GOBIERNO DE ARAGON

Departamento de Agricultura, Ganadería y Alimentación

ORGANISMO PAGADOR DEL GOBIERNO DE ARAGÓN - DEPARTAMENTO DE AGRICULTURA, GANADERÍA Y ALIMENTACIÓN

Política de seguridad de la información
Código OP-POL-PolíticaSeguridad

Versión: 19.0
Fecha: 24/10/2023

CLASIFICACIÓN:

Público

APROBACIÓN:

Nombre: ***D. Luis Francisco Biendicho Gracia***
Cargo: ***Director del Organismo Pagador***

Nombre: ***D. Ángel Sanz Barea***
Cargo: ***Director Gerente de AST***

Nombre: ***D. Carlos Calvo Gracia***
Cargo: ***Director General de Producción Agraria***

Nombre: ***D.ª Rosa M.ª Charneca Quílez***
Cargo: ***Directora General de Desarrollo Rural***

Nombre: ***D. Julio Borque Almajano***
Cargo: ***Jefe del SATPI***

Control de cambios del documento:

Referencia	Fecha	Autor	Descripción
1.0	23/12/2005	Equipo de redacción	Borrador.
2.0	30/12/2005	Organismo Pagador	Aprobación.
3.0	15/02/2006	Organismo Pagador	Incorporación de seguridad personal.
4.0	07/05/2007	Organismo Pagador	Borrador de la revisión anual. Incorporación de referencias y anexo. Actualización de cabecera e introducción.
	03/09/2007	Organismo Pagador	Aprobación de la revisión anual.
5.0	01/09/2008	Organismo Pagador	Cambio de denominación de la ISO 17799 a 27002. Aprobación de la revisión anual.
6.0	23/02/2010	Organismo Pagador	Actualización de la legislación sobre protección de datos personales. Aprobación de la revisión anual.
7.0	05/09/2011	Organismo Pagador	Cambio de departamento. Marco de fijación de objetivos. Referencias al ENS. Aprobación de la revisión anual.
8.0	30/08/2012	Organismo Pagador	Referencias al OP-DAGMA y al SCAPI. Tratamiento de los resultados de las auditorías. Difusión en correo, intranet y formación. Aprobación de la revisión anual.
9.0	19/09/2013	Organismo Pagador	Aprobación de la revisión anual.
10.0	09/10/2014	Organismo Pagador	Aprobación de la revisión anual.
11.0	19/10/2015	Organismo Pagador	Actualización de la 27002. Cambio de nombre del Departamento. Aprobación de la revisión anual.
12.0	02/06/2016	Organismo Pagador	Referencias al SATPI. Mejora continua. Cumplimiento legal. Aprobación de la revisión anual.
12.1	09/09/2016	Organismo Pagador	Paso de restringida a pública. Partes interesadas.
13.0	16/06/2017	Organismo Pagador	Aprobación de la revisión anual.

13.1	**15/11/2017**	**Organismo Pagador**	**Detalle de legislación aplicable.**
14.0	**20/08/2018**	**Organismo Pagador**	**Inclusión de más partes interesadas.** **Aprobación de la revisión anual.**
15.0	**21/08/2019**	**Organismo Pagador**	**Cambio de nombre del Departamento.** **Actualización de la legislación sobre datos personales.** **Aprobación de la revisión anual.**
16.0	**25/08/2020**	**Organismo Pagador**	**Leyes de propiedad intelectual y de firma electrónica.** **Aprobación de la revisión anual.**
17.0	**20/08/2021**	**Organismo Pagador**	**Necesidades y expectativas de las partes interesadas.** **Legislación de administración electrónica.** **Aprobación de la revisión anual.**
18.0	**25/8/2022**	**Organismo Pagador**	**Nuevo ENS y RD 203/2021.** **Aprobación de la revisión anual.**
19.0	**24/10/2023**	**Organismo Pagador**	**Cambio de nombre del Departamento.** **Aprobación de la revisión anual.**

Lista de distribución:

- Organismo Pagador del Gobierno de Aragón – Departamento de Agricultura, Ganadería y Alimentación

ÍNDICE

1 INTRODUCCIÓN

Mediante el Decreto 167/2006, de 18 de julio, del Gobierno de Aragón, se constituye el Organismo Pagador de los gastos imputables al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER) en la Comunidad Autónoma de Aragón y se establece su organización y funcionamiento.

El Decreto 25/2020, de 26 de febrero, del Gobierno de Aragón, por el que se aprueba la estructura orgánica del Departamento de Agricultura, Ganadería y Medio Ambiente, indica que corresponde al citado departamento la actuación como Organismo Pagador de los gastos imputables al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER) en la Comunidad Autónoma de Aragón.

El Decreto de 11 de agosto de 2023, del Presidente del Gobierno de Aragón, por el que se modifica la organización de la Administración de la Comunidad Autónoma de Aragón y se asignan competencias a los departamentos, especifica que:

- Al Departamento de Agricultura, Ganadería y Alimentación se le atribuyen las competencias del anterior Departamento de Agricultura, Ganadería y Medio Ambiente en producción agraria, desarrollo rural, promoción e innovación agroalimentaria, caza y pesca, así como en calidad y seguridad alimentaria.

