones técnicas

Conforme al artículo 71. 1ª del Estatuto de Autonomía de Aragón, corresponde a la Comunidad Autónoma de Aragón, en los términos expuestos en dicho precepto, la competencia exclusiva en materia de autoorganización. Asimismo, de acuerdo con el artículo 75 del Estatuto de Autonomía de Aragón, le corresponde, en los términos expuestos en dicho precepto, las competencias compartidas en materia de protección de datos de carácter personal (5ª), así como sobre el régimen jurídico de la Administración Pública de la Comunidad Autónoma (12ª).

La Administración de la Comunidad Autónoma de Aragón ha ido creando una organización para la aplicación de las Políticas de Protección de Datos Personales y de Seguridad de la Información, así hay que hacer referencia al Acuerdo de 24 de julio de 2018, del Gobierno de Aragón, por el que se adoptan medidas organizativas en materia de administración electrónica, protección de datos de carácter personal y seguridad de la información, aplicables a la Administración de la Comunidad Autónoma de Aragón. En el mismo, se crean la Unidad de Protección de Datos y la Unidad del responsable de la Seguridad de la Información (CISO), así como las Unidades de Apoyo a la Administración Electrónica y Gobernanza de los datos, para cada Departamento y organismo autónomo.

Con posterioridad, el artículo 45 de la Ley 5/2021, de 29 de junio, de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón, dispone que la Comunidad Autónoma de Aragón establecerá una Política de Protección de Datos y una Política de Seguridad de la Información que especifique los principios rectores, obligaciones, organización y responsabilidades que deberán contemplar los organismos y entidades de la Administración pública de la Comunidad Autónoma de Aragón, que se aprobarán por decreto del Gobierno de Aragón y serán de aplicación directa a dicha Administración, pudiendo ser adaptada la Política de Seguridad de la Información por los diferentes Departamentos y organismos públicos de forma motivada y atendiendo, en todo caso, al cumplimiento del Esquema Nacional de Seguridad.

Mediante el Decreto de 5 de agosto de 2019, del Presidente del Gobierno de Aragón, se modificó la organización de la Administración de la Comunidad Autónoma de Aragón y se asignaron competencias a los Departamentos, creándose el Departamento de Ciencia, Universidad y Sociedad del Conocimiento, al que se le atribuyeron la totalidad de las competencias del anterior Departamento de Innovación, Investigación y Universidad. Al amparo de este decreto, se dictó el Decreto 7/2020, de 10 de febrero, por el que se aprueba la estructura orgánica del Departamento de Ciencia, Universidad y Sociedad del Conocimiento. En dicho decreto, en su artículo 1.2, se le atribuye el ejercicio de la competencia en materia de protección de datos personales. Asimismo, es el competente para el desarrollo, en materia de seguridad de la información, de las actuaciones necesarias para garantizar la adecuada protección de los bienes y tecnologías de la información en la Administración pública de la Comunidad Autónoma de Aragón, definiendo la política de seguridad de la información de la misma.

La actuación de las Administraciones Públicas, en el ejercicio de sus competencias, se asienta sobre los datos personales que trata y sobre el conjunto de la información de la que dispone. Los medios electrónicos que permiten el tratamiento y almacenamiento de esos datos se denominan sistemas de información. La forma en la que las Administraciones traten y consideren los datos personales, los conjuntos de datos de los que disponen y sus sistemas de información, va a determinar la mejora del servicio que éstas presten a la ciudadanía.

Asimismo, en el marco de una Administración pública orientada a los derechos e intereses de la ciudadanía, se debe hacer especial incidencia en los derechos de acceso a la información, transparencia y reutilización de la información del sector público. Todos estos derechos son dimensiones de un mismo modelo de Administración, que tiene, al mismo tiempo, que velar por el derecho a la intimidad de la ciudadanía.

Las normativas en materia de protección de datos personales y en materia de seguridad de la información no son mundos aislados. Ambas versan sobre datos e información; datos que maneja la Administración, su tratamiento y la forma en la que la información y los sistemas en los que se integra, y sobre la que se asienta la actuación administrativa, es tratada por cada órgano administrativo. Se trata de diferentes perspectivas sobre un mismo objeto.

La protección de los datos personales se configura como un derecho fundamental de la persona y, desde esa dimensión, deben de valorarse los riesgos que pueden derivarse para la misma a la hora de tratar sus datos.

Pero esos datos personales se encuentran incluidos en sistemas de información, que también deben ser analizados y evaluados desde la perspectiva del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que

comprende el conjunto de criterios y obligaciones a aplicar en materia de seguridad, conservación y normalización de la información.

Asimismo, en el artículo 3.2 de la Ley 40/2015, de 1 de octubre, se afirma que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y las soluciones adoptadas por cada una de ellas, garantizando la protección de los datos de carácter personal, y facilitando, preferentemente, la prestación conjunta de servicios a las personas interesadas.

En ese contexto también hay que destacar que, el citado artículo 45.3 de la Ley 5/2021, de 29 de junio, determina que la preservación de la seguridad en la utilización de medios electrónicos será considerada objetivo común de todas las personas al servicio de la Administración pública de la Comunidad Autónoma de Aragón, siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

Así, el punto de inicio del que se derivan ambas políticas es la responsabilidad de las personas titulares de los órganos y entes administrativos sobre el tratamiento de los datos personales, sobre la información que sirve de base para la actuación administrativa y sobre los sistemas de información que la integran. Y sobre esta idea de responsabilidad se estructuran las Políticas de Protección de Datos Personales y de Seguridad de la Información.

Las interrelaciones entre dichas materias motivan que sea una única norma reglamentaria la que apruebe ambas.

Este decreto se estructura en cinco capítulos, 40 artículos, dos disposiciones adicionales, una disposición derogatoria y dos finales, así como un anexo.

El capítulo I establece las disposiciones generales que afectarán a las citadas políticas, determinando así el objeto de la norma y el ámbito de aplicación de la misma a la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos, si bien los principios rectores y objetivos de dichas políticas también serán de aplicación al resto de la Administración pública de la Comunidad Autónoma de Aragón, conforme a lo dispuesto en el artículo 45 de la Ley 5/2021, de 29 de junio.

Asimismo, en este capítulo se enumeran una serie de objetivos comunes a ambas políticas.

El capítulo II es el relativo a la Política de Protección de Datos Personales, cuyo objeto es regular aspectos derivados de las novedades introducidas por el nuevo marco jurídico, propios de los cambios sociales y tecnológicos que se han producido en nuestra sociedad.

La protección de las personas físicas, en relación con el tratamiento de datos personales, es un derecho fundamental garantizado en el artículo 18.4 de la Constitución Española. Por ello, el actual régimen legal previsto, tanto en 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, tiene como objetivo la protección de los derechos y libertades de las personas físicas.

En primer lugar, tal como señala el artículo 24 del Reglamento general de protección de datos, una de las principales obligaciones del responsable del tratamiento de datos personales es poder demostrar que el tratamiento es conforme a lo dispuesto en el mismo. Para ello, debe aplicar medidas técnicas y organizativas apropiadas a fin de garantizarlo. Entre dichas medidas se incluirá, cuando sea proporcional al tratamiento, la aplicación de las oportunas políticas de protección de datos. A este respecto, el capítulo II se inicia con la enumeración de los principios rectores bajo los que debe desarrollarse la Política de Protección de Datos de la Administración pública de la Comunidad Autónoma de Aragón, tales como el principio de minimización de datos, el de responsabilidad proactiva o los de protección de datos por defecto y desde el diseño.

En consonancia con dichos principios, los derechos en materia de protección de datos, regulados en los artículos 15 a 22 del Reglamento general de protección de datos, se amplían y adaptan a la realidad social del tiempo en que deben ser ejercidos.

En relación con el ejercicio de estos derechos, el presente decreto concreta determinadas reglas referidas a la tramitación de las solicitudes que presenten las personas afectadas, en el ámbito de la Administración autonómica y sus organismos autónomos, en los términos en él previstos.

Otra de las principales novedades del Reglamento general de protección de datos es la desaparición de los ficheros de datos de carácter personal. En su lugar, el artículo 30 de dicha norma comunitaria, determina la obligación de los responsables del tratamiento de llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, en el que debe recogerse diversa información como las bases de legitimación y las finalidades del tratamiento, las categorías de los datos personales tratados o las cesiones que, en su caso, se realicen. Conforme a este nuevo contexto, el decreto dedica un artículo al Registro de actividades de tratamiento definiendo su alcance y carácter público.

Asimismo, se debe destacar la creación de la figura del Delegado o Delegada de Protección de Datos, regulada en los artículos 37 a 39 del Reglamento general de protección de datos. Sus funciones son las de informar y asesorar al responsable del tratamiento y supervisar el cumplimiento de lo dispuesto en la normativa en materia de protección de datos personales. Así, su naturaleza jurídica se incardina dentro del modelo de “compliance officer” como agente responsable del cumplimiento normativo. Entre las entidades que, conforme al Reglamento general de protección de datos, tienen la obligación de designar Delegado o Delegada de Protección de Datos Personales, se encuentran las autoridades u organismos públicos. De acuerdo con lo expuesto, entre las medidas organizativas que se determinan en el capítulo II, destaca la regulación relativa a la designación, en el ámbito de la Administración de la Comunidad Autónoma de Aragón y sus organismos autónomos, de la Unidad de Protección de Datos del Gobierno de Aragón y de las Unidades de Apoyo a la Administración Electrónica y Gobernanza de Datos, conforme a los criterios que se determinan en este capítulo.

Asimismo, se regulan otras cuestiones como la exigencia de evaluaciones de impacto en materia de protección de datos y el análisis de los riesgos que puedan afectar a los derechos y libertades de la ciudadanía.

El capítulo III de este decreto es el relativo a la Política de Seguridad de la Información, que tiene como uno de sus antecedentes normativos la Ley 40/2015, de 1 de octubre, que define, en su artículo 156, el Esquema Nacional de Seguridad, con objeto de establecer unos requerimientos de seguridad en la utilización de medios electrónicos en el ámbito de las Administraciones Públicas. Éste ya fue regulado por del Real Decreto 3/2010, de 8 de enero, que definía los principios básicos y requisitos mínimos que garantizaran adecuadamente la seguridad de la información. Dicha norma ha sido derogada por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que viene a facilitar una mejor respuesta a las tendencias en ciberseguridad, con el objeto de reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad de la información

El Real Decreto 311/2022, de 3 de mayo, en su artículo 12.2, establece que cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente. No obstante, la totalidad o una parte de los sujetos de un sector público institucional, podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando

así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

Para dar cumplimiento a este mandato, el capítulo III de este decreto establece la Política de Seguridad de la Información, con base en los principios básicos recogidos en el capítulo II del referido real decreto, y desarrolla los requisitos establecidos en su artículo 12.1.

Este capítulo contiene una regulación común en materia de seguridad de la información dividida en dos secciones.

En la sección primera se determinan los principios y requisitos que serán de aplicación para el aseguramiento de los datos, información y servicios utilizados en medios electrónicos, gestionados por la Administración pública de la Comunidad Autónoma de Aragón en el ejercicio de sus competencias, con el objeto de proteger su acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación.

Por su parte, en la sección segunda, se establecen las responsabilidades, la organización y la gestión para la gobernanza de la seguridad de la información que será de aplicación en el ámbito de los Departamentos y organismos públicos de la Administración de la Comunidad Autónoma de Aragón.

