CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN



D. ANDRÉS PÉREZ-MONEO AGAPITO, secretario del Pleno, por Resolución del Presidente del Consejo de Cuentas de Castilla y León de 8 de enero de 2014,

CERTIFICO: Que el Pleno del Consejo de Cuentas de Castilla y León, en sesión celebrada el día 14 de mayo de 2025, cuya acta está pendiente de aprobación, adoptó el Acuerdo 61/2025, por el que se aprueba el INFORME "ANÁLISIS DE LA GOBERNANZA EN MATERIA DE CIBERSEGURIDAD DE LA CONSEJERÍA DE AGRICULTURA, GANADERÍA Y DESARROLLO RURAL COMO ORGANISMO PAGADOR DE LA COMUNIDAD DE CASTILLA Y LEÓN", correspondiente al Plan Anual de Fiscalizaciones para el ejercicio 2024.

Asimismo, de conformidad con lo previsto en el artículo 28 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas, el Pleno acuerda la remisión del informe a las Cortes de Castilla y León, al Tribunal de Cuentas y a la Junta de Castilla y León. Del mismo modo, acuerda su remisión a la Fiscalía del Tribunal de Cuentas.

Y para que conste, a los efectos oportunos, expido la presente certificación, con el visto bueno del presidente del Consejo de Cuentas de Castilla y León, en Palencia, a la fecha de la firma electrónica.

V.º B.º
EL PRESIDENTE
*(Art. 21.5 de la Ley 2/2002, de 9 de abril)*

Mario Amilivia González

CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

# ANÁLISIS DE LA GOBERNANZA EN MATERIA DE CIBERSEGURIDAD DE LA CONSEJERÍA DE AGRICULTURA, GANADERÍA Y DESARROLLO RURAL COMO ORGANISMO PAGADOR DE LA COMUNIDAD DE CASTILLA Y LEÓN

PLAN ANUAL DE FISCALIZACIONES 2024

# ÍNDICE

# SIGLAS Y ABREVIATURAS

| | |
|---|---|
| **Art.** | Artículo |
| **BOCYL** | Boletín Oficial de Castilla y León |
| **ENS** | Esquema Nacional de Seguridad |
| **FEADER** | Fondo Europeo Agrícola de Desarrollo Rural |
| **FEAGA** | Fondo Europeo Agrícola de Garantía Agraria |
| **FYM** | Consejería de Fomento y Medio Ambiente |
| **GPF-OCEX** | Guía práctica de fiscalización de los órganos de control externo |
| **ISSAI-ES** | Normas Internacionales de las Entidades Fiscalizadoras Superiores |
| **M€** | Millones de euros |
| **MTD** | Consejería de Movilidad y Transformación Digital |
| **NIA** | Normas Internacionales de Auditoría |
| **OP** | Organismo Pagador |
| **PAT** | Consejería de Presidencia y Administración Territorial |
| **TI** | Tecnologías de la información |
| **TIC** | Tecnologías de la Información y Comunicaciones |

Las siglas correspondientes a la normativa utilizada se encuentran incluidas en el apartado I.2. MARCO NORMATIVO.

# NOTAS SOBRE ORIGEN DE DATOS

Los cuadros insertados a lo largo del presente Informe, salvo que se especifique otra cosa, se han elaborado a partir de la información facilitada por la entidad fiscalizada.

# I. INTRODUCCIÓN

## I.1. INICIATIVA DE LA FISCALIZACIÓN

De conformidad con lo preceptuado en el artículo 90 del Estatuto de Autonomía de Castilla y León y en el artículo 1 de la Ley 2/2002, de 9 de abril, Reguladora del Consejo de Cuentas de Castilla y León, corresponde al Consejo la fiscalización externa de la gestión económica, financiera y contable del Sector Público de la Comunidad Autónoma y demás entes públicos de Castilla y León.

Por su parte, el apartado 2.º del artículo 3 de la misma Ley reconoce la iniciativa fiscalizadora del Consejo por medio de las fiscalizaciones especiales, en cuya virtud se incluye dentro del Plan Anual de Fiscalizaciones para el ejercicio 2024 del Consejo de Cuentas, aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León en su Resolución de 12 de febrero de 2024 (BOCYL n.º 44/2024 de 1 de marzo), la relativa al «Análisis de la gobernanza en materia de ciberseguridad de la Consejería de Agricultura, Ganadería y Desarrollo Rural como Organismo Pagador de la Comunidad de Castilla y León».