- Al Departamento de Medio Ambiente y Turismo se le atribuyen las competencias del anterior Departamento de Agricultura, Ganadería y Medio Ambiente sobre cambio climático, educación ambiental, planificación y control ambiental, suelos contaminados, medio natural y gestión forestal.

Por lo tanto, ambos departamentos comparten actualmente la actuación como Organismo Pagador de los citados fondos.

Los procesos necesarios para gestionar las distintas líneas de ayuda con cargo a estos fondos agrarios dependen cada vez más de distintos sistemas de información, que permiten la automatización de las principales tareas. El marco normativo cambiante, la interrelación de múltiples sistemas heterogéneos y la propia complejidad de estos procesos hacen necesario un especial control sobre los procedimientos que permiten el desarrollo, mantenimiento y gestión de estos sistemas de información.

La Dirección del Organismo Pagador considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Asume, por lo tanto, la seguridad de la información como una responsabilidad asociada a la protección de la información (incluyendo también los sistemas que la procesan, la infraestructura tecnológica soporte y las instalaciones desde las que se realiza ese tratamiento) de las amenazas que puedan afectar a su integridad, disponibilidad y/o confidencialidad.

En el punto 3. B) del anexo I del Reglamento Delegado (UE) n.° 907/2014 de la Comisión, de 11 de marzo de 2014, se establecen los criterios necesarios para la autorización de los organismos pagadores en lo que se refiere a la seguridad de sus sistemas de información:

> *i) Sin perjuicio del inciso ii) siguiente, la seguridad de los sistemas de información estará basada en los criterios fijados en una versión aplicable en el ejercicio financiero considerado de una de las siguientes normas:*
>
> - *International Standards Organisation 27002: Code of practice for Information Security management (Organización internacional de normalización 27002: Código de prácticas para la gestión de la seguridad de la información) (ISO),*
> - *Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch/IT Baseline Protection Manual (Manual de protección informática de base) (BSI),*
> - *Information Systems Audit and Control Association: Control objectives for Information and related Technology (Asociación para la auditoría y el control de los sistemas de información: Objetivos de control para la información y tecnologías afines) (COBIT).*
>
> *ii) A partir del 16 de octubre de 2016, la seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001: Information Security management systems – Requirements (ISO) (Sistemas de gestión de la seguridad de la información-Requisitos) (ISO).*
>
> *La Comisión podrá autorizar a los Estados miembros para certificar la seguridad de sus sistemas de información de conformidad con otras normas aceptadas si estas normas garantizan un nivel de seguridad equivalente, como mínimo, al previsto en la norma ISO 27001.*
>
> *En el caso de los organismos pagadores responsables de la gestión y control de un gasto de la Unión anual no superior a 400 millones EUR, el Estado miembro podrá decidir no aplicar lo dispuesto en el párrafo primero. Dichos Estados miembros seguirán aplicando las disposiciones del inciso i). Informarán a la Comisión de su decisión.*

El Organismo Pagador de Aragón consciente de la importancia de la seguridad de la información (y en línea con los requerimientos derivados de la normativa comunitaria), adoptó el estándar ISO 27002 como el marco general para la definición de un sistema de gestión de seguridad de la información. Esta decisión se basa en la consideración de la seguridad no como un estado sino como un proceso.

Tal y como señala el Reglamento Delegado (UE) n.° 907/2014, siendo el Organismo Pagador de Aragón responsable de la gestión y control de un gasto de la Unión anual superior a 400 millones de euros, la seguridad de su sistema de información debe estar certificada de conformidad con la norma ISO 27001, y así es desde el 6 de octubre de 2016.

Como parte de toda esta estrategia, la Dirección del Organismo Pagador define, a través de este documento, una política de seguridad de la información, válida igualmente para cumplir con el artículo 12 del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad), que define la política de seguridad formalmente aprobada por el órgano competente con la que habrá de contar cada administración pública

La Dirección del Organismo Pagador, el personal adscrito al mismo, así como aquellos terceros (internos en el ámbito del Gobierno de Aragón o externos) que presten sus servicios en la realización de actividades de gestión o soporte a procesos de gestión de ayudas con cargo a los fondos FEAGA y FEADER están sujetos a los requerimientos que se derivan de esta política de seguridad.

En este sentido, los diferentes agentes con acceso a la información están obligados a conocer esta política (en lo que les pueda afectar) y comprometidos a preservar la seguridad de la información y, en particular, su confidencialidad, integridad y disponibilidad.

Este es un objetivo estratégico[1] alineado con los objetivos generales del Organismo Pagador y las funciones del mismo, dado que constituye un instrumento básico para prevenir y perseguir las irregularidades que afecten a la realidad y regularidad de las operaciones financiadas por fondos FEAGA y FEADER.

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, incluidos los organismos públicos adscritos, por lo que las medidas de seguridad que se aplican al primero abarcan igualmente al segundo. En la documentación de seguridad se hace referencia al OP-DAGA: Organismo Pagador-Departamento de Agricultura, Ganadería y Alimentación.