En sus disposiciones se concretan las responsabilidades exigidas por el Esquema Nacional de Seguridad y su adaptación a la realidad de los Departamentos y organismos públicos de la Administración de la Comunidad Autónoma de Aragón. En particular, se asignan las responsabilidades sobre la información y los servicios a los órganos directivos o de dirección, de los citados Departamentos y organismos, sobre los sistemas de información bajo su competencia. También se regula la designación de una persona responsable de seguridad dentro de cada Departamento y organismo público.

Igualmente, se identifica a la entidad Aragonesa de Servicios Telemáticos como responsable genérica de sistema.

Para dar coherencia a las actuaciones entre ellos, se crea un Comité de Seguridad de la Información en cada Departamento y organismo público, como herramienta de supervisión e impulso de la ciberseguridad en cada ámbito.

Todo ello se ve complementado con la regulación de la Comisión Interdepartamental de Servicios Digitales- prevista en el capítulo V- como el máximo órgano encargado de velar por el efectivo cumplimiento de la Política de Seguridad de la Información, a través de su Subcomisión de Seguridad de la Información. En todo caso, las actuaciones en materia de seguridad deben realizarse de manera global y coordinada entre todos los Departamentos y organismos públicos.

Complementariamente se regula la Unidad del responsable de la Seguridad de la Información (CISO), encargada de velar y apoyar el desarrollo de la seguridad de la información de manera transversal.

Para la gestión efectiva de las medidas de seguridad se define un Cuerpo Normativo de Seguridad de la Información, que se estructura jerárquicamente en un primer nivel compuesto por la propia Política de Seguridad de la Información —aprobada en este decreto—, un segundo nivel de Normas Técnicas de Seguridad de la Información y un tercer nivel que las desarrolla. El segundo nivel normativo será aprobado por la Comisión Interdepartamental de Servicios Digitales, en aras de permitir que, cada Departamento y organismo público, establezca las normas técnicas de seguridad que deben de regir sus actividades realizadas por medios electrónicos. El tercer nivel será elaborado por la Unidad del responsable de la Seguridad de la Información (CISO) y la entidad pública Aragonesa de Servicios Telemáticos.

De esta forma, el decreto configura un Cuerpo Normativo de Seguridad de la Información que establece las garantías de seguridad generales para todos los Departamentos y organismos públicos de la Administración aragonesa. Complementariamente, se prevé la posibilidad de que órganos superiores o directivos puedan aprobar disposiciones propias con regulaciones específicas para realizar una protección de la información y los servicios digitales más efectiva en el ámbito de sus competencias, siempre que no contravengan el cuerpo común.

El Capítulo IV se dedica a cuestiones comunes a ambas políticas, tales como la formación, la regulación de las auditorías, así como las obligaciones comunes para los órganos y el personal de la Administración pública de la Comunidad Autónoma de Aragón.

Finalmente, el Capítulo V aborda como una medida organizativa de estas políticas, la nueva regulación, conforme a las actuales exigencias normativas, de la Comisión Interdepartamental de Servicios Digitales, así como la de sus diferentes subcomisiones, que tiene su origen en el Decreto 28/2011, de 22 de febrero, del Gobierno de Aragón, por el que se crea y se regula la Comisión interdepartamental de Administración electrónica, el cual queda derogado conforme a la disposición derogatoria única de este decreto.

Por último, hay que destacar que, en la parte final, además de la citada disposición derogatoria y de las disposiciones finales referidas a la habilitación para el desarrollo de este decreto y su entrada en vigor, se recogen dos disposiciones adicionales en las que, respectivamente, se prevé la actualización automática de aquellas definiciones recogidas en el anexo de este decreto que provienen de otras normas y la posi-

bilidad de que los grupos de trabajo para la protección de datos personales y los Comités de seguridad de la información, previstos en los capítulos II y III, puedan aprobar las reglas de régimen interno para un mejor funcionamiento, como meros escenarios de encuentro, sin que puedan ser considerados órganos colegiados.

En la aprobación de este decreto se ha actuado de acuerdo con los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, en los términos previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Publicas y en el artículo 49 del Decreto Legislativo 1/2022, de 6 de abril, del Gobierno de Aragón, por el que se aprueba el texto refundido de la Ley del Presidente o Presidenta y del Gobierno de Aragón.

De manera específica, los principios de necesidad y eficacia aparecen justificados por la exigencia de elaborar las Políticas de Protección de Datos y de Seguridad de la Información de la Administración pública de la Comunidad Autónoma de Aragón. La proporcionalidad y eficiencia de la norma se ve garantizada por la adecuación de los medios existentes a las funciones encomendadas. Por último, en su elaboración se ha atendido a los trámites exigidos legalmente, así como dado audiencia a los interesados con lo que se ha dado cumplimiento a los principios de seguridad jurídica y transparencia.

En el procedimiento de elaboración del proyecto se ha cumplido con la obligación de publicidad de la información de relevancia jurídica exigida en el artículo 15 de la Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón, a través del Portal de Transparencia del Gobierno de Aragón.

Para la elaboración y aprobación de esta norma se ha dado cumplimiento a los trámites previstos en el ordenamiento jurídico y, en especial, en el Decreto Legislativo 1/2022, de 6 de abril, del Gobierno de Aragón, por el que se aprueba el texto refundido de la Ley del Presidente o Presidenta y del Gobierno de Aragón, habiéndose realizado audiencias de los Departamentos y organismos públicos y otros informes preceptivos. Asimismo, se han emitido los preceptivos informes de evaluación de impacto de género, de la Secretaría General Técnica del Departamento de Ciencia, Universidad y Sociedad del Conocimiento y de la Dirección General de Servicios Jurídicos.

En su virtud, a iniciativa de la Consejera de Ciencia, Universidad y Sociedad del Conocimiento, de acuerdo con/ visto el dictamen del Consejo Consultivo de Aragón de fecha de …., y previa deliberación del Gobierno de Aragón en su reunión de XXXX de XXXX de XXXXX,

DISPONGO

CAPÍTULO I
Disposiciones generales

Artículo 1. *Objeto.*

1. Este decreto tiene por objeto aprobar la Política de Protección de Datos Personales y la Política de Seguridad de la Información de la Administración pública de la Comunidad Autónoma de Aragón.

2. Las Políticas de Protección de Datos Personales y de Seguridad de la Información se definen, en el marco del ordenamiento jurídico estatal y de la Unión Europea, como el conjunto de principios rectores, obligaciones, organización y responsabilidades que deben adoptarse, en los términos previstos en este decreto, por la Administración pública de la Comunidad Autónoma de Aragón, para dar cumplimiento a la normativa de protección de datos personales y de seguridad de la información.

Artículo 2. *Ámbito subjetivo.*

1. Las Políticas de Protección de Datos Personales y de Seguridad de la Información serán de aplicación a la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos en los términos previstos en este decreto.

2. La Política de Seguridad de la Información será de aplicación a los datos, información y servicios utilizados por medios electrónicos por la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos.

Esta podrá ser adaptada por los diferentes Departamentos y organismos públicos de forma motivada y atendiendo, en todo caso, al cumplimiento del Esquema Nacional de Seguridad.

3. Los principios rectores y objetivos de las Políticas de Protección de Datos Personales y de Seguridad de la Información serán también de aplicación al resto de organismos y entidades de la Administración pública de la Comunidad Autónoma de Aragón.

Artículo 3. *Responsabilidad sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad.*

En los Departamentos y organismos públicos de la Administración de la Comunidad Autónoma y, dentro del ejercicio de sus competencias, las personas titulares de los órganos directivos y los órganos de dirección tendrán la condición de responsables de sus respectivas actividades de tratamiento de datos personales debiendo determinar los medios y fines de las mismas.

Asimismo, serán responsables de la aplicación de las medidas de seguridad sobre sus sistemas de información y de la integridad y exactitud de los datos sobre los que se adopten decisiones administrativas, sean automatizadas o no.

Artículo 4. *Objetivos comunes.*

Las Políticas de Protección de Datos Personales y de Seguridad de la Información tienen los siguientes objetivos:

a) Establecer las bases de un modelo integral de gestión de la información que comprenda la protección de datos personales y la seguridad de la información de la Administración pública de la Comunidad Autónoma de Aragón, en un ciclo continuo de mejora de los aspectos técnicos, organizativos y procedimentales, con la finalidad de establecer un marco orientado a garantizar los derechos de acceso a la información, transparencia y reutilización de la información.
b) Garantizar a la ciudadanía que sus datos personales serán tratados por la Administración pública de la Comunidad Autónoma de Aragón conforme a la normativa en materia de protección de datos personales, así como a los estándares y buenas prácticas en seguridad de la información, contribuyendo a la mejora de los servicios públicos ofrecidos y su coordinación con el resto de políticas complementarias, en particular las de reutilización de la información, datos abiertos y transparencia.
c) Aumentar el nivel de concienciación en materia de protección de datos personales y seguridad de la información en todo el personal de la Administración pública de la Comunidad Autónoma de Aragón.
d) Asegurar a la ciudadanía el ejercicio de sus derechos en materia de protección de datos personales ante los órganos, organismos y entidades de la Administración pública de la Comunidad Autónoma de Aragón.
e) Velar por la efectiva protección de los datos personales y la seguridad de la información en la prestación conjunta de servicios a las personas interesadas y en cualquiera de las trasmisiones de datos entre administraciones públicas**.**

CAPITULO II
Política de Protección de Datos Personales

SECCION 1ª. PRINCIPIOS RECTORES

Artículo 5. *Principios rectores de la Política de Protección de Datos Personales.*

La Política de Protección de Datos Personales se desarrollará, con carácter general, de acuerdo a los siguientes principios rectores, que serán de aplicación a la Administración pública de la Comunidad Autónoma de Aragón:

a) Licitud, lealtad y transparencia: los datos personales serán tratados de manera lícita, leal y transparente en relación con la persona interesada.
b) Legitimación en el tratamiento de datos personales: solo se tratarán los datos personales cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del Reglamento general de protección de datos.
c) Limitación de la finalidad: los datos personales serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
d) Minimización de datos: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
e) 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.
f) Limitación del plazo de conservación: los datos personales serán mantenidos de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines que justificaron su tratamiento.
g) Integridad y confidencialidad: los datos personales serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto, incluso después de haber concluido la relación que justificaba su intervención.

h) Responsabilidad proactiva: Los responsables del tratamiento de datos personales serán responsables del cumplimiento de los principios anteriormente señalados y los posteriores y adoptarán las medidas técnicas y organizativas que les permitan estar en condiciones de demostrar dicho cumplimiento.
i) Atención de los derechos de las personas afectadas: se adoptarán las medidas en la organización que garanticen el adecuado ejercicio por las personas afectadas, cuando proceda, de los derechos reconocidos en los artículos 15 al 22 del Reglamento general de protección de datos.
j) Protección de datos por defecto: Los responsables del tratamiento de datos personales promoverán que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen la protección de datos por defecto, en especial en lo que hace referencia a la minimización de los datos y del acceso a la información.
k) Protección de datos desde el diseño: Los responsables del tratamiento de datos personales promoverán la implantación del principio de protección de datos desde el diseño, con el objetivo de cumplir los requisitos definidos en el Reglamento general de protección de datos y garantizar los derechos de las personas interesadas, de forma que la protección de datos se encuentre presente desde las primeras fases de concepción de un proyecto.
l) Llevanza actualizada del Registro de las actividades de tratamiento: se mantendrá un registro público de las actividades de tratamiento, en los términos previstos en el artículo 14 de este decreto.

