
RESOLUCIÓN del Presidente del Instituto Aragonés de Gestión Ambiental por la que se aprueban los criterios en materia de protección de datos de carácter personal y seguridad de la información del Instituto Aragonés de Gestión Ambiental.

Con el fin cumplir efectivamente las obligaciones derivadas de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y del Reglamento (UE) 2016/679, del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, el Gobierno de Aragón, una vez analizada la situación existente en los diferentes Departamentos de la Administración de la Comunidad Autónoma de Aragón y a la vista del diagnóstico inicial realizado a nivel de Dirección General e incluso Servicios, adoptó un Acuerdo el 24 de julio de 2018 aprobando la implantación de medidas organizativas en materia de administración electrónica, protección de datos de carácter personal y seguridad de la información

Entre las medidas organizativas adoptadas destacan, por una parte, la creación de tres Unidades específicas (Unidad de Protección de Datos del Gobierno de Aragón, Unidad del responsable de la Seguridad de la Información y Unidad de Diseño de procedimientos y servicios digitales) encuadradas en la Dirección General competente en materia de administración electrónica, que tendrán las funciones que se detallan en el Anexo I del referido Acuerdo y dependerán de la citada Dirección General tanto orgánica como funcionalmente.

Por otra parte, también se crea por cada Departamento una Unidad de Apoyo a la Administración electrónica y Gobernanza de los Datos y, además, para cada uno de los Organismos Autónomos que tenga adscrito cada Departamento, una Unidad de Apoyo adicional. Todas estas Unidades de Apoyo tendrán dependencia orgánica de cada Organismo Autónomo o Departamento, si bien funcionalmente dependerán de la Dirección General competente en materia de administración electrónica.

La Dirección General competente en materia de administración electrónica, a través de la Unidad de Protección de Datos del Gobierno de Aragón, ejercerá las funciones de Delegado de protección de Datos excepto para los Departamentos y Organismos Autónomos que realicen tratamiento a gran escala de categorías especiales de datos personales según dispone el artículo 9 del Reglamento General de Protección de Datos.

Asimismo, el citado Acuerdo dispone que las Entidades de Derecho Público y Consorcios adscritos a la Administración de la Comunidad Autónoma de Aragón, a los que es de aplicación el artículo 37.1 a) del Reglamento General de protección de Datos, deberán designar Delegado de Protección de Datos, pudiendo articular dicha designación de cualquiera de las formas admitidas por la normativa vigente, si bien la coordinación corresponderá a cada Departamento de adscripción.

El Instituto Aragonés de Gestión Ambiental, Organismo Público con naturaleza jurídica de Entidad de Derecho Público, ejerce las competencias para la tramitación, resolución y emisión de informes en relación con las materias de contenido ambiental detalladas en el artículo 3 de la Ley 10/2013, de 19 de diciembre. No obstante, las competencias en materia de vigilancia, control, inspección y sanción respecto de las resoluciones e informes que emite el Instituto



Aragonés de Gestión Ambiental corresponde a los órganos integrados en la estructura administrativa del Departamento competente en materia de medio ambiente, ya sean Servicios Provinciales o Direcciones Generales.

Por otra parte, la entidad de derecho público Aragonesa de Servicios Telemáticos – AST – que tiene como objetivos generales el cumplimiento y ejecución de las directrices estratégicas del Gobierno de Aragón en materia de servicios y sistemas corporativos de información y de telecomunicación, actúa como proveedor principal ante la administración de la Comunidad Autónoma de Aragón para la cobertura global de las necesidades de ésta en relación con los servicios, sistemas y aplicaciones para la información y las telecomunicaciones.

Así, AST, en el ámbito de la seguridad propone, implanta y coordina 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 por ende, de INAGA.

Asimismo, también resulta procedente que el Instituto Aragonés de Gestión Ambiental quede subrogado en la política de seguridad del Departamento al que se encuentra adscrito (Departamento de Desarrollo Rural y Sostenibilidad) de modo que las medidas de seguridad que se aplican al Departamento sean de obligado cumplimiento para el INAGA.