2 ÁMBITO DE APLICACIÓN

El ámbito de aplicación de la política de seguridad es especialmente el asociado a la prestación de los siguientes procesos:

- Gestión de ayudas: recepción, registro y tramitación de las solicitudes hasta su resolución.
- Autorización de pagos: determinación de la cantidad que debe ser pagada a cada solicitante de acuerdo con la normativa comunitaria.
- Ejecución de los pagos: emisión de una instrucción de pago, dirigida a la Tesorería General del Gobierno de Aragón, para el pago de la cantidad autorizada al solicitante.
- Contabilidad: registro del pago en los libros de contabilidad del organismo y preparación de las cuentas recapitulativas de gastos para la Comisión.

[1] La Dirección del Organismo Pagador, a través de la aprobación de este documento, establece el compromiso específico de implantar la política, alinear la operativa con las directrices que se derivan de la misma y promover el cumplimiento efectivo de los diferentes agentes que acceden a la información.

Adicionalmente, también se consideran dentro del ámbito de aplicación de esta política los aspectos que puedan incidir en la preparación de cualquier otra información para el Órgano de Coordinación y para la Comisión Europea.

La Dirección del Organismo Pagador, es decir, el Departamento de Agricultura, Ganadería y Alimentación y, en su caso, el Secretario General Técnico, son los máximos responsables de promover la aplicación efectiva[2] de la política de seguridad en este ámbito.

3 PARTES INTERESADAS

En el sistema de gestión de seguridad de la información del OP-DAGA se determinan las siguientes partes interesadas relevantes con los correspondientes requisitos relacionados con ellas, así como sus necesidades y expectativas:

- Empleados del Departamento de Agricultura, Ganadería y Alimentación: Normativa sobre la función pública y legislación laboral aplicable al personal del Gobierno de Aragón, tanto nacionales como autonómicas, y normativa sobre las obligaciones del personal (OP-NOR-ObligacionesPersonal). Necesidades y expectativas: cumplir con un trabajo que les permita vivir dignamente, y opcionalmente con la posibilidad de realizarse a través de él.

- Personal contratado: Contratos con las empresas correspondientes basados en el procedimiento de externalización de trabajos (OP-PROC-ExternalizaciónTrabajos) y normativa sobre las obligaciones del personal (OP-NOR-ObligacionesPersonal). Necesidades y expectativas: cumplir con un trabajo que le permita vivir dignamente, y opcionalmente con la posibilidad de realizarse a través de él.

- Aragonesa de Servicios Telemáticos (AST): Ley 7/2001, de 31 de mayo, de creación de la Entidad Pública Aragonesa de Servicios Telemáticos y procedimiento de interacción con AST y seguimiento de los servicios prestados (OP-PROC-InteracciónAST). Necesidades y expectativas: servir adecuadamente al Gobierno de Aragón y progresar tecnológicamente adaptándose a los tiempos.

- Sociedad Aragonesa de Gestión Agroambiental, S. L. U. (SARGA): Decreto 198/2000, de 21 de noviembre, del Gobierno de Aragón, por el que se crea la empresa pública "Sociedad de Infraestructuras Rurales Aragonesa, S. A." (SIRASA) y Decreto 237/2003, de 2 de septiembre, del Gobierno de Aragón, por el que se crea la empresa pública “Sociedad de Desarrollo Medioambiental de Aragón, S. A. (SODEMASA)”, por cuya fusión se constituye como sociedad mercantil autonómica de capital social íntegramente público, suscrito en su totalidad por el Gobierno de Aragón a través de la Corporación Empresarial Pública de Aragón. Necesidades y expectativas: servir adecuadamente al Departamento de Agricultura, Ganadería y Alimentación.

[2] Con el necesario concurso del personal adscrito a la entidad pública Aragonesa de Servicios Telemáticos (AST).

- Proveedores de desarrollo: Contratos basados en el procedimiento de externalización de trabajos (OP-PROC-ExternalizaciónTrabajos). Necesidades y expectativas: cumplir los contratos, obtener rentabilidad y mantener una imagen.

- Fondo Español de Garantía Agraria (FEGA): Real Decreto 1441/2001, de 21 de diciembre, por el que se aprueba el Estatuto del Fondo Español de Garantía Agraria. Necesidades y expectativas: hacer que los fondos europeos asignados a España se apliquen estrictamente a lograr los objetivos de las políticas correspondientes.

- Comisión Europea: Normativa de la Unión Europea sobre los organismos pagadores de los gastos imputables al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER). Necesidades y expectativas: hacer que los fondos europeos se apliquen estrictamente a lograr los objetivos de las políticas correspondientes.

- Entidades colaboradoras: Acuerdos firmados amparados por la normativa para la cesión de *software* y datos a entidades colaboradoras (OP-NOR-CesiónSoftware), tales como entidades bancarias, sindicatos agrarios, cooperativas agrarias, grupos de acción local, etc. Necesidades y expectativas: cumplir los acuerdos, obtener rentabilidad y/o servir adecuadamente a sus clientes o asociados y mantener una imagen.

- Beneficiarios de ayudas: Regulación legal múltiple, tanto nacional como autonómica, de concesión de ayudas. Necesidades y expectativas: cobrar en sus plazos las ayudas que les correspondan.

- Otros administrados: Regulación legal múltiple, tanto nacional como autonómica, de temas diferentes a la concesión de ayudas, en el ámbito ajeno al Organismo Pagador. Necesidades y expectativas: relacionarse con la administración autonómica en los ámbitos legales correspondientes.