SECCION 2ª. MEDIDAS ORGANIZATIVAS

Artículo 6. *Los responsables del tratamiento de datos personales.*

1. En los Departamentos y organismos autónomos de la Administración pública de la Comunidad Autónoma, dentro del ejercicio de sus competencias, las personas titulares de los órganos directivos o de dirección, ejercerán las funciones de responsables del tratamiento en lo que se refiere a sus respectivas actividades de tratamiento de datos personales debiendo determinar los medios y fines de las mismas.

2. Son funciones del responsable del tratamiento las que le correspondan, en su ámbito de competencia, conforme al Reglamento general de protección de datos y a la Ley Orgánica 3/2018, de 5 de diciembre, y en particular las siguientes:

a) Velar por el efectivo cumplimiento de la normativa vigente en el tratamiento de los datos personales.

b) Mantener y actualizar el Registro de las actividades de tratamiento de datos personales.
c) Informar a la Persona Delegada o Delegado de Protección de Datos del registro de las actividades de tratamiento de datos personales, así como las modificaciones del mismo.
d) Responder a los requerimientos que le envíe la Persona Delegada o Delegado de Protección de Datos en relación con los tratamientos de datos personales.
e) Establecer y aplicar las medidas técnicas y organizativas de privacidad y seguridad necesarias para la protección de los datos personales en los tratamientos.
f) Garantizar el cumplimiento de las obligaciones de secreto y confidencialidad derivadas de la normativa en materia de protección de datos personales en relación con los tratamientos.
g) Garantizar el cumplimiento de la obligación de informar adecuadamente, y aplicando el principio de transparencia, en la recogida de los datos personales.
h) Cumplir todas aquellas obligaciones y respetar los derechos de las personas interesadas, de acuerdo con lo previsto en el Reglamento general de protección de datos, en la Ley Orgánica 3/2018, de 5 de diciembre y demás normativa vigente.
i) Realizar los pertinentes análisis de riesgos y evaluaciones de impacto.
j) Notificar, en su caso, las brechas de seguridad de datos personales a la autoridad de control, a las personas interesadas y a la persona Delegada o Delegado de protección de datos, así como, en su caso, a la persona Subdelegada o Subdelegado de protección de datos, conforme a lo dispuesto en el artículo 28.
k) El seguimiento de la correcta aplicación de las medidas técnicas y organizativas que se determinen en cada tratamiento de datos personales.
l) La celebración de un contrato o acto jurídico que le vincule con el encargado del tratamiento, en el que se establezcan las obligaciones de ambas partes, así como la verificación del cumplimiento de las mismas.

Artículo 7. *Los encargados del tratamiento de datos personales.*

1. Cuando se vaya a realizar un tratamiento de datos por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el

tratamiento sea conforme con los requisitos del Reglamento general de protección de datos y garantice la protección de los derechos de la persona interesada.

2. Tanto en la elección del encargado del tratamiento de datos personales, como en el cumplimiento y control de las obligaciones que se establecen, para responsable y encargado del tratamiento, en el artículo 28 del Reglamento general de protección de datos, el responsable estará asistido por su Delegado o Delegada de Protección de Datos.

3. La entidad pública Aragonesa de Servicios Telemáticos, como proveedora principal ante la Administración de la Comunidad Autónoma de Aragón de la cobertura global de las necesidades de ésta en relación con los servicios, sistemas y aplicaciones para la información y las telecomunicaciones, se configura como encargada genérica de los órganos responsables del tratamiento de datos del Gobierno de Aragón, en relación a las citadas funciones, conforme a lo previsto en el artículo 33.5 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 8*. Unidad de Protección de Datos del Gobierno de Aragón*

En la Unidad de Protección de Datos del Gobierno de Aragón, adscrita a la Dirección General competente en materia de Administración electrónica, se desempeñarán las siguientes funciones:

a) Ejercer las funciones de Delegado de Protección de Datos para los conjuntos de datos homogéneos de los Departamentos y organismos autónomos de la Administración pública de la Comunidad Autónoma de Aragón, sin actividades que requieran una observación habitual y sistemática de interesados a gran escala o un tratamiento a gran escala de categorías especiales de datos.
b) Coordinar a las diferentes Unidades de Apoyo a Administración Electrónica y Gobernanza de los Datos, previstas en el artículo 9, que ejerzan funciones de Delegado o Subdelegado de Protección de Datos y de las comunicaciones dirigidas a la Agencia Española de Protección de Datos, salvo aquellas que deban realizarse expresamente por los responsables de los tratamientos
c) Realizar las comunicaciones dirigidas a la Agencia Española de Protección de Datos, salvo aquellas que deban realizarse expresamente por los responsables de los tratamientos de datos personales de los Departamentos y organismos autónomos.

Artículo 9. *Unidades de Apoyo a la Administración Electrónica y Gobernanza de los datos de los Departamentos y de sus organismos autónomos.*

1. Bajo la dependencia funcional de la Dirección General competente en materia de administración electrónica, se identificará, en el seno de cada Departamento, una Unidad de Apoyo de la Administración Electrónica y Gobernanza de los datos y, además, una Unidad de apoyo adicional por Departamento para los organismos autónomos que tengan adscritos.

2. Estas unidades asumirán las funciones de subdelegadas de protección de datos que conllevan la colaboración, asistencia y apoyo a la Unidad que ejerza las funciones de Delegada de Protección de Datos y a los responsables de los tratamientos de su Departamento u Organismo Autónomo de adscripción, en las tareas definidas por el Reglamento General de Protección de Datos.

No obstante, estas unidades realizarán las funciones de Delegadas de protección de datos, a propuesta de las unidades responsables de estos tratamientos, en los siguientes supuestos:

a) La Unidad de Apoyo del Departamento con competencias en materia de educación, que será propuesta por los responsables de actividades de tratamiento de datos de carácter personal de los centros educativos.
b) Las Unidades de Apoyo de los Departamentos y organismos autónomos que tengan responsables de tratamientos de datos genéticos, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales, respecto a estos datos.
c) Las Unidades de Apoyo de los Departamentos y organismos autónomos que tengan responsables de tratamientos de datos de afiliación sindical, respecto a estos datos.
d) Cuando existan otras actividades de tratamiento, diferentes a las indicadas en las letras anteriores del presente apartado, que requieran una observación habitual y sistemática de personas interesadas a gran escala, así como cuando se realicen tratamientos a gran escala de categorías especiales de datos personales con arreglo al artículo 9 del Reglamento General de Protección de Datos. En este caso, se propondrá por los responsables de esas áreas funcionales la designación de unidades que ejerzan las funciones Delegadas de Protección de Datos, propuesta que deberá ser aprobada por el Gobierno de Aragón.

3. Asimismo dichas unidades asumen las siguientes funciones:

a) La implementación de los procesos que posibiliten una adecuada transformación digital de los procedimientos y servicios gestionados por cada Departamento y la definición de nuevos servicios y procedimientos digitales.
b) La adecuación de la información a los estándares de interoperabilidad, así como el resto de las funciones previstas en las directrices de interoperabilidad y reutilización de datos para su apertura en el punto de acceso de datos abiertos del Gobierno de Aragón, aprobadas por Decreto 90/2019, de 18 de junio, por el que se aprueban las directrices de interoperabilidad y reutilización de datos para su apertura en el punto de acceso de datos abiertos del Gobierno de Aragón.
c) El apoyo en la implementación de medidas de seguridad lógica.
d) La asistencia a los órganos administrativos competentes en materia de reutilización de la información y publicación de la misma de acuerdo a las necesidades de publicidad.
e) Cualesquiera otras vinculadas con los objetivos de implementar de forma adecuada la administración electrónica.

Artículo 10. *Las personas que sean Delegadas o Subdelegadas de Protección de Datos de otras entidades de la Administración de la Comunidad Autónoma de Aragón.*

En el caso de las entidades de derecho público y consorcios, adscritos a la Administración de la Comunidad Autónoma de Aragón, deberán designar un Delegado o una Delegada de Protección de Datos, pudiendo articular dicha designación de cualquiera de las formas admitidas por la normativa vigente.

Artículo 11. *Funciones de las personas que sean Delegadas y Subdelegadas de Protección de Datos.*

1. Las personas que sean Delegadas y Subdelegadas de protección de datos ejercerán con autonomía funcional las siguientes funciones:

a) Informar y asesorar a los órganos que ejercen las funciones de responsables o encargados del tratamiento y al personal que lleve a cabo tratamientos de datos, de las obligaciones que les incumben en relación con la normativa de protección de datos personales, en particular, sobre la obligación de llevar un Registro de actividades de tratamiento.

b) Supervisar el cumplimiento de lo previsto en la normativa de protección de datos personales y de los dispuesto en este decreto, la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y la realización de auditorías.
c) Proporcionar el asesoramiento necesario en relación con las evaluaciones de impacto en la protección de datos personales y supervisar su aplicación, de conformidad con el artículo 35 del Reglamento general de protección de datos.
d) Emitir recomendaciones a los órganos responsables o encargados del tratamiento en materia de protección de datos personales.
e) Asesorar al responsable del tratamiento en la gestión de las brechas de seguridad de datos personales asegurándose de que las mismas sean notificadas a la Agencia Española de Protección de Datos. El asesoramiento que preste lo hará en coordinación con las personas responsables en materia de seguridad de la información.
f) Cualesquiera otras funciones que le atribuya la normativa en materia de protección de datos personales.

2. Los Subdelegados de protección de datos asistirán al Delegado de protección de datos en el ejercicio de las atribuciones descritas en el apartado anterior. Las personas que sean Delegadas de protección de datos podrá delegar el ejercicio de dichas funciones en el subdelegado.

3. Las personas que sean Delegadas de Protección de Datos ejercerán sus funciones con total independencia, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. Igualmente, ejercerán sus funciones de forma coordinada con las personas o unidades responsables de seguridad de la información de su Departamento u organismo autónomo.

Artículo 12. *Los grupos de trabajo para la protección de datos personales.*

1. Se podrá constituir un grupo de trabajo para la protección de datos personales en cada uno de los Departamentos de la Administración autonómica que tengan adscritos organismos públicos o algún otro tipo de entidades de las que configuran el sector público autonómico, para su coordinación con los mismos en materia de protección de datos personales.

2. Los grupos de trabajo para la protección de datos personales ejercerán las siguientes funciones:

a) Velar por el cumplimiento de las normas en materia de protección de datos personales.
b) Coordinar criterios de actuación y control en el tratamiento de los datos personales.
c) Impulsar la protección de datos personales desde el diseño y por defecto, así como la minimización de datos.
d) Promover la formación y concienciación en su ámbito.

3. El grupo de trabajo estará compuesto por los siguientes miembros:

a) Una persona representante de cada una de las entidades del sector público autonómico adscritas al Departamento, o tuteladas por el mismo, que será designada por cada una de dichas entidades.
b) Las personas que sean Delegadas y Subdelegadas de Protección de Datos del Departamento y, en su caso, del organismo autónomo adscrito.
c) La persona responsable de la seguridad de la información participará, si corresponde, en las reuniones de dichos grupos de trabajo cuando en los mismos vayan a abordarse cuestiones relacionadas con la seguridad de la información, así como siempre que se requiera su participación.