En este contexto, el Instituto Aragonés de Gestión Ambiental, en el mismo marco que el resto de los órganos y entidades dependientes de la Administración de la Comunidad Autónoma de Aragón - sobre la base de la Ley 7/2001, de 31 de mayo, de creación de la entidad pública AST, así como del Convenio de colaboración entre la Administración de la Comunidad autónoma de Aragón y la entidad de derecho público Aragonesa de Servicios Telemáticos, al que se dio publicidad mediante Resolución de 10 de diciembre de 2002 de la Dirección General de Organización, Inspección y Servicios - quedan reguladas las relaciones entre el responsable de datos y el encargado de tratamiento de datos a los efectos de lo dispuesto en el artículo 28 del RGPD, de modo que AST tiene la consideración de encargado e INAGA la consideración de responsable. A tal efecto, podrá instrumentarse dicha relación de una forma más concreta y particular para el caso que nos ocupa en el documento que formalicen ambas entidades de derecho público.

Los criterios aprobados en materia de protección de datos y de la seguridad de la información es el documento base mediante el cual se define el marco de referencia que permite la gestión de la protección de datos y de la seguridad de la información en el contexto de las actividades de tratamiento con datos de carácter personal y los sistemas de información del Instituto Aragonés de Gestión Ambiental.

El Reglamento General de Protección de Datos dispone que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del citado Reglamento. Así, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

En este sentido, el artículo 24 del RGPD establece como obligaciones generales del responsable del tratamiento y del encargado del tratamiento la aplicación de las medidas técnicas y

organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento. Entre las medidas mencionadas se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

La Ley 39/2015 ya citada recoge también en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas.

La Ley 40/2015 igualmente citada establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos, y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la indicada Ley 40/2015 cita el Esquema Nacional de Seguridad, regulado mediante Real Decreto 3/2000, de 8 de enero, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, y que establece los principios básicos y requisitos mínimos que permitan una protección adecuada de la información y tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación.

El Real Decreto 3/2010 exige en su artículo 11 que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá de acuerdo con los principios básicos (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.

Mediante Decreto 51/2010, de 13 de abril, del Gobierno de Aragón, por el que se crean los ficheros de datos de carácter personal de la entidad de derecho público Instituto Aragonés de Gestión Ambiental, el citado organismo público daba cumplimiento a lo dispuesto en materia de protección de datos de carácter personal.

No obstante, la entrada en vigor del RGPD con fecha 25 de mayo de 2018 exige que el Instituto Aragonés de Gestión Ambiental apruebe los criterios en materia de protección de datos a fin de garantizar y poder demostrar que los tratamientos que lleva a cabo son conformes al citado Reglamento, quedando desplazado y superado lo regulado en el citado Decreto 51/2010.

La presente Resolución, dictada de acuerdo con las competencias que dispone el artículo 8 de la Ley 10/2013, de 19 de diciembre, del Instituto Aragonés de Gestión Ambiental, tiene la finalidad de aprobar los criterios en materia de protección de datos de carácter personal y seguridad de la información del Instituto Aragonés de Gestión Ambiental, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

En su virtud, dispongo:

Artículo 1.- Objeto y ámbito de aplicación.

1. Constituye el objeto de la presente Resolución la aprobación de los criterios en materia de protección de datos de carácter personal y de seguridad de la información en el marco de



los sistemas de información y de las actividades de tratamiento con datos de carácter personal del Instituto Aragonés de Gestión Ambiental (en adelante INAGA).

2. El contenido de la presente Resolución será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable el INAGA.
3. La presente Resolución será de obligado cumplimiento para todas las unidades que conforman la estructura del INAGA y para todo el personal con acceso a la información de la que es responsable INAGA con independencia de su destino, condición laboral o relación por la que se accede a la información. Asimismo, la presente Resolución será también de obligado cumplimiento para todo el personal de la Administración de la Comunidad Autónoma de Aragón que tenga acceso a los registros y aplicaciones informáticas de INAGA.
4. La presente Resolución afectará a la información y datos personales tratados por medios electrónicos y en soporte en papel que el INAGA gestiona en el ámbito de sus competencias. Esta información se define según las siguientes normas:
 - a. La información con datos personales estará regulada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo en cuanto no contradigan el citado RGPD o por la normativa de derecho interno que reemplace en el futuro a dichas normas.
 - b. La información contenida en los sistemas de información en el ámbito de la administración electrónica queda regulada por el Real Decreto 3/2000, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Artículo 2.- Misión y objetivos del INAGA.