- Gobierno de España: Regulación legal nacional múltiple, especialmente el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Necesidades y expectativas: cumplir la ley y mantener una imagen.

- Gobierno de Aragón: Regulación legal autonómica múltiple. Necesidades y expectativas: cumplir la ley y mantener una imagen.

4 DESCRIPCIÓN DE LA POLÍTICA

La Dirección del Organismo Pagador, tras haber seleccionado el estándar ISO 27002[3], ha determinado las directrices generales para la seguridad de la información.

4.1 Marco general para la selección de controles

El análisis de riesgos permite identificar las áreas en las que el OP-DAGA presenta una mayor exposición y, por otra parte, priorizar las líneas de actuación con el fin de minimizar las situaciones de riesgo.

En particular, el análisis de riesgos[4] considerará dos variables:

- La probabilidad del riesgo.
- El impacto que tendría para la organización.

En este sentido, los elementos estructurales con los que abordar el análisis de riesgos son[5]:

- El valor para el OP-DAGA de los diferentes activos (vinculado al impacto del riesgo).
- La probabilidad potencial de ocurrencia de las amenazas que pueden afectar a los activos (vinculado a la probabilidad del riesgo).
- Las vulnerabilidades que un determinado activo presenta y que podrían permitir la materialización de un daño sobre el mismo, si ocurriera la amenaza.

La vulnerabilidad tiene influencia tanto en la probabilidad (según la facilidad de explotación de esa vulnerabilidad) como en el impacto del riesgo (según la gravedad relativa de la vulnerabilidad).

En cualquier caso, la Dirección del Organismo Pagador considera que la relevancia de una determinada vulnerabilidad sobre un activo es inversamente proporcional al nivel de control en ese activo. Es decir, una vulnerabilidad será más grave y/o más fácil de explotar en la medida de que no existan controles preventivos o de detección adecuadamente implantados.

[3] Para más información al respecto, consultar el documento OP-NOR-EstándarAlcance: Procedimiento de selección del estándar y determinación del alcance.

[4] Para más información al respecto, consultar el documento OP-PROC-AnálisisRiesgos: Procedimiento de análisis de riesgos.

[5] En un ejemplo simplificado, podría considerarse un *ordenador personal* como un activo, una amenaza podría ser la *sustracción o robo* y una vulnerabilidad que este ordenador personal esté en un lugar sin ningún tipo de protección que prevenga el acceso no autorizado (i. e.: *puertas abiertas sin control*, etc.).

Por lo tanto, la selección de controles considerará la relevancia en la operativa del OP-DAGA y, específicamente, los resultados del análisis de riesgos realizado por el OP-DAGA.

Periódicamente el OP-DAGA realizará una actualización del análisis de riesgos conforme al procedimiento establecido, que podrá derivar en una revisión de la selección de los controles[6], así como del marco normativo del sistema de gestión de seguridad de la información incluyendo el presente documento de política de seguridad.

4.2 Principios de seguridad

4.2.1 Organización de la seguridad de la información

De cara a mantener una organización adecuada de la seguridad, la Dirección del Organismo Pagador establecerá un Comité de Gestión y Coordinación de la Seguridad, en el que se incluirá representación de las distintas áreas implicadas (Dirección, área técnica, control interno, Servicio de Asistencia Técnica y Procesos Informáticos y AST: Aragonesa de Servicios Telemáticos).

Este Comité se reunirá con la periodicidad definida en su propia reglamentación y los principales cometidos del mismo serán:

- Formulación, revisión y aprobación de la política de seguridad, así como de las metodologías y procedimientos asociados al sistema de gestión de seguridad de la información.
- Aprobar la asignación de responsabilidades específicas dentro de la organización relativas a la seguridad de la información.
- Promover planes y programas de concienciación del personal en esta materia
- Evaluar la idoneidad de los distintos controles de seguridad, facilitar los recursos necesarios y coordinar su implantación efectiva.
- Utilizar el plan general de acción establecido para cada año y la hoja de ruta correspondiente como marco de fijación de los objetivos de seguridad, orientados siempre hacia la mejora continua de la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información.
- Estudiar las no conformidades y observaciones detectadas en las auditorías y preparar las acciones correctoras correspondientes.

En aquellos casos en los que se estime conveniente, este Comité podrá estar asesorado por especialistas en seguridad de la información.

[6] Para más información al respecto, consultar el documento de declaraciones de aplicabilidad de los controles y las medidas (OP-NOR-DeclaracionesAplicabilidad).

4.2.2 Seguridad relativa a los recursos humanos

Con carácter general se arbitrarán mecanismos que permitan fomentar la sensibilización del personal del OP-DAGA en aspectos relacionados con la seguridad de la información. En este sentido el OP-DAGA es consciente que la participación activa de los usuarios en el mantenimiento de un adecuado nivel de seguridad es relevante.

Por otra parte, las bajas de personal como consecuencia de cambios en su adscripción organizativa (o por otros motivos) se gestionarán de acuerdo a los procedimientos y protocolos establecidos.

Adicionalmente, se establecerá un procedimiento de expiración automática de cuentas en los sistemas del OP-DAGA para los usuarios temporales y contratados.

4.2.3 Gestión de activos

La Dirección del Organismo Pagador promoverá el mantenimiento de un inventario de activos[7]. Asimismo, se establecerá un método de valoración de los activos según el impacto que sobre, la operativa del OP-DAGA, pueda tener la materialización de un riesgo que afecte a la integridad, confidencialidad o disponibilidad de la información.