En el contexto actual, la seguridad de la información se posiciona como un aspecto fundamental para cualquier organización, especialmente en el sector público, ya que se caracteriza por la gestión de datos altamente sensibles y críticos. En este sentido, la implementación de una gobernanza efectiva en seguridad se vuelve imprescindible para garantizar una gestión eficaz y eficiente de la seguridad en el ámbito público.

La gobernanza en la seguridad, en el contexto del ámbito público, juega un papel decisivo al establecer los procesos, estructuras y políticas que garantizan la protección integral de los activos, datos y sistemas. Esto requiere la creación de un marco normativo robusto que defina claramente las responsabilidades, roles y procedimientos a seguir en materia de seguridad de la información. Asimismo, implica una asignación adecuada de recursos y una implementación diligente de medidas de seguridad con el fin de mitigar riesgos y salvaguardar la integridad del sistema.

Para gestionar los riesgos asociados a este nuevo entorno, se deben examinar tanto los aspectos técnicos como los aspectos organizativos y de gestión relacionados con la seguridad de la información, que permitan ayudar a identificar las áreas de mejora y fortalecer la seguridad en el ámbito público.

## I.2. MARCO NORMATIVO

La normativa en materia de la organización de la Comunidad Autónoma de Castilla y León y de la gobernanza de la seguridad que resulta más relevante a los efectos del objeto de esta fiscalización, se encuentra recogida fundamentalmente en las siguientes disposiciones:

### I.2.1. NORMATIVA AUTONÓMICA

- Ley Orgánica 4/1983, de 25 de febrero, de Estatuto de Autonomía de Castilla y León.
- Ley Orgánica 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León.
- Ley 2/2002, de 9 de abril, reguladora del Consejo de Cuentas de Castilla y León.
- Decreto 310/1999, de 16 de diciembre, por el que se aprueba el Plan de Empleo de personal informático al servicio de la Administración de la Comunidad de Castilla y León.
- Decreto 137/2001, de 3 de mayo, por el que se modifican las relaciones de puestos de trabajo de personal laboral de la Administración General y de la Gerencia de Servicios Sociales de Castilla y León y se desarrollan otras medidas previstas en el Decreto 310/1999, de 16 de diciembre, por el que se aprueba el Plan de Empleo del personal informático al Servicio de la Administración de Castilla y León.
- Decreto 86/2006, de 7 de diciembre, por el que se designa al Organismo Pagador y al Organismo de Certificación de los gastos financiados por el Fondo Europeo Agrícola de Garantía (FEAGA) y por el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) en la Comunidad Autónoma de Castilla y León, modificado por el Decreto 29/2018, de 6 de septiembre.
- Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León.
- Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León (PSIPD).
- Decreto 1/2022, de 19 de abril, del Presidente de la Junta de Castilla y León, de reestructuración de consejerías.
- Decreto 10/2022, de 5 de mayo, por el que se establece la estructura orgánica de la Consejería de Movilidad y Transformación Digital.
- Decreto 11/2022, de 5 de mayo, por el que se establece la estructura orgánica de la Consejería de Agricultura, Ganadería y Desarrollo Rural.
- Orden FYM/337/2022, de 8 de abril, por la que se aprueba la norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León.
- Orden MTD/526/2022, de 27 de mayo, por la que se desarrolla la estructura orgánica de los servicios centrales de la Consejería de Movilidad y Transformación Digital.

- Orden AGR/527/2022, de 27 de mayo, de la Consejería de Agricultura, Ganadería y Desarrollo Rural, por la que se desarrolla la estructura orgánica de los servicios centrales de la Consejería de Agricultura, Ganadería y Desarrollo Rural.

#### I.2.2. NORMATIVA ESTATAL

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

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC).

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

- 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 (ENI).

- 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.

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

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

#### I.2.3. NORMATIVA COMUNITARIA

- 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, RGPD).

- Reglamento (UE) 2021/2115 del Parlamento Europeo y del Consejo, de 2 de diciembre de 2021, por el que se establecen normas en relación con la ayuda a los planes

estratégicos que deben elaborar los Estados miembros en el marco de la política agrícola común (planes estratégicos de la PAC), financiada con cargo al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (FEADER), y por el que se derogan los Reglamentos (UE) n.º 1305/2013 y (UE) n.º 1307/2013.

- Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo, de 2 de diciembre de 2021, sobre la financiación, la gestión y el seguimiento de la política agrícola común y por el que se deroga el Reglamento (UE) n.º 1306/2013.

- Reglamento Delegado (UE) 907/2014 de la Comisión, de 11 de marzo de 2014, que completa el Reglamento (UE) 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.