SECCION 3ª. MEDIDAS PARA EL EJERCICIO DE LOS DERECHOS DE PROTECCIÓN DE DATOS POR LA CIUDADANÍA

Artículo 13. *Ejercicio de los derechos de protección de datos personales.*

1. Los derechos reconocidos en materia de protección de datos personales, en los artículos 15 a 22 del Reglamento general de protección de datos, se ejercerán de conformidad con lo previsto, tanto en el mismo, como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, pudiendo ejercerse directamente o por medio de representante legal o voluntario.

2. Las solicitudes de ejercicio de los derechos de protección de datos personales que se dirijan a un órgano responsable del tratamiento se resolverán por el mismo; contarán para ello con la asistencia del encargado del tratamiento, en el caso de que así consten en el contrato o acto jurídico que les vincule, y con el asesoramiento de su delegado o subdelegado de protección de datos.

El encargado del tratamiento podrá tramitar, por cuenta del responsable, las solicitudes si así se estableciere en el contrato o acto jurídico que les vincule.

3. Los formularios para la presentación de las solicitudes estarán disponibles en la sede electrónica de la Administración pública de la Comunidad Autónoma de Aragón, pudiendo presentarse a través de la misma o en cualquiera de los registros previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre.

4. Las resoluciones de los órganos responsables del tratamiento pondrán fin a la vía administrativa, salvo lo previsto para los organismos públicos en el artículo 98.4 de la Ley 5/2021, de 29 de junio, de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón. Podrán impugnarse en vía judicial, así como acudir al Delegado o Delegada de Protección de Datos o presentar reclamación ante la Agencia Española de Protección de Datos.

SECCION 4ª. SOBRE DETERMINADAS OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Artículo 14. *Registro de las actividades de tratamiento.*

1. El Registro de las actividades de tratamiento incluye el conjunto de actividades de tratamiento de datos personales.

2. El Registro de las actividades de tratamiento de los Departamentos y organismos autónomos será público, salvo en aquellos datos identificativos de personas, y podrá consultarse desde la sede electrónica del Gobierno de Aragón.

3. Los responsables del tratamiento mantendrán actualizado el Registro de las actividades de tratamiento de datos personales, con el asesoramiento de sus diferentes delegados o subdelegados de protección de datos e incluirán toda la información a la que se refiere el artículo 30 del Reglamento general de protección de datos.

Artículo 15. *Análisis de riesgos y evaluación de impacto en la protección de datos personales.*

1. Los órganos responsables del tratamiento de datos personales deberán realizar un análisis del riesgo que, para los derechos y libertades de las personas físicas, pueda conllevar el tratamiento de dichos datos que realizan como responsables y/o como encargados.

Su finalidad será identificar, evaluar y tratar los riesgos que el tratamiento pueda suponer para los derechos y libertades de las personas físicas hasta los niveles que puedan considerarse aceptables.

El análisis de riesgos sobre los derechos y libertades de las personas se realizará de forma coordinada con el análisis de riesgos en relación con las tecnologías de la información y las comunicaciones.

2. Asimismo, los órganos responsables del tratamiento de datos personales llevarán a cabo una evaluación de impacto de las actividades de tratamiento cuando, del análisis realizado, resulte probable que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del Reglamento general de protección de datos.

El informe para la evaluación de impacto en materia de protección de datos personales será firmado por la persona titular del órgano responsable del tratamiento de datos personales.

Las medidas técnicas y organizativas exigidas en el artículo 35.7.d) del Reglamento general de protección de datos que se implementen, se propondrán mediante planes de acción, serán aprobadas por la persona titular del órgano responsable del tratamiento de datos personales y serán comunicados a la Comisión Interdepartamental de Servicios Digitales a través de la Subcomisión de Protección de Datos, reguladas en el capítulo V de este decreto.

3. En cada órgano responsable del tratamiento habrá una persona que ejerza las funciones de coordinación de las diferentes fases del análisis de riesgos y de la evaluación de impacto de las actividades de tratamiento de datos de carácter personal.

4. El órgano responsable del tratamiento y la persona coordinadora serán asesorados en estas tareas por su respectivo Delegado o Subdelegado de Protección de Datos para la realización, tanto del análisis de riegos como para la evaluación de impacto.

La Unidad de Protección de Datos del Gobierno de Aragón, coordinará a Las personas que sean Delegadas y Subdelegadas de Protección de Datos en la realización de las evaluaciones de impacto llevadas a cabo por los Departamentos y sus organismos autónomos.

5. Si la evaluación de impacto mostrara que el tratamiento entraña alto riesgo para los derechos y libertades de la ciudadanía, el órgano responsable del tratamiento, asistido por el Delegado de Protección de Datos, deberá consultar a la Agencia Española de Protección de Datos.

CAPÍTULO III
Política de Seguridad de la Información

SECCIÓN 1ª. PRINCIPIOS Y REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA ADMISTRACIÓN PÚBLICA DE LA COMUNIDAD AUTÓNOMA DE ARAGÓN

Artículo 16. *Principios de seguridad de la información.*

La Política de Seguridad de la Información se desarrollará de acuerdo a los siguientes principios:

a) Alcance estratégico: La seguridad de la información contará con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Gobierno de Aragón para conformar un todo coherente y eficaz.
b) Diferenciación de responsabilidades: La responsabilidad de la seguridad de los sistemas de información estará identificada y se diferenciará de la responsabilidad sobre la prestación de los servicios electrónicos.
c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información. La seguridad de la información se considerará como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información y durante toda su explotación.
d) Gestión de la seguridad basada en los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos que puedan afectar al tratamiento de los datos o de la información hasta niveles aceptables.
e) Establecimiento de medidas para la prevención, detección, respuesta y conservación: La reducción de los niveles de riesgo se realizará mediante el despliegue de medidas de seguridad organizativas, procedimentales y técnicas que minimicen las vulnerabilidades o el impacto de potenciales amenazas.
f) Defensa en profundidad: Se establecerá una estrategia de protección basada en múltiples capas de seguridad que reduzcan la probabilidad de compromiso completo de los sistemas.

g) Proporcionalidad: Las medidas se establecerán en equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos, así como la eficacia y el coste de las medidas de seguridad.
h) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
i) Seguridad por defecto: Los sistemas se diseñarán y configurarán de forma que garanticen un grado suficiente de seguridad por defecto.
j) Responsabilidades de terceros: En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión, contrato o cualquier otro instrumento jurídico, las medidas de seguridad se ajustarán al Esquema Nacional de Seguridad y a la normativa vigente, y serán conformes con la Política de Seguridad de la Información aprobada por este decreto y por sus normas técnicas de desarrollo.
k) Servicio a la ciudadanía: El fin último de las medidas de seguridad es garantizar plenamente los derechos que asisten a la ciudadanía en sus relaciones con la Administración pública de la Comunidad Autónoma de Aragón, asegurando la protección de sus datos, el uso adecuado de los mismos, el acceso de confianza a los medios telemáticos y el desarrollo óptimo de sus derechos en materia de transparencia, acceso a la información pública y reutilización de la información.

Artículo 17. *Requisitos mínimos de seguridad.*

La Política de Seguridad de la Información se articulará de acuerdo con los siguientes requisitos mínimos que deberán adoptar los órganos directivos y órganos de dirección de la Administración pública de la Comunidad Autónoma de Aragón:

a) Gestión de activos de información: Los activos de información se encontrarán inventariados y categorizados y estarán asociados a una persona responsable.
b) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que pueda acceder a los activos de información conozca sus deberes y obligaciones en materia de seguridad y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos. Sus actuaciones serán supervisadas para verificar que se siguen los procedimientos establecidos.

c) Medidas técnicas de seguridad: la estrategia de protección de los sistemas de información se basará en el establecimiento de múltiples capas de seguridad y en la protección del perímetro. Se establecerán controles para la prevención, detección, reacción y recuperación ante amenazas de seguridad con el objetivo de reducir su probabilidad e impacto hasta los niveles de riesgo aceptados por la organización.
d) Seguridad física: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, la operación y la actualización de los sistemas de Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
f) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado.
g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
h) Integridad y actualización: todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se conocerá en todo momento el estado de seguridad de los sistemas y componentes, aplicando con diligencia sus actualizaciones.
i) Gestión de incidentes y brechas de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro, contención, comunicación a las autoridades de referencia, resolución y recuperación ante cualquier suceso que potencialmente pueda comprometer la seguridad de los activos de información

j) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantenimiento de la continuidad de la actividad en el caso de materialización de algún incidente de seguridad, de acuerdo a las necesidades de nivel de servicio. Se dispondrá de planes de recuperación ante incidentes y desastres, los cuales se mantendrán actualizados y reevaluados periódicamente.

k) Formación y concienciación: se realizarán planes para la formación y concienciación para todo el personal en materia de seguridad de la información, de acuerdo a las necesidades y responsabilidades de sus puestos de trabajo. Se asegurará que el personal técnico responsable de la gestión y mantenimiento de los sistemas de información posean formación específica en seguridad para garantizar el adecuado desempeño de sus funciones.

l) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa vigente en materia de seguridad de la información.

m) Auditoría: se evaluarán de manera recurrente las medidas técnicas, organizativas y procedimentales de seguridad desplegadas para asegurar su efectividad y actualización continua ante la aparición de nuevas amenazas.

SECCIÓN 2ª. RESPONSABILIDADES, ORGANIZACIÓN Y GESTIÓN DE LA SEGURIDAD EN LOS DEPARTAMENTOS Y ORGANISMOS PÚBLICOS DE LA ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA DE ARAGÓN

Artículo 18. *Responsabilidades en materia de seguridad.*

1. En la gestión de la seguridad de la información se identificarán las siguientes responsabilidades:

a) La responsabilidad sobre la información, que recaerá en aquel órgano o unidad con competencia para determinar los requisitos de seguridad de la información tratada, estableciendo los niveles de protección, el riesgo aceptable y valorando los impactos de los incidentes que pueden afectar a su seguridad.

b) La responsabilidad sobre el servicio, que recaerá en aquel órgano o unidad con competencia para determinar los requisitos de seguridad de los servicios prestados, estableciendo los niveles de protección, el riesgo aceptable y valorando los impactos de los incidentes que pueden afectar a su seguridad.

c) La responsabilidad sobre la seguridad, que recaerá en aquel órgano o unidad que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

d) La responsabilidad sobre el sistema, que recaerá en aquellos órganos o unidades que operan, desarrollan o mantienen el sistema de información durante todo su ciclo de vida, siendo responsables de la implementación efectiva de las medidas de seguridad determinadas y de la correcta gestión de la seguridad del sistema.

2. Las personas titulares de los órganos directivos y de los órganos de dirección de los Departamentos y organismos públicos, serán las responsables de la información y del servicio, respecto a los sistemas de información bajo su competencia.

3. Las personas responsables de servicio y de la información, con la asistencia de la persona responsable de la seguridad, supervisarán los riesgos existentes sobre los sistemas de información bajo su competencia, impulsando las salvaguardas que resulten adecuadas para su tratamiento o, cuando proceda, aceptando los riesgos residuales.