1. El Instituto Aragonés de Gestión Ambiental – INAGA - es un organismo público de la Administración de la Comunidad autónoma de Aragón, regulado en la Ley 10/2013, de 19 de diciembre, competente para la tramitación, resolución y emisión de informes de los procedimientos que, con carácter general se le atribuyan en relación con las siguientes materias:
 - a) Evaluación ambiental y evaluación de impacto ambiental.
 - b) Autorización ambiental integrada y calificación ambiental de actividades clasificadas.
 - c) Residuos y sistemas integrados de gestión, emisiones a la atmósfera, incluidos los gases efecto invernadero.
 - d) Actividades y usos sujetos a intervención administrativa en espacios que se encuentren sometidos a cualquier régimen de protección ambiental.
 - e) Actividades y usos que afecten a especies de flora y fauna con figuras de protección.
 - f) Caza y pesca, y usos y actividades que afecten a la fauna cinegética y piscícola.

- g) Informes sobre afecciones ambientales en general, incluidos en procedimientos de las diferentes legislaciones sectoriales.
 - h) Aplicación de reglamentos comunitarios destinados a la obtención de certificaciones ambientales.
 - i) Informes de evaluación de cumplimiento ambiental asociados a verificaciones de inversiones y otras evaluaciones fiscales o financieras.
2. Los objetivos y fines generales del Instituto Aragonés de Gestión Ambiental – INAGA – son, entre otros, los siguientes:
- a. Mejorar la calidad de la prestación de los servicios de la administración ambiental.
 - b. Conseguir mayor economía, eficiencia y eficacia en la gestión medioambiental autonómica.
 - c. Promover e impulsar la participación pública en la toma de decisiones en materia de medio ambiente dentro de su ámbito competencial.
 - d. Agilizar y simplificar la tramitación de los procedimientos administrativos de contenido ambiental.
 - e. Fomentar la divulgación de la información ambiental, especialmente la relativa a su ámbito competencial.
3. En todo caso el INAGA no ejercerá en ningún caso competencias en materia de vigilancia, control, inspección y sanción respecto de las resoluciones administrativas e informes que emita.

Artículo 3.- Marco normativo.

El Instituto Aragonés de Gestión Ambiental desarrolla sus funciones en el marco normativo de protección de datos y de la administración electrónica que se detalla a continuación:

- a) Reglamento General de Protección de Datos (Reglamento UE 2016/679).
- b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como las normas que pudieran reemplazarlas en el futuro.
- c) Ley 10/2013, de 19 de diciembre, del Instituto Aragonés de Gestión Ambiental.
- d) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- f) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- g) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- h) Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y buen gobierno.
- i) En general, la normativa en materia de administración electrónica, registro telemático y de seguridad de la información que resulte aplicable a las Administraciones Públicas.

Artículo 4.- Principios de protección de datos y seguridad de la información.

- 1. El INAGA tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:



- a. Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.
- b. Legitimación en el tratamiento de datos personales: solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.
- c. Limitación de la finalidad: los datos de carácter personal 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 de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- e. Exactitud: los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán 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 de carácter personal serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento.
- g. Integridad y confidencialidad: los datos de carácter personal 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 aquel.
- h. Responsabilidad proactiva: el INAGA será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento.
- i. Atención a los derechos de los afectados: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.
- j. Alcance estratégico: la protección de datos y la seguridad de la información de INAGA debe estar coordinada e integrada con el resto de iniciativas estratégicas del Gobierno de Aragón para conformar un todo coherente y eficaz.
- k. Responsabilidad diferenciada: en los sistemas de información cuya responsabilidad corresponda a INAGA se observará el principio de responsabilidad diferenciada de modo que se delimiten las siguientes responsabilidades y roles:
 - i. Responsable del tratamiento: determina los fines y medios del tratamiento.
 - ii. Encargado de tratamiento: trata datos personales por cuenta del responsable del tratamiento.
 - iii. Delegado de protección de datos: informa y asesora al responsable del tratamiento de las obligaciones en materia de cumplimiento del RGPD.
 - iv. Responsable de la información: determina los requisitos de seguridad de la información tratada.
 - v. Responsable del servicio: determina los requisitos de seguridad de los servicios prestados.
 - vi. Responsable del sistema: tiene la responsabilidad sobre la prestación de los servicios.
 - vii. Responsable de seguridad de la información: determina las decisiones para satisfacer los requisitos de seguridad.