- Reglamento de Ejecución (UE) 908/2014 de la Comisión, de 6 de agosto de 2014, por el que se establecen disposiciones de aplicación del Reglamento (UE) 1306/2013 del Parlamento Europeo y del Consejo en relación con los organismos pagadores y otros organismos, la gestión financiera, la liquidación de cuentas, las normas relativas a los controles, las garantías y la transparencia.

- Reglamento Delegado (UE) 2022/126 de la Comisión, de 7 de diciembre de 2021, de por el que se completa el Reglamento (UE) 2021/2115 del Parlamento Europeo y del Consejo en lo relativo a los requisitos adicionales para determinados tipos de intervención especificados por los Estados miembros en sus planes estratégicos de la PAC para el período 2023-2027 en virtud de dicho Reglamento, y a las normas sobre la proporción relativa a la norma 1 de las buenas condiciones agrarias y medioambientales (BCAM).

- Reglamento Delegado (UE) 2022/127 de la Comisión, de 7 de diciembre de 2021, que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro.

- Reglamento Delegado (UE) 2022/1172 de la Comisión, de 4 de mayo de 2022, por el que se completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo en lo que respecta al sistema integrado de gestión y control de la política agrícola común y la aplicación y el cálculo de las sanciones administrativas en el marco de la condicionalidad.

- Reglamento de Ejecución (UE) 2022/1173 de la Comisión, de 31 de mayo de 2022, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo en lo que respecta al sistema integrado de gestión y control de la política agrícola común.

- Reglamento Delegado (UE) 2023/57 de la Comisión, de 31 de octubre de 2022, que modifica y corrige el Reglamento Delegado (UE) 2022/127 por el que se completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo.

- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2, también conocida por sus siglas en inglés NIS2).

# II. OBJETIVOS, ALCANCE Y LIMITACIONES

## II.1. OBJETIVOS

Se trata de una fiscalización especial cuyo objetivo principal es verificar si el ente auditado ha establecido y puesto en práctica una estructura de gobernanza sólida en ciberseguridad que no solo cumpla con los requisitos mínimos de seguridad, sino que también proporcione un marco adecuado para proteger la información que administra y garantizar la prestación de los servicios de su competencia.

Para ello se ha llevado a cabo una auditoría operativa en la que se han analizado las actuaciones, medidas y procedimientos adoptados para la efectiva implantación de este marco de gobernanza, los recursos destinados y su eficacia, sin perjuicio de que implique la verificación del cumplimiento de la legalidad en lo referente a la normativa en materia de seguridad de la información y protección de datos de carácter personal, que debe exigirse al ente auditado.

De acuerdo con ello, se identifican los siguientes objetivos:

- Proporcionar una evaluación sobre el grado de implantación y el funcionamiento efectivo del marco de gobernanza de la ciberseguridad en el ente auditado, así como posibles incumplimientos normativos relacionados con la ciberseguridad.
- Complementariamente al objetivo principal, evaluar si se ha provisto por parte de la entidad de los recursos necesarios (humanos y materiales) para el correcto funcionamiento de este marco.

## II.2. ALCANCE

La fiscalización tiene como ámbito subjetivo la Consejería de Agricultura, Ganadería y Desarrollo Rural como Organismo Pagador de la Comunidad de Castilla y León. En la Ley 5/2024, de 9 de mayo, de Presupuestos Generales de la Comunidad de Castilla y León para 2024 se consigna en el estado de gastos de la Política Agrícola Común (PAC) un importe de 924.421.069 €, lo que supone en torno al 8 % del estado de gastos de la Administración General de la Comunidad de Castilla y León (12.189.061.812 €).

El Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo de 2 de diciembre de 2021 sobre la financiación, la gestión y el seguimiento de la política agrícola común y por el que se deroga el Reglamento (UE) n.º 1306/2013 establece la financiación, gestión y seguimiento de la Política Agrícola Común.

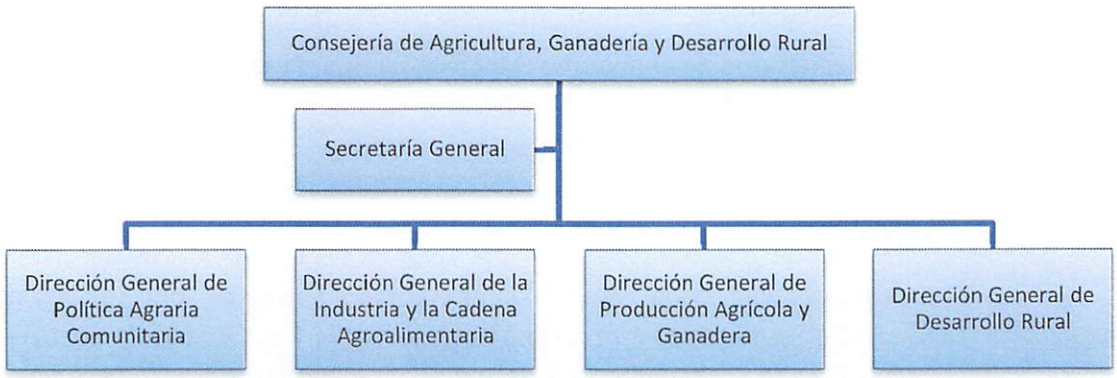
Por otra parte, el Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021, que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro, establece en su anexo I disposiciones relativas a la autorización de los organismos pagadores.