4. La entidad pública Aragonesa de Servicios Telemáticos actuará como responsable genérico del sistema en todos aquellos sistemas de información alojados dentro de su infraestructura. Complementariamente, dicha responsabilidad sobre el sistema podrá recaer de manera compartida sobre otros órganos o unidades, conforme al apartado 1.d.

5. Las personas responsables del sistema velarán por la adecuada aplicación de las medidas de seguridad establecidas, informando a la persona responsable de seguridad de las anomalías que se detecten. Asimismo, supervisarán el estado de las variables de seguridad de su sistema y colaborarán en la investigación y resolución de los incidentes de seguridad.

Artículo 19. *Organización para la gobernanza en materia de seguridad.*

1. Las funciones en materia de seguridad de la información transversales a la Administración de la Comunidad Autónoma de Aragón y a sus organismos públicos se ejercen a través de los siguientes órganos o unidades comunes:

a) La Comisión Interdepartamental de Servicios Digitales a través de su pleno y de la Subcomisión de Seguridad de la Información, prevista en el artículo 32.

b) La Entidad Pública Aragonesa de Servicios Telemáticos, como medio técnico en materia de tecnologías de la información y comunicaciones, prevista en el artículo 23.

c) La Unidad del responsable de la Seguridad de la Información (CISO - *Chief Information Security Officer*), regulada en el artículo 22.

2. En cada Departamento y organismo público de la Administración de la Comunidad Autónoma de Aragón la organización relativa a la gestión de la seguridad de la información estará compuesta por:

a) Las personas responsables de la información, el servicio y los sistemas de información gestionados bajo su ámbito de competencia, conforme al artículo 18.
b) La persona responsable de seguridad de la información, conforme al artículo 20.
c) El comité de la seguridad de la información, conforme al artículo 21.

3. Las Unidades de Apoyo a Administración Electrónica y Gobernanza de los datos adscritas a cada Departamento y organismo autónomo colaborarán en la implantación de medidas de seguridad lógica, conforme a las funciones que tienen atribuidas en el artículo 9.

Artículo 20. *Los responsables de seguridad de la información de los Departamentos y organismos públicos.*

1. En cada Departamento y organismo público se designará a una persona responsable de seguridad de la información por la persona titular del Departamento u órgano directivo del organismo público, respectivamente.

2. Serán funciones de las personas responsables de la seguridad de la información de los Departamentos y organismos públicos, dentro de su ámbito de competencia, las siguientes:

a) Asesorar y asistir al comité de la seguridad de la información de su Departamento u organismo público para hacer efectiva la adecuada protección de los sistemas de información y servicios digitales.
b) Asistir a los órganos y unidades del Departamento u organismo público en la aplicación efectiva de la Política de Seguridad de la Información, del Cuerpo Normativo de Seguridad de la Información y, cuando proceda, en el desarrollo normativo particular en esta materia.
c) Determinar la categoría de seguridad de los sistemas de información, conforme al Esquema Nacional de Seguridad, de acuerdo con las valoraciones de las personas responsables de la información y servicio correspondientes.
d) Asistir a las personas responsables del servicio y de la información en el análisis de riesgos de sus sistemas de información y en la aplicación de las

medidas de seguridad que resulten adecuadas para preservar los servicios electrónicos prestados.

e) Realizar auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, haciendo seguimiento y control de su estado.
f) Coordinar las actuaciones para la conformidad de sus sistemas con el Esquema Nacional de Seguridad y, en particular, atendiendo a los procesos de declaración o certificación regulados en el mismo.
g) Notificar los incidentes de seguridad al equipo de seguridad de Aragonesa de Servicios Telemáticos y a la Unidad del responsable de la Seguridad de la Información (CISO), conforme al protocolo establecido, coordinando las actuaciones de respuesta ante los mismos.
h) Proporcionar al equipo de seguridad de Aragonesa de Servicios Telemáticos y a la Unidad del responsable de la Seguridad de la Información (CISO) la información que le pudiera ser requerida para colaborar en la investigación de incidentes de seguridad o en la inspección de los sistemas de información.
i) Elaborar informes periódicos del estado de la seguridad de la información para el Comité de seguridad de la información del Departamento u organismo público, para su posterior elevación a la Subcomisión de Seguridad de la Información, prevista en el artículo 36, que recojan el estado de las principales variables de seguridad de sus sistemas de información, así como de los resultados de los análisis de riesgos realizados, los planes y actuaciones llevadas a cabo en materia de seguridad, incidentes ocurridos y acciones de respuesta adoptadas.
j) Recopilar los datos necesarios para completar el Informe Nacional del Estado de la Seguridad de la Información, así como otros indicadores requeridos por la Comisión Interdepartamental de Servicios Digitales y la normativa de seguridad vigente.

3. Para el desempeño de las mencionadas funciones, las personas responsables de seguridad de la información contarán con la asistencia de la Unidad del responsable de Seguridad de Información (CISO), así como de la entidad pública Aragonesa de Servicios Telemáticos, en el ámbito técnico de los sistemas de información gestionados por ella.

Artículo 21. Los *comités de seguridad de la información de los Departamentos y organismos públicos*

1. El comité de seguridad de la información de cada Departamento u organismo público se constituirá como un grupo de trabajo para el impulso, seguimiento y coordinación de la gestión de la Política de Seguridad de la Información en el ámbito de los sistemas gestionados bajo su competencia y de acuerdo con las funciones previstas en este artículo.

2. El Comité de seguridad de la información del Departamento u organismo público estará integrado por:

a) Cada una de las personas responsables de la información, del servicio y del sistema, dentro del Departamento u organismo público, identificadas conforme al artículo 18, o un representante de las mismas, que se designe entre el personal público dentro de su área de competencia con capacidad de decisión sobre los sistemas de información. Entre ellos se designará al presidente del Comité.
b) La persona responsable de seguridad de la información del Departamento u organismo público**.**
c) Un representante de la Entidad Pública Aragonesa de Servicios Telemáticos.
d) El Delegado de Protección de Datos y el Subdelegado de Protección de Datos participará, si corresponde, en las reuniones de dichos comités cuando en las mismas vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación.
e) Complementariamente, se podrán designar otros miembros que resulten relevantes para la gestión de la seguridad del Departamento u organismo público.

3. La constitución de cada comité de seguridad de la información, así como la designación de los distintos responsables, será comunicada por la Secretaría General Técnica del Departamento, u órgano similar del organismo público, a la Subcomisión de Seguridad de la Información en el plazo máximo de un mes desde su constitución y designación, respectivamente.

4. El Comité de seguridad de la información del Departamento u organismo público ejercerá las siguientes funciones en su ámbito de competencias:

a) Realizar el seguimiento del cumplimiento del Cuerpo Normativo de Seguridad de la Información y, cuando proceda, de su desarrollo normativo particular en esta materia.

b) Impulsar el análisis del riesgo de sus sistemas de información, supervisando el estado de aplicación de las medidas de seguridad que resulten adecuadas y el riesgo residual resultante.
c) Realizar el seguimiento de las auditorías de los sistemas de información.
d) Desarrollar planes de mejora de la seguridad de la información.
e) Impulsar la formación y concienciación.
f) Coordinar las actuaciones para la respuesta ante incidentes de seguridad.
g) Informar a la Subcomisión de Seguridad de la Información sobre el estado de la seguridad de la información.
h) Resolver los conflictos que puedan surgir entre las diferentes personas responsables o entre las diferentes áreas.

Artículo 22. *Unidad del responsable de la Seguridad de la Información (CISO).*

1. La Unidad del responsable de la Seguridad de la Información está adscrita a la Dirección General con competencia en materia de administración electrónica. La jefatura de la Unidad del responsable de la Seguridad de la Información ejercerá las funciones de CISO (Chief Information Security Officer) de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos.

2. Son funciones de la Unidad del responsable de la Seguridad de la Información (CISO):

a) Garantizar que los bienes y tecnologías de la información de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos estén adecuadamente protegidos.
b) Definir la Política de Seguridad de la Información del Gobierno de Aragón, conforme a lo previsto en el apartado 3.
c) Realizar el seguimiento necesario para garantizar el cumplimiento del Esquema Nacional de Seguridad (ENS) a través de las certificaciones y auditorías necesarias. Para ello esta Unidad tendrá acceso al establecimiento y supervisión de arquitectura de la seguridad de la organización y coordinará el enlace de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos con el Centro Criptológico Nacional en todo lo relativo a la seguridad.
d) Coordinar a las Unidades de Apoyo a la Administración Electrónica y Gobernanza de los datos de los diferentes Departamentos y organismos autónomos del Gobierno de Aragón en materia de seguridad de la información, así como prestarles asistencia en sus funciones de Subdelegadas de Protección de Datos vinculadas con las evaluaciones de

impacto y la adaptación de medidas de seguridad por parte de los responsables.

e) Contribuir al fomento de la seguridad de la información en la sociedad aragonesa

3. Para el desempeño de las citadas funciones llevará a cabo las siguientes actividades:

a) Asesorar en materia de seguridad de la información al pleno de la Comisión Interdepartamental de Servicios Digitales, participando en su pleno cuando sea requerido, con voz, pero sin voto.

b) Presidir la Subcomisión de Seguridad de la Información y designar a su secretaría.

c) Coordinar los trabajos de las personas responsables de seguridad de la información de los Departamentos y organismos públicos.

d) Coordinar actuaciones para el cumplimiento de la normativa vigente en materia de seguridad de la información, impulsando actuaciones transversales.

e) Elaborar las propuestas de modificación de la Política de Seguridad de la Información para su revisión por la Comisión Interdepartamental de Servicios Digitales y su aprobación como decreto del Gobierno de Aragón, conforme al art 32.

f) Elaborar el segundo nivel del Cuerpo Normativo de Seguridad de la Información conforme al art 24.3.b, con la participación de la Entidad Pública Aragonesa de Servicios Telemáticos, para su revisión por la Subcomisión y su aprobación por el pleno de la Comisión Interdepartamental de Servicios Digitales.

g) Elaborar y aprobar la documentación del tercer nivel del Cuerpo Normativo de Seguridad de la Información, sin perjuicio de la que corresponda aprobar a la entidad Aragonesa de Servicios Telemáticos, conforme al artículo 24.3.c.

h) Publicar y mantener actualizado el Cuerpo Normativo de Seguridad de la Información en la intranet de Gobierno de Aragón, para su conocimiento por el personal público

h) Asistir a los Departamentos y organismos públicos en la aplicación efectiva del Cuerpo Normativos de Seguridad de la Información.

i) Prestar apoyo transversal a Departamentos y organismos públicos de la Comunidad Autónoma de Aragón en las funciones de gestión de riesgos de la información, estableciendo un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

j) Inspeccionar y auditar el estado de seguridad de los sistemas de información, metodologías y herramientas de gestión de la seguridad de la información de la Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos, elaborando propuestas de mejora.

k) Recopilar información de vigilancia digital e inteligencia de amenazas potenciales sobre los sistemas de información de la Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos.

l) Supervisar la corrección de las deficiencias detectadas en los sistemas de información y de las notificaciones practicadas a las autoridades y a la ciudadanía de las brechas de seguridad.

n) Colaborar con la entidad Aragonesa de Servicios Telemáticos en la investigación de incidentes de seguridad.

n) Dirigir las actuaciones de respuesta ante una situación de emergencia que afecte o pueda afectar gravemente a la seguridad de la información y servicios informáticos de la Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos, o afecte o pueda afectar gravemente a los derechos a la protección de datos personales de la ciudadanía y del personal público, en coordinación con la entidad pública Aragonesa de Servicios Telemáticos y la Unidad de Protección de Datos del Gobierno de Aragón.