- l. Seguridad integral: la seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural.
 - m. Gestión de Riesgos: la gestión del riesgo es el conjunto de actividades coordinadas que el INAGA desarrolla para dirigir y controlar el riesgo, entendiéndose como riesgo el efecto de la incertidumbre sobre la consecución de los objetivos que, en el marco del RGPD, es la protección de los derechos y libertades de los titulares de los datos que trata el INAGA. El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información del INAGA, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo el INAGA tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.
 - n. Proporcionalidad: el INAGA establecerá medidas de protección, detección y recuperación de forma que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.
 - o. Proceso de verificación: el INAGA implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.
 - p. Protección de datos y seguridad desde el diseño: el INAGA promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se tratará de aplicar desde el diseño inicial de los sistemas de información.
 - q. Protección de datos por defecto: el INAGA promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen la protección de datos por defecto.
2. Las directrices fundamentales de protección de datos y seguridad de la información se concretan en un conjunto de principios particulares y responsabilidades específicas que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la presente Resolución y que inspiran las actuaciones de INAGA en dicha materia. Se establecen los siguientes:
 - a. Registro de actividades de tratamiento y gestión de activos de información: se utilizará Notif_LOPD como herramienta en la que mantener actualizado el Registro de actividades de tratamiento. Notif_LOPD expondrá la información de forma que pueda ser pública en la página web del INAGA. Asimismo, los activos de información se encontrarán inventariados y categorizados y estarán asociados a un responsable.



- b. Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información y a los datos de carácter personal, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
- c. 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.
- d. Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las 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.
- e. 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. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- f. 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.
- g. Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en el RGPD, de los incidentes de seguridad.
- h. Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- i. Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos de carácter personal.

3.- En todo caso, todas las directrices, criterios, decisiones y actuaciones en materia de protección de datos de carácter personal y de seguridad de la información del INAGA deberán cumplir la política de protección de datos de carácter personal y de seguridad de la información fijada con carácter general por el Gobierno de Aragón y, en particular, la fijada por el Departamento de Desarrollo Rural y Sostenibilidad en el marco del Organismo Pagador de Aragón.

Artículo 5.- Registro de actividades de tratamiento.

El INAGA mantendrá actualizado el registro de las actividades de tratamiento con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del RGPD.

El registro de actividades de tratamiento se mantendrá continuamente actualizado y podrá consultarse en la página web del INAGA.

Artículo 6.- Análisis de riesgos, evaluación de impacto en la protección de datos y gestión de los riesgos de seguridad de la información.

1. Cuando la información contenga datos de carácter personal, se estará igualmente a lo señalado en el artículo siguiente y se llevará a cabo, con la periodicidad que determine el responsable de la información, un análisis de riesgos que permita identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleve a cabo el INAGA, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento. Además, el INAGA llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.
2. La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.
El Responsable de Seguridad es el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.
El Responsable de la información y los responsables de los Servicios son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.
3. Para el análisis y gestión de riesgos se utilizarán las herramientas facilitadas por el Centro Criptológico Nacional, PILAR o las que estén a disposición o se desarrollasen en el futuro, así como las guías, recomendaciones y herramientas elaboradas por la Agencia Estatal de Protección de Datos, así como aquellas que sean proporcionadas por el Gobierno de Aragón como Notif_LOPD.

Artículo 7.- Notificación de violaciones de seguridad de los datos de carácter personal.

El INAGA adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse a través del procedimiento establecido al efecto, de conformidad con lo dispuesto en el artículo 33 del RGPD.

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, conforme a lo dispuesto en el artículo 34 del RGPD.

Artículo 8.- Revisión y auditoría.

El INAGA llevará a cabo de forma periódica cuando lo determine el responsable de la información y del tratamiento, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

La decisión del responsable de la información y del tratamiento para realizar una auditoría en el sentido expuesto en el párrafo anterior, deberá contar en todo caso con la previa conformidad de



Aragonesa de Servicios Telemáticos y del Departamento de Desarrollo Rural y Sostenibilidad habida cuenta la subrogación de INAGA en la política de seguridad del Sistema de Gestión de Seguridad de la Información del citado Departamento.

Artículo 9.- Estructura organizativa.