De conformidad con la referida normativa comunitaria, mediante el Decreto 86/2006, de 7 de diciembre (BOCYL n.º 237, de 12 de diciembre de 2006), se designa a la Consejería de Agricultura y Ganadería para actuar como Organismo Pagador en la Comunidad Autónoma de Castilla y León, de los gastos financiados por el FEAGA y por el FEADER. Esta normativa básica se complementa con el Decreto 87/2006 de 7 de diciembre, por el que se establecen las normas sobre la gestión presupuestaria de los créditos gestionados por el Organismo Pagador correspondientes a gastos financiados por estos fondos comunitarios y se desconcentran competencias en esta materia, y por la Orden PAT/163/2007, de 30 de enero, por la que se determina el Procedimiento de actuación del Organismo Pagador de Castilla y León.

En el Decreto 86/2006 también se le atribuyen funciones de autorización y control de pagos relativas a las actuaciones del FEADER para las competencias que tenga asumidas en esta materia a la Dirección General del Medio Natural de la Consejería de Medio Ambiente (actualmente la Dirección General de Patrimonio Natural y Política Forestal de la Consejería de Medio Ambiente, Vivienda y Ordenación del Territorio). Esta dirección general constituye el órgano delegado del Organismo Pagador.

En el siguiente gráfico se muestra la estructura orgánica de la Consejería de Agricultura, Ganadería y Desarrollo Rural.

**Gráfico 1. Estructura orgánica de la Consejería de Agricultura, Ganadería y Desarrollo Rural**




El ámbito temporal de la fiscalización alcanza a la situación existente en el año 2024, sin perjuicio de las comprobaciones correspondientes a actuaciones realizadas en años anteriores que sean necesarias para cumplir los objetivos.

Los trabajos de fiscalización se han realizado de acuerdo con lo dispuesto en las ISSAI-ES (Nivel III) aprobadas por la Conferencia de Presidentes de las Instituciones Autonómicas de Control Externo el 16 de junio de 2014, y ordenada su aplicación por el Acuerdo 64/2014, del Pleno del Consejo de Cuentas. Supletoriamente se aplicarán los Principios y Normas de Auditoría del Sector Público, elaborados y aprobados por la Comisión de Coordinación de los Órganos Públicos de Control Externo del Estado Español.

En la GPF-OCEX 5331 «Gobernanza corporativa, gobernanza sobre las TI y su auditoría» se señalan las razones por la que tiene gran relevancia en una auditoría

financiera analizar la situación de la gobernanza sobre las tecnologías de la información y las comunicaciones (TIC) y de la gobernanza de la ciberseguridad al revisar el componente «Entorno de control» del sistema de control interno de la entidad auditada, de acuerdo con los requerimientos de la NIA-ES 315 Revisada / GPF-OCEX 1315 Revisada.

Una revisión completa de todos los aspectos relativos a una adecuada gobernanza en la ciberseguridad incluye un conjunto muy amplio de controles y aspectos a revisar, lo que requiere de un alto grado de dedicación, por parte del ente auditado y del organismo que audita.

Sin embargo, siguiendo el criterio de la GPF-OCEX 5314 «Gobernanza de la ciberseguridad y su auditoría» se puede determinar en primer lugar si se ha establecido un marco para la gestión eficaz de la ciberseguridad, y en segundo lugar si se han definido adecuadamente los roles y responsabilidades de los diferentes actores en la gestión de la ciberseguridad proporcionando una metodología para la auditoría de la gobernanza de la ciberseguridad.

En consecuencia, es posible identificar los componentes esenciales de una sólida gobernanza en ciberseguridad. Estos incluyen el modelo de gobernanza, el comité de seguridad TIC, los roles relacionados con la seguridad de la información y la normativa interna de ciberseguridad.