En particular, los activos se clasificarán considerando, al menos, las siguientes categorías:

- Información.
- Programas y aplicaciones.
- Físicos.
- Servicios.

Sobre estos activos se determinará, en función del análisis del entorno (amenazas) y las vulnerabilidades que les apliquen, el nivel de protección a aplicar.

[7] Los activos son los recursos asociados a la información, a los sistemas de información y a la infraestructura tecnológica soporte a dichos sistemas y/o instalaciones necesarios para el correcto funcionamiento del Organismo Pagador. Constituyen el sujeto pasivo sobre los que se aplican los controles o salvaguardas que se definan en función del análisis de riesgos.

4.2.4 Control de acceso

La Dirección del Organismo Pagador ha previsto que los permisos de acceso de los usuarios a la red, sistemas e información se concedan, específicamente, según las necesidades derivadas de sus funciones y responsabilidades. Es decir, cada usuario tendrá acceso, únicamente, a los recursos e información necesarios para el desempeño de las tareas que tenga encomendadas.

La concesión del acceso a los recursos de los sistemas de información (incluida la red) del OP-DAGA llevará asociado un proceso previo formal de solicitud, evaluación y aprobación. Este procedimiento de gestión de accesos considerará también las bajas o modificaciones en los derechos de acceso, así como indicaciones para la gestión de usuarios temporales (i. e. personal externo).

En este sentido, los usuarios (salvo situaciones excepcionales que deberán estar identificadas y aprobadas) dispondrán de un identificador de usuario unívoco. Además, se bloquearán los terminales con un salvapantallas protegido por contraseña que se activará automáticamente transcurrido cierto periodo de inactividad.

Para que un usuario pueda acceder a un determinado sistema de información deberá superar un proceso de identificación (por ejemplo, a través de un identificador de usuario), autenticación[8] (por ejemplo, a través de una contraseña) y autorización (por ejemplo, a través de perfiles o roles que determinen a qué funcionalidades y/o datos tendrán acceso los usuarios). Asimismo, podrán establecerse mecanismos de registro y monitorización de acceso y/o uso de los sistemas. Las credenciales de acceso de cada usuario serán personales e intransferibles y su proceso de asignación y comunicación garantizará su confidencialidad y prevendrá el acceso no autorizado a través de la suplantación de identidad.

Los usuarios serán responsables de preservar la confidencialidad de las contraseñas y asegurar el correcto uso de los sistemas de información y recursos a los que tienen acceso. Además, dado que la información en papel u otros soportes también está sujeta a requerimientos de seguridad, se conservará evitando, en la medida de lo posible, las situaciones de riesgo[9].

Periódicamente (al menos de forma anual) existirá un proceso de revisión por parte de los servicios responsables de la gestión de las diferentes líneas de ayuda para verificar que sólo los usuarios autorizados tienen acceso a los diferentes sistemas de información y aplicaciones. Para garantizar este objetivo, las diferentes aplicaciones permitirán obtener listados actualizados con los usuarios activos (con capacidad para identificarse y autenticarse en el sistema) y sus privilegios de acceso (perfiles o roles asignados). Este proceso incluirá también un estudio de posibles usuarios con roles incompatibles, de acuerdo al modelo de segregación de funciones definido.

[8] En el caso de contraseñas, se establecerá un período de validez de forma que, una vez superado el mismo, el usuario deberá cambiarla.

[9] Por ejemplo, evitando dejar información sensible en lugares de libre acceso a cualquiera que se encuentre en el edificio (como las mesas de trabajo).

Por último, existirá un registro con los usuarios que tienen capacidades de administración sobre los sistemas e infraestructura tecnológica de soporte a la operativa del OP-DAGA. Estos usuarios con amplias capacidades se restringirán al máximo, así como los accesos directos a las bases de datos. La Dirección del Organismo Pagador podrá consultar (según los procedimientos específicos que pudieran definirse) qué actividades han realizado estos usuarios más potentes.

4.2.5 Criptografía

Se determinará cómo utilizar controles criptográficos para proteger la información del OP-DAGA en las situaciones en que resulte conveniente.

Estas situaciones formarán parte de del ciclo de vida de la información descrito en la normativa de clasificación de la información (OP-NOR-ClasificaciónInformación). Concretamente, las medidas a adoptar para proteger la información están específicamente descritas en el apartado “medidas de seguridad” de dicho documento.

En la normativa de uso de controles criptográficos y certificados digitales (OP-NOR-ControlesCriptográficos) se especifican los criterios para la selección y uso de los mecanismos criptográficos más adecuados a cada situación de forma que se maximicen los beneficios derivados de su utilización y se evite el uso inapropiado de los mismos.

Se pretende específicamente dar las orientaciones adecuadas para una correcta gestión de las claves, así como para el uso correcto de los certificados electrónicos utilizados para la gestión de ayudas FEAGA y FEADER.

4.2.6 Seguridad física y del entorno

Los sistemas de información estarán ubicados en áreas seguras protegidas con controles de acceso físico que prevengan accesos no autorizados.