ñ) Instar a la suspensión temporal del servicio de aquellos sistemas informáticos que manifiestamente estén provocando una quiebra de seguridad, previo informe de impacto a sus responsables de la información, servicio, sistema y seguridad.

o) Asistir a la Unidad de Protección de Datos del Gobierno de Aragón en las evaluaciones de impacto y en la adopción de medidas de seguridad de la información por parte de los órganos o unidades responsables.

p) Desarrollar actividades de formación y concienciación del personal de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos en materia de seguridad de la información.

4. Para el desarrollo de sus funciones, la Unidad del responsable de la Seguridad de la Información (CISO) estará facultada para recopilar de los órganos, unidades o personas responsables las evidencias técnicas o documentales que les sean requeridas. Asimismo, podrá realizar simulacros de ataque y ejercicios de intrusión con el objetivo de verificar la efectividad de las medidas de seguridad de la información dispuestas, notificándolo previamente a las personas responsables de

seguridad de la información de los sistemas auditados, así como a la persona responsable de seguridad de la información de Aragonesa de Servicios Telemáticos.

Artículo 23. *Aragonesa de Servicios Telemáticos.*

1. Corresponderá a Aragonesa de Servicios Telemáticos proponer, implantar y coordinar los medios técnicos que garanticen la seguridad, integridad, calidad y confidencialidad de los sistemas de información y telecomunicaciones de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos y el cumplimiento de la normativa en esta materia.

2. Para el desempeño de las citadas funciones llevará a cabo las siguientes actividades:

a) Certificar su arquitectura tecnológica conforme al Esquema Nacional de Seguridad

b) Implantar un ciclo de mejora continua de la seguridad.

c) Participar, junto con la Unidad del responsable de la Seguridad de la Información (CISO), en la elaboración del segundo nivel del Cuerpo Normativo de Seguridad de la Información, conforme al art. 24.3.b.

d) Elaborar y aprobar la documentación del tercer nivel del Cuerpo Normativo de Seguridad de la Información en el ámbito de los sistemas de información y comunicaciones gestionados por la entidad, conforme al artículo 24.3.c.

e) Establecer requisitos mínimos de seguridad de la información para las aplicaciones y sistemas informáticos desplegados por los Departamentos y organismos públicos, dentro de su infraestructura.

f) Mantener el inventario actualizado de los sistemas de información y comunicaciones bajo su gestión

g) Monitorizar en tiempo real los sistemas de información y comunicaciones de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos para prevenir, detectar y reaccionar ante incidentes de seguridad.

h) Ejecutar medidas preventivas y reactivas de respuesta ante eventuales incidentes por medio de la acción directa sobre los sistemas.

i) Investigar los incidentes de seguridad para identificar las causas raíz.

j) Notificar los incidentes de seguridad a la Unidad del responsable de la Seguridad de la Información (CISO) y autoridades competentes, conforme al artículo 28.

k) Auditar su infraestructura tecnológica y los servicios electrónicos alojados en la misma, para determinar el cumplimiento de los requisitos mínimos de seguridad de la información establecidos, informando a los responsables

correspondientes de las deficiencias encontradas, así como a la Unidad del responsable de la Seguridad de la Información (CISO) y a la Subcomisión de Seguridad de la Información de la Comisión Interdepartamental de Servicios Digitales.

l) Trasladar propuestas de mejora de la seguridad de la información a la Subcomisión de Seguridad de la Información de la Comisión Interdepartamental de Servicios Digitales y a los Comités de Seguridad de la Información de los Departamentos y organismos públicos.

n) Elevar a la Subcomisión de Seguridad de la Información el informe del estado de la seguridad.

n) Impulsar la cooperación con la «Red Nacional de SOCs (*Security Operation Centers*)» y otros CERTs (*Computer Emergency Response Team)* nacionales e internacionales.

4. Aragonesa de Servicios Telemáticos designará una persona responsable de seguridad que actuará como interlocutora operativa ante los órganos y unidades con competencias en materia de seguridad de la información de la Administración de la Comunidad Autónoma de Aragón y sus organismos públicos.

5. La persona responsable de seguridad de la citada entidad se designará como punto de contacto operativo y de coordinación técnica ante las autoridades legalmente establecidas en materia de seguridad de la información, en el ámbito de la infraestructura tecnológica gestionada por la entidad.

Artículo 24. *Cuerpo Normativo de la Seguridad de la Información.*

1. En el ámbito de la Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos, se elaborará y mantendrá actualizado el denominado Cuerpo Normativo de Seguridad de la Información, que recogerá de forma sistematizada el conjunto de normas, instrucciones, directrices, guías e instrumentos similares adoptados en materia de seguridad de la información.

2. Todos los instrumentos que se incorporen al Cuerpo Normativo de Seguridad de la Información deberán cumplir estrictamente con lo indicado en el Esquema Nacional de Seguridad y en el resto de normas aplicables a esta materia en el ámbito de Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos. Asimismo, cada uno de los niveles descritos en el apartado 3 deberá respetar lo dispuesto en los niveles superiores.

3. El Cuerpo Normativo de la Seguridad de la Información será de obligado cumplimiento y se estructurará en los siguientes niveles jerárquicos:

a) Primer nivel normativo de seguridad, que está constituido por la Política de Seguridad de la Información establecida en este decreto.

b) Segundo nivel normativo de seguridad, que está constituido por las «Normas Técnicas de Seguridad de la Información de la Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos». Estas normas establecerán los requisitos generales que deberán cumplirse para preservar la seguridad de la información.

c) Tercer nivel normativo de seguridad, que estará compuesto por procedimientos, guías, instrucciones técnicas, directrices, plantillas, recomendaciones y similares. Estos instrumentos desarrollarán lo definido en los niveles normativos superiores. Su ámbito de aplicación podrá ser general o corresponder a un ámbito orgánico específico o a un sistema de información determinado.

4. Los Departamentos, organismos públicos u órganos directivos podrán aprobar disposiciones específicas en cualquiera de los tres niveles normativos, atendiendo a necesidades propias de carácter legal, organizativo o técnico respecto a la seguridad de la información. En todo caso, dichos cuerpos normativos serán complementarios y no contravendrán el Cuerpo Normativo de Seguridad de la Información, previsto en el apartado 3, estando limitados a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean gestionados bajo su competencia.

3. El Cuerpo Normativo de Seguridad de la Información se encontrará a disposición de todo el personal en la intranet de Gobierno de Aragón.

CAPÍTULO IV

Disposiciones comunes a las Políticas de Protección de Datos y de Seguridad de la Información

Artículo 25. *Obligaciones del personal.*

1. Todo el personal al servicio de la Administración pública de la Comunidad Autónoma de Aragón que realice algún tipo de tratamiento de datos de carácter personal, que utilice o tenga acceso a los sistemas tecnológicos o de información corporativos, así como a la información en ellos contenida, tiene las siguientes obligaciones:

a) Conocer y respetar las Políticas de Protección de Datos y de Seguridad de la Información establecidas en este decreto, así como aquellas disposiciones

del Cuerpo Normativo de Seguridad de la Información que puedan afectar a sus funciones.

b) Atender a las acciones de concienciación en materia de protección de datos y seguridad de la información que se realicen.

c) Utilizar los servicios y sistemas de información, así como la información en ellos contenida y a la que tengan acceso, con una finalidad profesional acorde a las tareas encomendadas en función de su puesto de trabajo y a los fines y propósitos que motivaron la concesión del acceso.

d) Velar por la confidencialidad de la información a la que tenga acceso según la clasificación y características de la misma.

e) Notificar eventos que puedan suponer una brecha de seguridad o evidencien una debilidad que pueda implicar posteriores brechas.

f) Colaborar en la resolución de brechas de seguridad y en la realización de acciones preventivas cuando sea necesaria su participación.

g) Participar en la estructura de gestión de la seguridad de la información cuando corresponda según las competencias y funciones de su puesto de trabajo.

h) No realizar acciones intencionadas o negligentes que puedan perjudicar la seguridad de los sistemas tecnológicos o la información que contienen.

2. En el caso de personas vinculadas a entidades externas, el tratamiento de datos de carácter personal o el uso de los sistemas tecnológicos o de información corporativos se limitará a las tareas o actividades circunscritas, en los términos del contrato o acuerdo que regula la relación entre esa entidad y la Administración pública de la Comunidad Autónoma de Aragón.

3. El incumplimiento de las Políticas de Protección de Datos y de la de Seguridad de la Información podrá tener consecuencias disciplinarias, de acuerdo con el régimen disciplinario aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

Artículo 26. *Formación y concienciación.*

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal de la Administración pública de la Comunidad Autónoma de Aragón, así como a la difusión entre los mismos de las Políticas de Protección de Datos y de Seguridad de la Información y del Cuerpo Normativo de Seguridad de la Información

2. La Unidad del responsable de la Seguridad de la Información (CISO), la Entidad Pública Aragonesa de Servicios Telemáticos, así como las personas

responsables de seguridad de la información de los Departamentos y organismos públicos, se encargarán de promover las actividades de formación y concienciación en materia de seguridad de la información en cada uno de sus ámbitos. La Subcomisión de Seguridad de la Información de la Comisión Interdepartamental de Servicios Digitales actuará como coordinadora de dichas actividades.

3. Las personas que sean Delegadas y Subdelegadas de Protección de Datos y la Unidad de Protección de Datos del Gobierno de Aragón se encargarán de promover las actividades de formación y concienciación en materia de protección de datos.

Artículo 27. *Gestión de los riesgos de seguridad de la información.*

1. La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre cada sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y en la reevaluación periódica.

2. Las personas responsables de la información y del servicio de la Administración de la Comunidad Autónoma de Aragón y de sus organismos públicos se encargarán de analizar y evaluar los riesgos de funcionamiento de los servicios con el fin de establecer las correspondientes medidas preventivas, dentro de su ámbito de actuación y de sus competencias.

3. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de las Administraciones Públicas y, en especial, las guías elaboradas por el Centro Criptológico Nacional.

Artículo 28. *Notificación de incidentes y brechas de seguridad.*

1. Los incidentes con afección sobre la seguridad de la información se comunicarán en cuanto se tenga conocimiento de los mismos al correspondiente responsable de seguridad de la información, así como a la entidad pública Aragonesa de Servicios Telemáticos y a la Unidad del responsable de la Seguridad de la Información (CISO). La persona responsable de seguridad competente realizará la notificación al Centro Criptológico Nacional cuando sea pertinente, conforme al protocolo y sistema centralizado regulado en el apartado 4.

2. En el caso en que dicho incidente constituya una brecha de seguridad con afección sobre datos de carácter personal, ésta se comunicará también, en cuanto se tenga conocimiento de las mismas, al Delegado o, en su caso, al Subdelegado de Protección de Datos, así como a la persona responsable de la Unidad de Protección

de Datos del Gobierno de Aragón, para su notificación a la Agencia Española de Protección de Datos.

3. Cuando sea probable que la violación de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, conforme al artículo 34 del Reglamento general de protección de datos**,** el responsable del tratamiento lo comunicará a la persona interesada sin dilación indebida.