A continuación, se expone un resumen de las verificaciones realizadas en cada uno de los epígrafes que conforman los resultados de la presente auditoría en los que se indican las comprobaciones realizadas en cada una de las áreas de trabajo señaladas en las Directrices técnicas, coincidentes con la Guía práctica de fiscalización, GPF-OCEX 5314 «Gobernanza de la ciberseguridad y su auditoría»:

1) Políticas, normas y procedimientos sobre seguridad de la información

El objetivo del análisis de la política de seguridad de la información, las normas y los procedimientos asociados es evaluar su eficacia, coherencia y alineación con los objetivos de la organización, los riesgos identificados y los requisitos normativos para garantizar una protección adecuada de su información. Se ha evaluado cómo se establecen, implementan y mantienen las políticas, normas y procedimientos. En particular, se ha comprobado si la entidad auditada:

- Dispone de políticas sobre la seguridad de los sistemas de información aprobadas por los órganos superiores y difundidas entre sus empleados y, en su caso, a proveedores y terceros.

- Dispone de normativa interna donde se determine el uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido, aprobada por quien disponga la política de seguridad de la información.

- Dispone de un conjunto de procedimientos documentados que determinan cómo realizar las tareas habituales y quiénes son sus responsables.

- Realiza actividades de difusión y concienciación entre sus empleados para garantizar el conocimiento y cumplimiento de las políticas y normas de seguridad de la información.

2) Comité de seguridad TIC, roles y responsabilidades

El objetivo es verificar si la entidad auditada ha implementado estructuras de gobierno de ciberseguridad sólidas. Esto incluye un comité de seguridad bien definido y activo, roles y responsabilidades claras, participación adecuada de las partes interesadas relevantes, y suficientes capacidades y recursos. Se ha evaluado la composición, responsabilidades, nombramientos y capacidad del Comité de Seguridad TIC. En particular, se ha comprobado si en la entidad auditada:

- Se han realizado los nombramientos en materia de seguridad de la información de acuerdo con lo previsto en la política de seguridad de la información.

- Se han adoptado medidas para asegurar que las personas designadas disponen de recursos para llevar a cabo sus tareas de manera efectiva (tiempo, formación, posición en el organigrama, etc.).

3) Compromiso de la dirección y de la alta dirección

El objetivo es asegurar que la dirección y la alta dirección brindan el apoyo necesario, asignan recursos adecuados y promueven una cultura de seguridad alineada con los objetivos de la organización. Se ha evaluado el nivel de implicación y compromiso de la dirección en participar, respaldar y fomentar las acciones relacionadas con la gobernanza de la ciberseguridad. En particular, se ha verificado si en la entidad auditada:

- Los miembros de la dirección y la alta dirección participan de forma activa en el establecimiento de políticas y objetivos estratégicos de la entidad, la gestión de riesgos y en la aplicación de medidas para mitigarlos.

- Existe un liderazgo reconocible.

- La dirección fomenta una cultura de ciberseguridad en la entidad.

4) Gestión de riesgos

El objetivo de una gestión de riesgos es identificar, evaluar y mitigar los riesgos que puedan afectar a la información de la entidad. Se ha comprobado si la entidad ha realizado y documentado un análisis de los riesgos que afectan a sus sistemas de información. En particular, se ha verificado si en la entidad auditada:

- Los sistemas de información están definidos y clasificados por niveles de seguridad (alto, medio o bajo) de acuerdo con los requisitos del ENS (Art. 40 y 41).

- El análisis de riesgos realizado está actualizado e incluye los sistemas de información críticos de la entidad.

- Los riesgos analizados han sido aceptados, eliminados, transferidos o mitigados y, en su caso, si existe un plan de tratamiento de riesgos aprobado por los responsables previstos en la política de seguridad de la información.

5) Cumplimiento legal

El objetivo es asegurar que la entidad cumple con las leyes, regulaciones y estándares de aplicación y es capaz de identificar y aplicar los cambios legislativos o normativos que le aplican. En particular, se ha verificado si existe un mecanismo o procedimiento para identificar la legislación, los requisitos contractuales o reglamentarios que se aplican a la entidad.

Se ha evaluado si existe un adecuado nivel de cumplimiento legal respecto al ENS. En particular, se ha verificado los siguientes aspectos en la entidad auditada:

- Existencia de declaraciones de aplicabilidad y planes de adecuación.

- Realización de los informes anuales sobre seguridad de la información de acuerdo con el artículo 32 del ENS y la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Realización de los informes de auditoría de seguridad requeridos por el ENS (Art. 31).