Los sistemas de información que soportan la información asociada a la gestión de ayudas FEAGA/FEADER estarán protegidos frente a amenazas físicas y ambientales, sean estas intencionadas o accidentales.

En particular, existirán mecanismos que aseguren la continuidad del suministro eléctrico, la protección frente a la acción del fuego u otro tipo de incidencias y planes de mantenimiento periódico de la infraestructura tecnológica (especialmente en lo relativo a servidores de datos y aplicaciones del OP-DAGA).

4.2.7 Seguridad de las operaciones

Se establecerán procedimientos formalizados para la gestión y operación de los sistemas de información e infraestructura tecnológica soporte a la gestión de ayudas asociadas a fondos FEAGA/FEADER[10].

Los cambios sobre los sistemas y tecnologías de la información estarán identificados y aprobados de forma previa a su puesta en explotación[11]. En este sentido, los entornos de desarrollo y/o prueba estarán separados del entorno productivo o real para evitar incidencias que puedan afectar a la integridad y/o disponibilidad de la información. Esta separación también afectará a las personas con funciones asignadas a tareas de:

- Desarrollo y mantenimiento de sistemas de información.
- Administración de sistemas y tecnologías de la información.
- Usuario gestor de ayudas.

Se implantarán mecanismos que prevengan frente a daños consecuencia de software o programas maliciosos (especialmente frente a virus).e realizarán, con una frecuencia suficiente[12], copias de seguridad de la información y configuración de los sistemas y aplicaciones informáticas con el objetivo de permitir la vuelta a la normalidad en caso de producirse una incidencia o contingencia. Estas copias de seguridad se conservarán, con las medidas de protección suficientes (también durante su traslado), en una ubicación diferente[13].

Los sistemas de información considerarán la opción de registrar información asociada a actividades especialmente sensibles o realizadas por determinados usuarios. Estos *logs* o registros de auditoría se revisarán de forma periódica para identificar problemas o incidencias de seguridad. La Dirección del Organismo Pagador determinará las pistas de auditoría y la información a registrar relativa a cada evento auditable.

[10] Estas funciones serán realizadas en el caso del OP del Gobierno de Aragón, con carácter general, por AST.

[11] Es decir, antes de que puedan afectar a las operaciones que se realizan en el Organismo Pagador.

[12] Típicamente, la realización de copias de seguridad tendrá una periodicidad diaria.

[13] En este sentido, cuando un soporte que contenga información deje de ser útil se eliminará la información que contiene para prevenir accesos no autorizados por parte de terceros a los datos inicialmente almacenados.

4.2.8 Seguridad de las comunicaciones

Para asegurar la protección de la información en las redes y los recursos de tratamiento de la información, y según lo establecido en el procedimiento de interacción con AST y seguimiento de los servicios prestados (OP-PROC-InteracciónAST), la citada entidad se encargará del mantenimiento y configuración de redes y comunicaciones, incluyendo:

- Cortafuegos.
- Electrónica de red.
- Servicios de correo electrónico.
- Mecanismos de protección frente a virus.

4.2.9 Adquisición, desarrollo y mantenimiento de los sistemas de información

Los sistemas de información incluyen tanto las aplicaciones que han sido desarrolladas por el área responsable de sistemas de información como las soluciones que los propios usuarios hayan podido crear (basadas, con frecuencia, en herramientas microinformáticas como *Access*, *Excel*,…) y que tratan datos asociados a la gestión de ayudas.

El OP-DAGA, consciente de la mayor eficiencia de los controles automáticos, tiene como objetivo estratégico la integración en la propia aplicación o sistema de información de mecanismos de validación respecto a la exactitud y coherencia de los datos de entrada, correcto procesamiento de la información (considerando también los controles administrativos asociados a la gestión de cada línea de ayuda) y realidad y regularidad de los resultados obtenidos.

Además, los sistemas de información estarán desarrollados de forma que prevengan la pérdida, modificación o acceso no autorizado de la información que almacenan y procesan. Estos requerimientos de seguridad se considerarán en el documento de diseño funcional de la aplicación y estarán basados en la necesidad de identificación y autenticación para acceder a los sistemas y en medidas de control de acceso que determinen el alcance de los privilegios de los diferentes usuarios. Además, por su especial importancia, el acceso al código fuente[14] de la aplicación estará especialmente restringido.

Por último, existirán procedimientos de control de cambios que permitan asegurar que las modificaciones a realizar sobre las aplicaciones están identificadas (y el Servicio de Asistencia Técnica y Procesos Informáticos conserva un registro de las mismas), se verifican para comprobar su correcto funcionamiento (incluyendo pruebas realizadas por los servicios usuarios) y son aprobadas por parte del área técnica.

[14] La programación específica de las aplicaciones que determina qué funciones realizará el sistema.

4.2.10 Relación con proveedores

En los entornos tecnológicos utilizados para el desarrollo de nuevos sistemas o el mantenimiento de las aplicaciones existentes se minimizará la información sensible o los datos reales con los que deberán realizarse las pruebas[15], especialmente en la medida en que puedan acceder entidades colaboradoras o subcontratadas (públicas o privadas).

Con respecto a la externalización de funciones asociadas al desarrollo y mantenimiento de aplicaciones, el Servicio de Asistencia Técnica y Procesos Informáticos, en colaboración con AST, realizará un seguimiento sobre los servicios y asistencias contratadas y los contratos (o el marco de referencia para la prestación del servicio) considerarán cláusulas de confidencialidad, renuncia por parte del proveedor a la propiedad intelectual de los productos generados, garantía de calidad, etc.).