4. Las Unidades de Protección de Datos y del Responsable de Seguridad de la Información (CISO), con la colaboración de Aragonesa de Servicios Telemáticos, establecerán un protocolo y sistema centralizado para la comunicación y gestión de los incidentes y brechas de seguridad para la Administración pública de la Comunidad Autónoma de Aragón, el cual estará integrado con la Plataforma de notificación de incidentes referida en el artículo 19.4 del Real Decreto-Ley 12/2018, de 7 de septiembre, y con las autoridades nacionales competentes, en particular el Centro Criptológico Nacional y la Agencia Española de Protección de Datos.

Artículo 29. *Revisión y auditoría.*

1. Cada sistema de información de la Administración pública de la Comunidad Autónoma de Aragón deberá ser auditado con una periodicidad mínima de dos años o cuando se produzcan modificaciones sustanciales en el mismo, conforme a las disposiciones del Esquema Nacional de Seguridad. Las auditorías evaluarán la eficacia de las medidas técnicas y organizativas existentes para garantizar la seguridad de los tratamientos y sistemas de información.

2. Las auditorías serán realizadas por la persona responsable de seguridad del Departamento u organismo público correspondiente, con el apoyo de la Unidad del responsable de la Seguridad de la Información (CISO) y por la persona Delegado o Subdelegado de protección de datos personales correspondiente, y supervisadas por la Subcomisión de Seguridad de la Información de la Comisión Interdepartamental de Servicios Digitales.

3. Complementariamente, los sistemas de información de la Administración pública de la Comunidad de Aragón podrán ser auditados, para la verificación de su estado de seguridad, por la Unidad del responsable de la Seguridad de la Información (CISO), así como por la Entidad Pública Aragonesa de Servicios Telemáticos en aquellos sistemas de información bajo su gestión.

4. La persona Delegado o Delegada de protección de datos correspondiente supervisará las auditorías sobre el cumplimiento del Reglamento general de protección de datos que se realicen sobre responsables y encargados de tratamiento.

Artículo 30. *Relaciones con terceros.*

1. Cuando la Administración pública de la Comunidad Autónoma de Aragón preste servicios o ceda datos de carácter personal o información a otras Administraciones Públicas u organismos, se les hará partícipes a estas últimas de las Políticas de Protección de Datos y de Seguridad de la Información y de la normativa de seguridad derivada.

2. Cuando la Administración pública de la Comunidad Autónoma de Aragón utilice servicios de terceros o les ceda datos de carácter personal o información, se les hará igualmente partícipes de estas Políticas de Protección de Datos y Seguridad de la Información y de la normativa de seguridad que sea aplicable a dichos servicios o información, debiendo observarse las siguientes reglas:

a) Los terceros quedarán sujetos a las obligaciones y medidas de seguridad establecidas en dicha normativa de seguridad de la información pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

b) Se establecerán procedimientos específicos de detección y resolución de incidencias.

c) Se garantizará por parte de estos terceros, que su personal está adecuadamente concienciado en materia de protección de datos y de seguridad de la información, al menos al mismo nivel que el establecido en las Políticas de Protección de Datos y de Seguridad de la Información que aprueba este decreto.

d) Los terceros deberán garantizar el cumplimiento de las Políticas de Protección de Datos y Seguridad de la Información, para lo cual se requerirá evidencia de la conformidad de las medidas de seguridad implantadas por estos con las establecidas en el Esquema Nacional de Seguridad en función de la categoría del sistema, que será determinada por la persona responsable de seguridad del Departamento u organismo público correspondiente. Asimismo, se garantizará mediante auditoría o certificado de destrucción o borrado que el tercero, cancela y elimina los datos pertenecientes a la Administración pública de la Comunidad Autónoma tras la finalización del contrato.

e) Los terceros garantizarán la protección de datos y seguridad de la información sobre su cadena de suministro, siendo responsables de otros terceros subcontratados a los que trasladará el contenido y obligaciones de estas políticas y de la normativa aplicable. El Departamento u organismo público responsable de la dirección de un contrato prestado por un tercero deberá ser informado de las subcontrataciones realizadas por el mismo y

podrá auditar el cumplimiento por parte de los subcontratados de las medidas u obligaciones exigidas por parte de cada uno de los terceros involucrados en la ejecución.

f) Cuando algún aspecto de la Política de Protección de Datos y de Seguridad de la Información no pueda ser satisfecho por un tercero, se requerirá un informe de la persona Delegada de Protección de Datos y de la persona responsable de seguridad del Departamento u organismo público que precise los riesgos en que se incurre y la forma de tratarlos. A la vista de dicho informe, y antes de que se haga efectiva la prestación uso**,** acceso o cesión de que se trate, los responsables del tratamiento de datos y/o de la información o de los servicios decidirán sobre la aceptación o no del riesgo residual de las actividades de tratamiento y/o de los sistemas de información relacionados con la información o los servicios de los que son responsables.

Artículo 31. *Modificación de las Políticas de Protección de Datos y de Seguridad de la Información.*

Las Unidades de Protección de datos de Gobierno de Aragón y del responsable de la Seguridad de la Información (CISO) elaborarán las propuestas de modificación de la presente política, elevando las mismas para su revisión a la Comisión Interdepartamental de Servicios Digitales, para su aprobación como decreto por el Gobierno de Aragón.

CAPÍTULO V
La Comisión Interdepartamental de Servicios Digitales

Artículo 32. *La Comisión Interdepartamental de Servicios Digitales.*

1. La Comisión Interdepartamental de Servicios Digitales es el órgano colegiado de coordinación, desarrollo y seguimiento de los compromisos que los planes estratégicos en materia de servicios digitales atribuyen a la Administración de la Comunidad Autónoma de Aragón, así como respecto a las Políticas de Protección de Datos y de Seguridad de la Información de la Administración pública de la Comunidad Autónoma de Aragón.

2. La Comisión estará adscrita al Departamento competente en materia de administración electrónica.

3. En el momento de su creación sustituirá a la actual Comisión interdepartamental de Administración Electrónica.

4. La Comisión estará integrada por las siguientes subcomisiones técnicas, que no tendrán el carácter de órgano colegiado:

a) Subcomisión de Protección de Datos Personales.

b) Subcomisión de Seguridad de la Información.

c) *Subcomisión de Diseño y desarrollo de servicios públicos*.

d) Subcomisión de Gobernanza de datos.

5. Se podrán crear por el Pleno de la Comisión Interdepartamental de Servicios Digitales aquellas otras subcomisiones que se estimen necesarias para conseguir un mejor funcionamiento de la misma.

Artículo 33. *Competencias.*

1. Corresponden al pleno de la Comisión Interdepartamental de Servicios Digitales las siguientes competencias:

a) El impulso y la coordinación de las iniciativas de administración electrónica en la Administración pública de la Comunidad Autónoma.

b) El establecimiento de las líneas estratégicas de actuación y de las directrices generales, de acuerdo con la política del Gobierno de Aragón, en materia de administración electrónica.

c) La declaración de líneas prioritarias de actuación en materia de administración electrónica.

d) El seguimiento de los planes e iniciativas de la Administración pública de la Comunidad Autónoma en materia de administración electrónica, asegurando su alineamiento con las líneas estratégicas del Gobierno.

e) El impulso y coordinación de las Políticas de Protección de Datos Personales y de Seguridad de Información de la Administración pública de la Comunidad Autónoma de Aragón y de las actividades relacionadas con ellas, ejerciendo las siguientes funciones:

1.ª Revisar las propuestas de modificación de las Políticas de Protección de Datos y de Seguridad de la Información elaboradas por las Unidades de Protección de datos y la del responsable de la Seguridad de la Información (CISO), para su aprobación como decreto de Gobierno de Aragón, conforme al artículo 31.

2.ª Velar e impulsar el cumplimiento de ambas Políticas, el Reglamento general de protección de datos, el Esquema Nacional de Seguridad y la normativa vigente en estas materias.

3.ª Aprobar, a propuesta de la Subcomisión de Seguridad de la Información, el segundo nivel normativo del Cuerpo Normativo de Seguridad de la Información conforme al artículo 24.3.

4.ª Promover la protección de datos personales desde el diseño y por defecto.

5.ª Promover la mejora continua en la gestión de la seguridad de la información.

6.ª Impulsar la obtención de certificaciones y la realización de las auditorías necesarias en el ámbito, tanto de la protección de datos personales como de la seguridad de la información, por parte de los diferentes Departamentos y organismos públicos de la Administración de la Comunidad Autónoma de Aragón.

9.ª Impulsar la formación y concienciación en materia de privacidad y de seguridad de la información.

10.ª El impulso y la coordinación de las actuaciones en materia de gobierno y calidad de los datos, en la Administración pública de la Comunidad Autónoma

11.ª Resolver los conflictos que puedan aparecer entre los diferentes responsables o diferentes áreas de la organización.

f) Aquellas otras competencias que le sean atribuidas por el ordenamiento jurídico.

2. El pleno deberá ser informado, por las Subcomisiones correspondientes, de las siguientes materias:

a) Los criterios comunes y documentación general a utilizar en el tratamiento de datos personales. En especial, en relación a los tratamientos que consistan en una observación habitual y sistemática de interesados a gran escala, tratamientos a gran escala de categorías especiales de datos, geolocalización, actuaciones administrativas automatizadas, elaboración de perfiles, explotación masiva de datos, así como aquellos tratamientos realizados a partir de algoritmos.

b) Las evaluaciones de impacto y los planes de acción que se realicen por los responsables de tratamiento de datos personales.

c) El estado de las principales variables de seguridad en los sistemas de información de la Administración pública de la Comunidad Autónoma de Aragón y de los planes de mejora de la misma.

d) Los análisis de riesgo de los sistemas de información realizados, su grado de cobertura y resultados, conociendo aquellos riesgos residuales

identificados con alta probabilidad o alto impacto para el establecimiento de una estrategia para su gestión.

Artículo 34. *Composición del Pleno de la Comisión Interdepartamental de Servicios Digitales.*

1. El pleno de la Comisión Interdepartamental de Servicios Digitales estará constituida por los siguientes miembros:

a) La persona titular de la Secretaría General Técnica del Departamento competente en materia de administración electrónica, que presidirá y ostentará la representación de la Comisión. La presidencia podrá delegar sus funciones en la vicepresidencia.

b) La persona titular de la Dirección General competente en materia de administración electrónica, a quien le corresponderá la vicepresidencia.

c) Por las siguientes vocalías:

1º. Las personas titulares de la Secretaría General Técnica de cada Departamento de la Administración de la Comunidad Autónoma de Aragón.

2º. La persona titular de la Secretaría General de la Presidencia.

3º. El Director o la Directora Gerente de la entidad pública Aragonesa de Servicios Telemáticos.

2. La Secretaría corresponderá a un funcionario o funcionaria de la Dirección General competente en materia de administración electrónica, perteneciente a los Cuerpos Superiores de la Administración de la Comunidad Autónoma, que actuará con voz, pero sin voto.

3. La persona titular de la presidencia designará y cesará al secretario o secretaria titular, así como a la persona que, para los casos de vacante, ausencia, enfermedad, u otro impedimento personal u otra causa legal, actúe como suplente.