Se ha evaluado si se da cumplimiento a los requisitos mínimos del RGPD y la LOPDGDD. En particular, se ha verificado si la entidad auditada:

- Ha nombrado un delegado de protección de datos y lo ha comunicado a la Agencia Española de Protección de Datos (Art. 37 del RGPD).

- Ha elaborado y publicado por medios electrónicos el Registro de Actividades de Tratamiento (Art. 30 del RGPD y 31 de la LOPDGDD).

- Ha realizado análisis de riesgos y evaluaciones de impacto sobre los datos personales tratados por la entidad (Art. 32 y 35 del RGPD).

- Evalúa periódicamente la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad de los tratamientos (Art. 32 del RGPD).

6) Recursos del departamento TIC y de seguridad

El objetivo es comprobar si la organización asigna al departamento TIC y a la seguridad los recursos humanos y materiales necesarios para llevar a cabo tareas de seguridad y estos son adecuados al tamaño de la entidad. En particular, se ha analizado en la entidad auditada:

- El número de personas a tiempo completo (o equivalente) perteneciente al departamento/área/negociado de gestión de las TIC de la entidad, identificando cuántas de ellas se dedican a la seguridad de la información.
- La formación especializada en materia de ciberseguridad.
- La dotación presupuestaria de los Capítulos 1, 2 y 6 del departamento TIC y a la seguridad de la información.
- El total de las Obligaciones Reconocidas Netas (ORN) de los Capítulos 1, 2 y 6 del presupuesto.

Se ha evaluado la dotación de personal, su formación y los presupuestos asignados al departamento TIC y en particular, los destinados a la seguridad.

Los trabajos desarrollados para la elaboración del presente Informe finalizaron en enero de 2025.

## II.3. LIMITACIONES

Con carácter general no han existido limitaciones en el trabajo realizado, habiendo tenido el ente fiscalizado una actitud de colaboración.

Sin embargo, debido a la naturaleza compartida de los servicios TIC corporativos con el resto de la Administración de la Comunidad de Castilla y León y que no existe una contabilidad de costes que permita atribuir los costes corporativos entre las diferentes consejerías, resulta inviable realizar un análisis integral de la planificación estratégica, los presupuestos y los recursos de personal TIC y de ciberseguridad específicos del Organismo Pagador, ya que no es posible asignar de forma objetiva los recursos empleados exclusivamente por el Organismo Pagador frente a los utilizados por el conjunto de la Administración de la Comunidad de Castilla y León.

## II.4. TRÁMITE DE ALEGACIONES

En cumplimiento de lo dispuesto en el artículo 25.4 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas de Castilla y León, el Informe provisional se puso a disposición del ente fiscalizado el 14 de abril de 2025, para que en un plazo de 20 días naturales formulara alegaciones.

Transcurrido el plazo, el ente fiscalizado no ha realizado alegaciones.

# III. CONCLUSIONES

De los resultados de la fiscalización, así como de las limitaciones del apartado II.3, se deducen las conclusiones de los siguientes apartados.

## III.1. POLÍTICA DE SEGURIDAD, NORMAS Y PROCEDIMIENTOS

1) La Consejería de Agricultura, Ganadería y Desarrollo Rural, como Organismo Pagador de Castilla y León dispone de una política sobre la seguridad de los sistemas de información adecuada a sus objetivos y a su misión, aprobada por el titular de la Consejería como director del Organismo Pagador y difundida a todas las partes interesadas mediante su publicación en Internet y su inclusión en la formación obligatoria de seguridad de la información. Esta política cumple con lo establecido en la medida [org.1] del Esquema Nacional de Seguridad.

2) La Política de Seguridad de la Información del Organismo Pagador está supeditada y coordinada correctamente con la de la Administración de la Comunidad de Castilla y León definida en el «Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León». Esta política es pública y accesible a través de Internet.

3) El Organismo Pagador dispone de una norma de seguridad que determina el uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido, adaptada a las necesidades de la entidad, con actualizaciones habituales y disponible en el portal de aplicaciones del Organismo Pagador. Esta norma cumple con lo establecido en la medida [org.2] del Esquema Nacional de Seguridad.

4) Al Organismo Pagador, como parte integrante de la Administración de la Comunidad de Castilla y León, también le aplica su normativa de seguridad descrita en la «Orden FYM/337/2022, de 8 de abril, por la que se aprueba la norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León». Ambas normas son compatibles entre sí y, en caso de conflicto entre ambas, el Organismo Pagador aplica la norma más restrictiva.