4.2.11 Gestión de incidentes de seguridad de la información

La Dirección del Organismo Pagador considera la identificación de incidentes de seguridad que puedan afectar a la información y/o a los sistemas un instrumento efectivo que facilita la gestión de estos problemas o debilidades y puede prevenir su ocurrencia en el futuro.

En este sentido, se desarrollará e implantará un procedimiento formal que considere los mecanismos para la identificación y escalado de incidentes. Los incidentes se clasificarán en función de criterios que consideren su naturaleza[16] y los planes de respuesta considerarán, al menos, el análisis para la identificación de la causa, la planificación de medidas correctivas para evitar su ocurrencia, la comunicación a aquellos que puedan verse afectados y la inclusión, en un registro, de la información relevante para la caracterización del incidente de seguridad.

[15] En todo caso, este entorno utilizado para el desarrollo será distinto del entorno productivo o real.

[16] Por ejemplo: indisponibilidad de los sistemas, errores en el procesamiento de la información, utilización no autorizada o fraudulenta de la información o los sistemas,…

4.2.12 Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Se establecerá un proceso de gestión de la continuidad de la operativa del OP-DAGA que permita la recuperación de los procesos y sistemas críticos. Con el fin de reducir el tiempo de indisponibilidad a niveles aceptables, se combinarán controles de carácter organizativo, tecnológico y asociados a procedimientos, tanto preventivos como de recuperación.

En este sentido, estará disponible una infraestructura de respaldo (en una ubicación alternativa a la que, habitualmente, ubica los sistemas de información principales y considerando la problemática asociada a la conectividad y direccionamiento en la red de comunicaciones) que permita la recuperación de la operativa dentro de un marco temporal razonable a través de procedimientos, adecuadamente formalizados[17], de invocación y recuperación.

Asimismo, y con carácter periódico, se revisará mediante verificaciones selectivas y/o parciales la eficacia de las medidas planificadas para recuperar la operativa en caso de contingencia.

4.2.13 Cumplimiento

La Dirección del Organismo Pagador está comprometida con la adaptación de los sistemas de información (adoptando las medidas legales, técnicas y/o organizativas) a la normativa legal vigente.

En particular, se ajusta al Reglamento General de Protección de Datos, así como a la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

Como Organismo Pagador de Aragón, el Departamento de Agricultura, Ganadería y Alimentación, tal y como se ha especificado en el apartado de introducción, debe alinearse con la ISO 27002 y estar certificado además en la ISO 27001.

Igualmente, el Departamento, como administración pública, aplica el Esquema Nacional de Seguridad para asegurar la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de los datos, informaciones y servicios utilizados en medios electrónicos que gestiona en el ejercicio de sus competencias.

Por esta misma condición de administración pública, debe considerar la legislación nacional relativa a la administración electrónica.

Finalmente, se tiene presente la legislación sobre propiedad intelectual.

[17] Incluye también la asignación de responsabilidades.

A continuación se detalla toda la legislación aplicable relacionada según estos apartados:

PROTECCIÓN DE DATOS

- 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)

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

CONSTITUCIÓN DEL ORGANISMO PAGADOR

- Reglamento Delegado (UE) n.º 907/2014 de la Comisión de 11 de marzo de 2014 que completa el Reglamento (UE) n.º 1306/2013 del Parlamento Europeo y del Consejo en lo relativo a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro

- Decreto 167/2006, de 18 de julio, del Gobierno de Aragón, por el que se constituye el Organismo Pagador de los gastos imputables al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER) en la Comunidad Autónoma de Aragón y se establece su organización y funcionamiento

- Decreto 25/2020, de 26 de febrero, del Gobierno de Aragón, por el que se aprueba la estructura orgánica del Departamento de Agricultura, Ganadería y Medio Ambiente

- Decreto de 11 de agosto de 2023, del Presidente del Gobierno de Aragón, por el que se modifica la organización de la Administración de la Comunidad Autónoma de Aragón y se asignan competencias a los departamentos

ESQUEMA NACIONAL DE SEGURIDAD

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

ADMINISTRACIÓN ELECTRÓNICA

- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Decreto 38/2016, de 5 de abril, de aprobación de la Política de gestión y archivo de documentos electrónicos
- Ley 1/2021, de 11 de febrero, de simplificación administrativa
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

PROPIEDAD INTELECTUAL

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia

4.3 Difusión de la política de seguridad

El OP-DAGA potenciará el conocimiento y difusión de esta política de seguridad a los niveles adecuados, dado que interpreta este factor como crítico para asegurar su implantación eficaz y un cumplimiento efectivo. Para ello, hará pública la versión vigente en la extranet del Departamento de Agricultura, Ganadería y Alimentación, incluida en la página web del Gobierno de Aragón.

A nivel interno, permanecerá accesible en el apartado de seguridad de la información del portal del empleado, en la Intranet del Departamento. Asimismo se incidirá en ella en todas las jornadas de formación y concienciación en materia de seguridad informática. También se podrá enviar un mensaje de correo electrónico recordatorio de la política de seguridad a todo el personal.