1. La estructura organizativa interna para la gestión de la seguridad de la información en el ámbito del Instituto Aragonés de Gestión ambiental está compuesta por los siguientes agentes:
 - a. El Comité de Seguridad de la Información.
 - b. El Responsable de la Información
 - c. El Responsable de Seguridad de la información.
 - d. El responsable del Servicio
 - e. El Responsable del Sistema
 - f. El Delegado de la Protección de Datos.
2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir el contenido de la presente Resolución.
3. El nombramiento de los agentes indicados en el apartado 1 de este artículo se realizará mediante Resolución del Presidente del Instituto Aragonés de Gestión Ambiental. La designación del Delegado de la Protección de Datos se notificará a la Agencia Estatal de Protección de Datos, a la Secretaría General Técnica del Departamento de Desarrollo Rural y Sostenibilidad, y a la Dirección General de Administración Electrónica y Sociedad de la Información del Gobierno de Aragón.

Artículo 10.- El Comité de Seguridad de la Información.

1. El Comité de Seguridad de la Información es un órgano colegiado de los previstos en el artículo 20 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que gestionará y coordinará a nivel interno todas las actividades en materia de protección de datos y la seguridad de los sistemas de información. En todo caso, en el desarrollo de sus funciones y competencias seguirá rigurosamente las pautas e indicaciones que se dicten por el Departamento de Desarrollo Rural y Sostenibilidad en el marco del Sistema de Gestión de Seguridad de la Información del indicado Departamento.
2. El Comité de Seguridad de la información actuará en el ámbito del cumplimiento de las medidas a las que se refiere el RGPD, la Ley Orgánica 3/2018, el Real Decreto 3/2010 y el Real Decreto 951/2015.
3. El Comité de Seguridad está compuesto por los siguientes miembros:
 - a. El Responsable de la Información, que ostentará la condición de Presidente.
 - b. El Responsable de seguridad de la información en calidad de coordinador del Comité y que actuará como Secretario.
 - c. El Responsable del Sistema.
 - d. El delegado de protección de datos participará con voz pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a

abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.

4. El Comité de Seguridad de la información coordinará las actividades relacionadas con la seguridad de la información y los sistemas de información ejerciendo las siguientes funciones:
 - a. Establecer criterios para el procedimiento de análisis de riesgos y elaborar propuestas de niveles de riesgos aceptables para seguridad de la información del INAGA.
 - b. Promover ante el Presidente del INAGA la aprobación de normas y procedimientos para garantizar la seguridad de la información.
 - c. Facilitar recursos y medios para la concienciación y formación en materia de seguridad de la información a todo el personal del INAGA.
 - d. Participar en la toma de decisiones que garanticen la seguridad de la información y los servicios del INAGA.

Artículo 11.- El responsable de la información.

1. La condición de responsable de la información recae en la Dirección del INAGA que tendrá asimismo la condición de responsable de los tratamientos llevados a cabo por el propio Instituto. La aprobación de los criterios en materia de protección de datos y seguridad de la información corresponde al Presidente del INAGA habida cuenta su condición de máximo responsable del Instituto.
2. Son funciones del responsable de la información:
 - a. La aprobación formal de los niveles y medidas de seguridad de la información, a propuesta del Comité de Seguridad de la Información y según lo indicado por el Departamento de Desarrollo Rural y Sostenibilidad, dentro del marco de lo previsto en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
 - b. La aprobación, a propuesta del Comité de Seguridad de la Información, de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las y según lo indicado por el Departamento de Desarrollo Rural y Sostenibilidad personas, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, conforme a lo exigido en el RGPD.

Artículo 12.- El responsable de seguridad de la información.

1. El responsable de seguridad de la información es la persona a la que corresponde la toma de decisiones necesarias para satisfacer los requisitos exigibles para garantizar la seguridad de la información y la seguridad en el tratamiento de datos de carácter personal. Desarrollará su actividad en lo que respecta al cumplimiento de las medidas a las que se refieren la ley Orgánica 3/2018, y el Reglamento General de Protección de Datos o por la normativa de derecho interno que reemplace en el futuro a dichas normas, así como el Real Decreto 3/2010.
2. Son funciones del responsable de seguridad de la información del INAGA las siguientes:



- a. Promover la seguridad de la información entre el personal del INAGA.
- b. El mantenimiento de la mejora continua de la seguridad de la información.
- c. La elaboración de procedimientos y normativa de seguridad que serán presentados al Comité de Seguridad para su revisión y aprobación.
- d. El impulso y la realización de análisis de riesgos sobre los sistemas de información del INAGA.
- e. La coordinación de las actuaciones en materia de seguridad de la información entre las unidades y Áreas que explotan la información y los responsables de los servicios del INAGA.
- f. La coordinación y control del cumplimiento de las medidas de seguridad definidas en los documentos y normas que desarrollen la presente política.
- g. La gestión de las incidencias de seguridad de la información que se produzcan informando de las más relevantes al Comité de Seguridad y a los responsables de las unidades del INAGA afectadas por las incidencias.