5) Los procedimientos de seguridad del Organismo Pagador, junto con las instrucciones técnicas, determinan de forma adecuada cómo realizar las tareas habituales y quiénes son sus responsables en las áreas de seguridad consideradas críticas. Estos procedimientos cumplen con lo establecido en la medida [org.3] del Esquema Nacional de Seguridad.

## III.2. COMITÉ DE SEGURIDAD, ROLES Y RESPONSABILIDADES

6) El Organismo Pagador ha definido correctamente los diferentes roles de seguridad que se indican en el Esquema Nacional de Seguridad y todos ellos forman parte de su Comité de Seguridad de la Información.

7) El responsable de seguridad del Organismo Pagador no coincide con el responsable de seguridad designado por Consejería de Agricultura, Ganadería y Desarrollo Rural en la Política de Seguridad de la Información y Protección de Datos Personales de la Administración de la Comunidad de Castilla y León.

8) Las funciones del responsable del tratamiento de datos personales no están definidas formalmente en su normativa de organización de la seguridad de la información, aunque se evidencia en el Registro de Actividades de Tratamiento que estas funciones son realizadas por los responsables de la información, titulares de los centros directivos de la Consejería de Agricultura, Ganadería y Desarrollo Rural.

9) La formación que reciben los diferentes responsables de su política es de carácter genérico a través del curso obligatorio de seguridad de la información. Existen actividades de formación y concienciación relacionadas con sus funciones de forma ocasional.

10) El Comité de Seguridad de la Información del Organismo Pagador desempeña sus funciones de forma efectiva y con la periodicidad semestral establecida en su normativa.

### III.3. COMPROMISO DE LA DIRECCIÓN Y DE LA ALTA DIRECCIÓN

11) La dirección del Organismo Pagador ejerce un liderazgo reconocible en la gobernanza de la ciberseguridad, puesto que forma parte del Comité de Seguridad de la Información con su presidencia y vocalías. En este órgano la dirección del Organismo Pagador participa de forma activa en la aprobación y seguimiento de sus objetivos estratégicos en seguridad de la información y en la gestión de los riesgos.

12) La dirección del Organismo Pagador impulsa la formación y concienciación en seguridad de la información mediante la inclusión de un curso de ciberseguridad obligatorio para todos los miembros del Organismo Pagador y de actividades de concienciación en sus planes anuales de formación, aunque no se incluyen detalles. Estos planes dan cumplimiento a las medidas [mp.per.3] y [mp.per.4] del Esquema Nacional de Seguridad, sobre concienciación y formación respectivamente.

13) La dirección del Organismo Pagador facilita los recursos necesarios para el buen funcionamiento de su Sistema de Gestión de Seguridad de la Información a través del Comité de Seguridad de la Información según las necesidades definidas en análisis de Debilidades, Amenazas, Fortalezas y Oportunidades (DAFO).

### III.4. GESTIÓN DE RIESGOS

14) La dirección del Organismo Pagador fija dentro de la organización de seguridad las responsabilidades necesarias para llevar a cabo un proceso de apreciación y gestión de los riesgos con carácter anual y la aprobación de planes de tratamiento de riesgos y de los riesgos residuales por el Comité de Seguridad de la Información como

responsable de los riesgos. Este aspecto da cumplimiento a la medida [op.pl.1] del Esquema Nacional de Seguridad.

## III.5. CUMPLIMIENTO LEGAL

15) El Organismo Pagador contempla un marco normativo básico en su política de seguridad y mantiene un registro normativo actualizado con la totalidad de la legislación que le aplica. Sin embargo, no existe un procedimiento formal de gestión de dicho registro acorde con los estándares de documentación de seguridad del Organismo Pagador.

16) En cumplimiento de la legislación europea para organismos pagadores responsables de la gestión y control de un gasto de la Unión anual superior a 400 M€, el Organismo Pagador ha certificado su Sistema de Gestión de Seguridad de la Información conforme a la norma UNE-EN ISO/IEC 27001:2017.

17) Los sistemas de información del Organismo Pagador, todos ellos de categoría MEDIA, cumplen con los requisitos exigidos por el Esquema Nacional de Seguridad de acuerdo con el Perfil de Cumplimiento Específico de Organismos Pagadores (Perfil General) como muestra su certificado de conformidad publicado en la sede electrónica de la Administración de la Comunidad de Castilla y León.

18) El Organismo Pagador cumple con la normativa de protección de datos personales en cuanto al delegado de protección de datos, Registro de Actividades de Tratamiento y análisis y gestión de los riesgos que afectan este tipo de datos. El procedimiento de gestión de incidentes de seguridad tiene en cuenta las particularidades de los incidentes de seguridad que involucren datos personales, pero no se recogen de forma adecuada las funciones del responsable del tratamiento relativas a la notificación de incidentes a la Agencia Española de Protección de Datos y a la comunicación a las personas afectadas en los mismos.