En este sentido, el Secretario General Técnico, los directores generales y los jefes de los diferentes servicios adscritos al área técnica conocerán el contenido de este documento y colaborarán activamente para aplicar, en sus ámbitos de responsabilidad, lo dispuesto en la política de seguridad. Por otra parte, el área de control interno conocerá, también, el documento y podrá verificar el nivel de cumplimiento en el OP-DAGA, del mismo.

Adicionalmente, los responsables de los diferentes servicios informáticos o de comunicaciones que se prestan por parte de AST al OP-DAGA también conocerán esta política y contribuirán, en lo que a ellos competa, a su aplicación.

5 ACTUALIZACIÓN

El Departamento de Agricultura, Ganadería y Alimentación, como Organismo Pagador y, en particular, el Secretario General Técnico, ostenta la responsabilidad de mantener, revisar y evaluar la política de seguridad de la información[18].

Periódicamente (y siempre que sea posible en un plazo no superior a un año) se revisará la vigencia y razonabilidad de la política de seguridad y del enfoque con el que se aborda la protección de la información.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad como a la adaptación a los cambios en el marco legal, infraestructura tecnológica, organización general, etc.

Entre los elementos a considerar en la determinación de las modificaciones en el contenido y/o enfoque de la política de seguridad se incluyen las siguientes:

- Análisis y evaluación de riesgos[19].
- Resultados de auditorías o revisiones de terceros independientes al proceso de gestión de los sistemas de información y la infraestructura tecnológica.
- Estado de las medidas preventivas o correctivas que pudieran estar planificadas.
- Resultados de revisiones realizadas por parte de la Dirección del Organismo Pagador, la unidad de control interno o la intervención general.
- Análisis de cumplimiento por parte del organismo que presta los servicios en informática y comunicaciones en el Gobierno de Aragón (Aragonesa de Servicios Telemáticos).
- Tendencias asociadas a amenazas y vulnerabilidades.
- Información asociada a incidentes de seguridad identificados en la organización.
- Recomendaciones o directrices de órganos competentes (Comisión Europea, FEGA,…).
- Cambios en el estándar adoptado como marco de referencia.

[18] Todo ello sin perjuicio de las responsabilidades que la unidad de control interno y/o la intervención general pudieran tener en el ejercicio de sus competencias.

[19] Incluyendo las actualizaciones periódicas que se realicen sobre el mapa de riesgos.

El proceso de revisión se iniciará por parte de la Dirección del Organismo Pagador y contará con la participación, al menos, de las siguientes unidades organizativas:

- Servicio de Asistencia Técnica y Procesos Informáticos (SATPI).
- Aragonesa de Servicios Telemáticos (AST), específicamente, el área adscrita al Departamento de Agricultura, Ganadería y Alimentación, que podrá contar con la participación de otras áreas o direcciones responsables de servicios de informática y comunicaciones prestados al OP-DAGA.
- Servicio de Coordinación y Auditoría Interna de Ayudas (como unidad de control interno del OP-DAGA).
- Los responsables de los servicios adscritos al área técnica.

La Dirección del Organismo Pagador mantendrá un registro de las revisiones realizadas, reflejado en el apartado de control de cambios de este documento.

6 ANEXO: REFERENCIAS A OTROS DOCUMENTOS

Si bien el marco normativo del sistema de gestión de seguridad de la información implantado en el OP-DAGA está compuesto por un amplio conjunto de políticas, procedimientos y normativas, a continuación se detallan las referencias de los principales documentos:

DOCUMENTO	REFERENCIA
Selección del estándar y determinación del alcance	OP-NOR-EstándarAlcance
Procedimiento de inventario y valoración de activos	OP-PROC-Inventario
Procedimiento de análisis de riesgos	OP-PROC-AnálisisRiesgos
Definición del nivel de seguridad requerido	OP-NOR-NivelSeguridad
Declaración de aplicabilidad de los controles y las medidas	OP-NOR-DeclaracionesAplicabilidad
Informe sobre el plan general de acción del Organismo Pagador del Gobierno de Aragón y AST respecto al estándar ISO 27002.	OP-PlanGeneral
Normativa sobre las obligaciones del personal	OP-NOR-ObligacionesPersonal
Roles y responsabilidades de la seguridad de la información[20]	OP-NOR-RolesResponsabilidades
Procedimiento de interacción con AST y seguimiento de los servicios prestados	OP-PROC-InteracciónAST
Procedimiento de gestión de incidencias de seguridad	OP-PROC-GestiónIncidencias
Reglamento del Comité de Gestión y Coordinación de la Seguridad de la Información	OP-NOR-ReglamentoComité
Plan de formación, concienciación y sensibilización	OP-NOR-PlanFormación
Procedimiento de bajas de personal	OP-PROC-BajasPersonal
Plan de continuidad de negocio	OP-NOR-PlanContinuidad
Normativa de clasificación de la información	OP-NOR-ClasificaciónInformación
Procedimiento de contacto con autoridades	OP-PROC-ContactoAutoridades
Normativa para la cesión de *software* y datos a entidades colaboradoras	OP-NOR-CesiónSoftware
Procedimiento de seguridad física	OP-PROC-SeguridadFísica

[20] Esta normativa indica las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos según lo establecido en el Esquema Nacional de Seguridad.