3.- En todo caso, en el desarrollo de sus funciones y competencias seguirá rigurosamente las pautas e indicaciones que se dicten por el Departamento de Desarrollo Rural y Sostenibilidad en el marco del Sistema de Gestión de Seguridad de la Información del indicado Departamento.

Artículo 13.- Responsable del servicio.

- 1.- Las funciones de Responsable de Servicio recaerán en las personas titulares de las Áreas temáticas del INAGA que gestionen cada procedimiento administrativo y en el Director del propio Instituto.
- 2.- El responsable del servicio, dentro de su ámbito y Área, establecerá los requisitos del servicio y los niveles de seguridad del mismo dentro del marco que establece el anexo I del Real Decreto 3/2010.
- 3.- En todo caso, en el desarrollo de sus funciones y competencias seguirán rigurosamente las pautas e indicaciones que se dicten por el Departamento de Desarrollo Rural y Sostenibilidad en el marco del Sistema de Gestión de Seguridad de la Información del indicado Departamento.

Artículo 14.- Responsable del sistema.

- 1.- El responsable del Sistema será el encargado del desarrollo, el funcionamiento y el mantenimiento de los sistemas de información durante su ciclo de vida completo, así como elaborar los procedimientos, guías e instrucciones técnicas que, cumplimiento con lo establecido en la presente Resolución, determinan las acciones o tareas a realizar en el desempeño de un proceso.
- 2.- En todo caso, en el desarrollo de sus funciones y competencias seguirá rigurosamente las pautas e indicaciones que se dicten por el Departamento de Desarrollo Rural y Sostenibilidad en el marco del Sistema de Gestión de Seguridad de la Información del indicado Departamento.

Artículo 15.- El delegado de protección de datos.

El INAGA cuenta con un delegado de protección de datos, designado por Resolución del Presidente del Instituto Aragonés de Gestión Ambiental, a fin de dar cumplimiento a lo requerido en el artículo

37 del RGPD, que llevará a cabo las tareas establecidas en el artículo 39 del RGPD, así como las que se deriven de la normativa española de protección de datos de carácter personal y de los documentos de buenas prácticas que se adopten por la Agencia Española de Protección de Datos, en su condición de autoridad de control, o por el Comité Europeo de Protección de Datos.

En el desempeño de sus tareas el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento.

Artículo 16.- Asignación de tareas.

La dirección del INAGA, el Comité de Seguridad, el responsable de seguridad y el delegado de protección de datos de la información podrán, dentro de su respectivo ámbito, asignar tareas relativas a la mejora de los principios recogidos en la presente política a personas o grupos de trabajo. En la asignación de tareas se tendrá en cuenta a todo el personal que presta sus servicios en el INAGA y a especialistas externos cuando sea necesario.

Artículo 17.- Obligaciones del personal

Todas las unidades y Áreas del INAGA prestarán su colaboración en el cumplimiento de la presente Resolución.

Asimismo, todas las personas que presten servicio en el INAGA, directamente formando parte de su plantilla, o bien mediante contratos de servicio o encargos de servicios, tienen la obligación de conocer y cumplir lo previsto en la presente Resolución, así como en las normas y procedimientos que la desarrollen.

Todo el personal que presta servicio en el INAGA deberá colaborar en la mejora de los principios y requisitos en materia de protección de datos y seguridad de la información evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es titular el INAGA.

Artículo 18.- Formación.

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que presta sus servicios en el INAGA, así como a la difusión entre los mismos de la presente Resolución.

El INAGA dispondrá los medios necesarios para que todas las personas con acceso a la información sean informadas acerca de sus deberes y obligaciones, así como de los riesgos existentes en el tratamiento de la información.

El delegado de protección de datos supervisará las acciones de concienciación y formación del personal que participa en las operaciones de tratamiento con datos personales, a fin de garantizar el cumplimiento de la presente Resolución.

Artículo 19.- Desarrollo normativo y revisión de la PPDSI.