## III.6. RECURSOS DEL DEPARTAMENTO TIC Y DE SEGURIDAD

19) El Organismo Pagador dispone exclusivamente de 39 personas dedicadas a funciones TIC, de las cuales solo una se encarga específicamente de tareas relacionadas con la seguridad de la información. El resto de personal TIC que realiza tareas para el Organismo Pagador forma parte de los servicios corporativos y son compartidos con el resto de la Administración de la Comunidad de Castilla y León.

20) La proporción del personal dedicado a seguridad frente al dedicado a servicios TIC del Organismo Pagador (2,56 %) es escasa en comparación con la ofrecida por la Agencia Europea para la Ciberseguridad en las organizaciones afectadas por la Directiva SRI 2 (14,5 % en 2022 y 12,8 % en 2023), entre las que se encuentra el Sector Público, si bien este dato está limitado por el hecho de que no puede contabilizarse el personal TIC corporativo compartido que da servicios al Organismo Pagador con el resto de la Administración de la Comunidad de Castilla y León.

21) El personal TIC recibe formación regular en seguridad mediante cursos organizados por la Escuela de Administración Pública de Castilla y León, por el Centro Criptológico Nacional, por empresas externas y por el propio Organismo Pagador.

22) Los gastos TIC del Organismo Pagador en 2022 ascendieron a 4,2 M€, de los cuales un 0,45 % se destinaron a seguridad (19.111,95 €). En 2023 los gastos TIC se incrementaron un 14,14 % hasta los 4,8 M€, pero los destinados a seguridad (6.304,10 €) disminuyeron un 67,01 %, siendo un 0,13 % del total de gastos TIC.

23) La proporción de los gastos en seguridad frente a la totalidad de los gastos TIC del Organismo Pagador (0,45 % en 2022 y 0,13 % en 2023) son escasos en comparación con los ofrecidos por Agencia Europea para la Ciberseguridad en las organizaciones afectadas por la Directiva SRI 2 (7,6 % en 2022 y 9,6 % en 2023), entre las que se encuentra el Sector Público, si bien este dato está limitado por el hecho de que en los gastos del Organismo Pagador no es posible incluir los gastos de los servicios TIC corporativos compartidos con el resto de la Administración de la Comunidad de Castilla y León que utiliza el Organismo Pagador.

# IV. RECOMENDACIONES

Teniendo en cuenta lo expuesto a lo largo del presente Informe y las conclusiones contenidas en el mismo, se formulan las siguientes recomendaciones, orientadas a contribuir a la mejora de la gobernanza en materia de ciberseguridad:

1) El titular de la Secretaría General de Consejería de Agricultura, Ganadería y Desarrollo Rural debería realizar las acciones necesarias para que la designación del responsable de seguridad por la Consejería en la Política de Seguridad de la Información y Protección de Datos Personales de la Administración de la Comunidad de Castilla y León sea coherente con la del responsable de seguridad del Organismo Pagador.

2) La dirección del Organismo Pagador debería especificar en su normativa de organización de la seguridad de la información las funciones del responsable del tratamiento de datos personales.

3) El responsable de seguridad debería especificar en el procedimiento de gestión de incidentes de seguridad las funciones del responsable del tratamiento de datos personales relacionadas con la notificación a la Agencia Española de Protección de Datos y a las personas afectadas.

4) La dirección del Organismo Pagador, a propuesta de la Secretaría Técnica del Organismo Pagador, debería definir y planificar una formación destinada a los diferentes responsables de la organización de la seguridad del Organismo Pagador que comprenda sus funciones y obligaciones específicas. A su vez, debería establecer formalmente las características del curso de seguridad de la información en los planes anuales de formación para facilitar la asignación de recursos, organización, implementación, evaluación y seguimiento, al igual que el resto de las actividades formativas del Organismo Pagador.

5) La dirección del Organismo Pagador debería definir en los planes anuales de formación una planificación formal de las actividades de concienciación en seguridad especificando objetivos, contenidos, indicadores y cronograma de actividades puntuales o regulares que permita una evaluación y mejora continua de la concienciación del personal acerca de su papel y responsabilidad en la seguridad del Organismo Pagador.

6) El Servicio de Evaluación, Normativa y Procedimiento debería describir formalmente el procedimiento de gestión de la normativa de aplicación al Organismo Pagador conforme a sus estándares de documentación de seguridad.

# ÍNDICE DE GRÁFICOS