Artículo 35. *Subcomisión de Protección de Datos Personales*

1. Las funciones de la Subcomisión de Protección de Datos Personales son:

a) Elaborar y aprobar propuestas de desarrollo de la Política de Protección de Datos Personales, para su adopción por parte de la Administración pública de la Comunidad Autónoma de Aragón.

b) Supervisar y asegurar la coherencia de la normativa de protección de datos personales de la Administración pública de la Comunidad Autónoma de Aragón en relación al cumplimiento de lo dispuesto en el Reglamento general de protección de datos, en otras disposiciones de protección de datos de la Unión Europea, así como

en la normativa nacional en dicha materia, en particular la Ley Orgánica 3/2018, de 5 de diciembre, incluida la designación de los responsables de tratamiento, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

c) Elaborar criterios comunes y documentación general a utilizar en el tratamiento de datos personales. En especial, en relación a los tratamientos que consistan en una observación habitual y sistemática de interesados a gran escala, tratamientos a gran escala de categorías especiales de datos, geolocalización, actuaciones administrativas automatizadas, elaboración de perfiles, explotación masiva de datos, así como aquellos tratamientos realizados a partir de algoritmos.

d) Fijar directrices en materia de protección de datos personales y, específicamente, sobre la investigación y resolución de las brechas de confidencialidad, el ejercicio de derechos de protección de datos personales, así como las evaluaciones de impacto de los derechos y libertades de la ciudadanía.

e) Promover la realización de auditorías periódicas de protección de datos personales.

2. La Subcomisión de Protección de Datos Personales está compuesta por los siguientes miembros:

a) La persona titular de la Jefatura de la Unidad de Protección de Datos del Gobierno de Aragón a quien le corresponderá la presidencia.

b) Las personas que sean Delegadas y Subdelegadas de Protección de Datos de cada Departamento y cada organismo autónomo, que actuarán como vocales.

c) La persona titular de la jefatura de la Unidad del responsable de la Seguridad de la Información (CISO) que actuará en las reuniones de la Subcomisión cuando se vayan a abordar cuestiones relacionadas con la seguridad de la información.

d) La Secretaría corresponderá a un funcionario o funcionaria de la Unidad de Protección de Datos del Gobierno de Aragón.

3. La persona titular de la presidencia de esta Subcomisión designará y cesará al secretario o secretaria titular, así como a la persona que, para los casos de vacante, ausencia, enfermedad, u otro impedimento personal u otra causa legal, actúe como suplente.

Artículo 36. *Subcomisión de Seguridad de la Información*

1. Las funciones de la Subcomisión de Seguridad de la Información son:

a) Revisar las propuestas de desarrollo del segundo nivel del Cuerpo Normativo de Seguridad de la Información elaboradas por la Unidad del

responsable de la Seguridad de la Información (CISO) y elevarlas para su aprobación por parte del pleno.

b) Conocer de las particularizaciones que Departamentos, organismos públicos u órganos directivos realicen del Cuerpo Normativo de Seguridad de la Información, conforme al artículo 24.3.

c) Coordinar, impulsar y supervisar la realización de los análisis de riesgos de los sistemas de información en los diferentes Departamentos y organismos públicos, informando al pleno de su resultado y grado de cobertura y elevando al mismo aquellos riesgos residuales identificados con alta probabilidad o alto impacto para el establecimiento de una estrategia para la gestión de los mismos.

d) Evaluar el estado de seguridad de la información de la Administración pública de la Comunidad Autónoma de Aragón, diseñando planes de mejora de la misma. Para ello recabará información de los **r**esponsables de seguridad de la información de los Departamentos y organismos públicos, de la entidad pública Aragonesa de Servicios Telemáticos y de la Unidad del responsable de la Seguridad de la Información (CISO).

e) Realizar el seguimiento de las actuaciones en materia de seguridad de la información llevadas a cabo por los Departamentos y organismos públicos y coordinar acciones conjuntas.

f) Promover y realizar el seguimiento de los planes de formación en materia de seguridad de la información.

g) Promover y realizar seguimiento de la auditoría periódica de los sistemas de la información.

2. La Subcomisión de Seguridad de la Información está compuesta por los siguientes miembros:

a) La persona titular de la jefatura de la Unidad del responsable de la Seguridad de la Información (CISO) que ejercerá la presidencia.

b) La persona responsable de seguridad de la información de la entidad pública Aragonesa de Servicios Telemáticos que asumirá la vicepresidencia.

c) Las personas responsables de la seguridad de la información de cada Departamento y cada organismo autónomo, que actuarán como vocales.

d) La persona titular de la jefatura de la Unidad de Protección de Datos del Gobierno de Aragón que actuará en las reuniones de la Subcomisión cuando se vayan a abordar cuestiones relacionadas con el tratamiento de datos de carácter personal.

e) La Secretaría corresponderá a un funcionario o funcionaria de la Dirección General competente en materia de administración electrónica.

3. La persona titular de la presidencia de esta Subcomisión designará y cesará al secretario o secretaria titular, así como a la persona que, para los casos de vacante, ausencia, enfermedad, u otro impedimento personal u otra causa legal, actúe como suplente.

Artículo 37. *Subcomisión de Diseño y desarrollo de servicios públicos*

1. La Subcomisión de Diseño y desarrollo de servicios públicos conocerá de las actuaciones en materia de diseño y desarrollo de servicios, así como las relativas a la transformación digital, en el ámbito de la Administración pública de la Comunidad Autónoma de Aragón.

2. En el momento de su creación sustituirá a la actual Subcomisión de Administración Electrónica.

3. Su composición y funciones se desarrollarán por orden del Departamento competente en materia de administración electrónica.

Artículo 38. *Subcomisión de Gobernanza de datos*

1. La Subcomisión de Gobernanza de datos conocerá de las actuaciones en materia de gobierno y calidad de los datos, en el ámbito de la Administración pública de la Comunidad Autónoma de Aragón.

2. Su composición y funciones se desarrollarán por orden del Departamento competente en materia de administración electrónica.

Artículo 39*. Funcionamiento del pleno y de las subcomisiones.*

1. El pleno de la Comisión Interdepartamental de Servicios Digitales se reunirá en sesión ordinaria, al menos, dos veces al año y en sesión extraordinaria cuando lo decida el Presidente o Presidenta o por iniciativa de una quinta parte de sus miembros.

2. La Presidencia del pleno de la Comisión, de oficio o a propuesta de una quinta parte de sus miembros, podrán convocar para asistir a las reuniones con voz, pero sin voto, a personas, procedentes de la Administración o de terceras entidades, que sean expertas en la materia objeto de debate.

3.Sin perjuicio de lo dispuesto en este decreto, el funcionamiento del Pleno se regirá por la normativa aplicable a los órganos colegiados de la Administración de la Comunidad Autónoma de Aragón y por las propias normas de funcionamiento que pudieran aprobarse.

4. El régimen de funcionamiento de las subcomisiones será el establecido en una orden del Departamento competente en materia de administración electrónica.

Artículo 40. *Medios.*

El Departamento competente en materia de administración electrónica dotará a la Comisión Interdepartamental de Servicios Digitales de los medios personales y materiales que sean precisos para el desarrollo de sus funciones, sin que ello suponga incremento del gasto público.

Disposición adicional primera. Definiciones técnicas y su actualización.

Las definiciones incluidas en el Anexo que sean reproducción de las incluidas en normas ya vigentes se considerarán automáticamente sustituidas por las contenidas en las normas modificativas***.***

Disposición adicional segunda. Régimen jurídico de los comités y grupos de trabajo.

Los Grupos de trabajo para la protección de datos personales y los Comités de seguridad de la información de Departamentos u organismos públicos previstos en los artículos 12 y 21, respectivamente, podrán acordar para su funcionamiento las correspondientes reglas de régimen interno.

Disposición derogatoria única. Derogación normativa.

1. Queda derogado el Decreto 28/2011, de 22 de febrero, del Gobierno de Aragón, por el que se crea y se regula la Comisión Interdepartamental de Administración Electrónica.

2. Quedan derogas las disposiciones normativas que se opongan a este decreto.

Disposición final primera. Habilitación de desarrollo.

Se faculta al a la persona titular del Departamento competente en materia de administración electrónica para dictar cuantas normas fueran necesarias para el desarrollo y la ejecución de lo previsto en este decreto.

Disposición final segunda. Entrada en vigor.

Este decreto entrará en vigor el día siguiente al de su publicación en el “Boletín Oficial de Aragón”.

ANEXO

Definiciones técnicas

A los efectos previstos en este decreto, se entiende por:

a) Activo (de tecnologías de la información y las comunicaciones): cualquier información o sistema de información que tenga valor para la organización. Incluye información, datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.

b) Análisis de riesgos: método que, mediante la utilización sistemática de la información, proporciona una visión clara y priorizada de los riesgos a los que se enfrenta una organización respecto a un sistema de información o a una actividad de tratamiento de datos carácter personal, y el impacto que tendrían. Pretende identificar los riesgos más significativos que pueden afectar a la operativa de la organización y priorizar medidas a implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto en caso de materializarse.

c) Auditoría de la seguridad de los sistemas de información: Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del mismo, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles de la política y de los procedimientos.

d) Autenticidad**:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

e) Confidencialidad**:** Propiedad o característica consistente en que la información únicamente es puesta a disposición o revelada a individuos, entidades o procesos autorizados.

f) Contingencia grave: Incidente de seguridad relacionado con las tecnologías de la información y la comunicación cuya ocurrencia causaría la reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, el sufrimiento de un daño significativo a los activos de la organización, el incumplimiento material de alguna norma o directriz, un daño reputacional apreciable con la ciudadanía o con otras organizaciones o un perjuicio significativo de difícil reparación a personas.

g) Cuerpo normativo de seguridad: serie de documentos que desarrollan la Política de Seguridad de la Información de una organización, describiendo las di-

rectrices y procedimientos para el uso correcto de equipos, servicios e instalaciones, procesos para la ejecución de tareas y la responsabilidad del personal y terceros.

h) Datos personales: toda información sobre una persona física identificada o identificable. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
i) Disponibilidad**:** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
j) Encargado del tratamiento o encargado de datos personales: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
k) Exactitud: Principio relativo al tratamiento de los datos de carácter personal respecto a su finalidad y que se refiere a que el contenido de los mismos se ajuste a la realidad.
l) Incidente o brecha de seguridad TIC: Suceso, accidental o intencionado, a consecuencia del cual se ve afectada alguna de las dimensiones de la seguridad de la información: integridad, confidencialidad o disponibilidad.
m) Integridad**:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
n) Inventario de activos de tecnologías de la información y las comunicaciones: Lista de todos aquellos activos de tecnologías de la información y las comunicaciones que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
o) Plan de acción: Documento que determina las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas y, si procede, el resultado de la consulta previa a la Agencia Española de Protección de Datos.
p) Responsable del tratamiento de datos personales: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable

del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

q) Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. La evaluación de un riesgo se determina en función de su probabilidad de suceso y de su impacto en caso de materializarse.
r) Riesgo residual: Nivel de riesgo que permanece en la organización tras el tratamiento realizado tras un análisis de riesgos.
s) Sistema de información: Conjunto organizado de recursos destinado a recoger, almacenar, procesar, presentar o transmitir la información.
t) Tratamiento de datos personales: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
u) Tratamiento del riesgo: actuaciones desarrolladas para conducir un riesgo identificado a un nivel aceptable para la organización a través de su eliminación, mitigación, transferencia o aceptación.
v) Trazabilidad**:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.