1. Corresponderá a la Dirección del INAGA, a propuesta del Comité de Seguridad de la información y, cuando proceda, por el delegado de protección de datos, la adopción de los procedimientos, guías e instrucciones técnicas necesarios para el desarrollo de la presente Resolución.
2. En el proceso de desarrollo normativo podrá requerirse la colaboración de las unidades organizativas que componen la estructura orgánica del INAGA.
3. La presente Resolución se someterá a un proceso de revisión que la Dirección considere oportuna a fin de adaptarse a las circunstancias técnicas u organizativas y evitar su obsolescencia.

Disposición adicional primera. - Subrogación de INAGA en la política de seguridad de Aragonesa de Servicios Telemáticos y del Departamento de Desarrollo Rural y Sostenibilidad.

Los activos TIC de INAGA están alojados en los servidores corporativos de Aragonesa de Servicios Telemáticos –AST-. Asimismo, los activos microinformáticos, de redes de telecomunicaciones y demás activos hardware y software corporativos son provistos y gestionados por AST, de modo que INAGA se subroga en la política de seguridad de AST.

INAGA se subroga también en la política de seguridad del Departamento al que se encuentra adscrito (Departamento de Desarrollo Rural y Sostenibilidad) habida cuenta que, por decisión del Secretario General Técnico del Departamento, Director del Organismo Pagador, el sistema de gestión de seguridad de la información del citado organismo se extiende a todo el Departamento, de modo que las medidas de seguridad que se aplican al Departamento abarcan igualmente al INAGA.

Disposición adicional segunda. - Datos de carácter personal incorporados en herramientas de gestión y aplicaciones informáticas de carácter corporativo del Gobierno de Aragón.

En relación a las aplicaciones informáticas del Gobierno de Aragón, SIRGHGA, SERPA, entre otras, de las que sean responsable de su tratamiento los respectivos Departamentos del Gobierno de Aragón competentes en cada materia, el Instituto Aragonés de Gestión Ambiental ostentará al respecto, únicamente la condición de usuario de dichas aplicaciones a efectos de realizar la gestión oportuna en cada una de ellas.

Disposición adicional tercera. - Encargado de tratamiento a efectos del RGPD.

Con carácter general la condición de encargado de tratamiento de los datos de carácter personal de los que disponga el Instituto Aragonés de Gestión Ambiental en el marco de sus competencias corresponderá a la entidad de derecho público Aragonesa de Servicios Telemáticos –AST- habida cuenta que los activos TIC de INAGA se encuentran alojados en servidores corporativos de AST. No obstante, podrá extenderse también la condición de encargado de tratamientos al propio INAGA en el ejercicio de sus competencias cuando corresponda.

Según lo dispuesto en el artículo 28 del RGPD la condición de encargado de tratamiento de AST se instrumentará, en su caso, en un documento formalizado entre el Instituto Aragonés de Gestión Ambiental (RESPONSABLE) y Aragonesa de Servicios Telemáticos (ENCARGADO DE TRATAMIENTO) que recogerá el régimen de derechos y obligaciones a que se sujetarán ambas partes.

Disposición adicional cuarta. - Equipo de Administración Electrónica de INAGA.

Se crea el Equipo de Administración Electrónica del Instituto Aragonés de Gestión Ambiental, integrada por los siguientes funcionarios de la Secretaría General del Instituto:

- Técnico de Gestión de la Información
- Analista-Programador
- Técnico de Gestión General

El Equipo de Administración Electrónica de INAGA tendrá como objetivo facilitar a la Unidad de Apoyo a Administración Electrónica y Gobernanza de los datos del Departamento de Desarrollo Rural y Sostenibilidad, y a la Unidad de Protección de Datos del Gobierno de Aragón toda la colaboración necesaria para desarrollar las acciones pertinentes en materia de protección de datos y seguridad de la información.

Disposición adicional quinta. - Publicidad y aplicación.

De conformidad con lo dispuesto en el artículo 6 de la Ley 40/2015, de 1 de octubre del régimen Jurídico del Sector Público, a los efectos de garantizar el cumplimiento de los principios de transparencia, publicidad y concurrencia, la presente Resolución se hará pública mediante su inserción en la página web del Instituto Aragonés de Gestión Ambiental.

El contenido de la presente Resolución será de aplicación desde el día de la fecha de su firma por el Presidente del Instituto Aragonés de Gestión Ambiental.

En Zaragoza, a fecha de firma electrónica
JOAQUÍN OLONA BLASCO,
Presidente del Instituto Aragonés de Gestión Ambiental.