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

El objetivo de esta fiscalización operativa es verificar si el ente auditado ha puesto en práctica una estructura de gobernanza sólida en ciberseguridad que no solo cumpla con los requisitos mínimos, sino que también proporcione un marco adecuado para proteger la información que administra y garantizar la prestación de los servicios de su competencia. Se analiza la situación existente en 2024 sobre las actuaciones, medidas y procedimientos adoptados para implantar este marco de gobernanza, los recursos destinados y su eficacia, sin perjuicio de 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.

En la Ley de Presupuestos Generales de la Comunidad para 2024 se consignó en el estado de gastos de la Política Agrícola Común (PAC) un importe de 924 millones, lo que supone en torno al 8% del estado de gastos de la Administración general, cifrado en 12.189 millones.

Política de seguridad, normas y procedimientos. La Consejería, como organismo pagador, tiene una política sobre la seguridad de los sistemas de información adecuada, aprobada por su titular y difundida a las partes interesadas mediante su publicación en Internet y su inclusión en la formación obligatoria de seguridad de la información. Dicha política está supeditada y coordinada correctamente con la de la Administración autonómica.

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 su portal de aplicaciones. Los procedimientos de seguridad, 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. La política de seguridad, norma y procedimientos mencionados cumplen con lo establecido sobre el marco organizativo del Esquema Nacional de Seguridad (ENS).

Comité de seguridad, roles y responsabilidades. El organismo pagador ha definido correctamente los diferentes roles de seguridad que se indican en el ENS y todos ellos forman parte de su Comité de Seguridad de la Información. No obstante, el responsable de seguridad no coincide con el designado por la Consejería en la Política de Seguridad de la Información y Protección de Datos Personales de la Administración autonómica. Además, 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.

La formación que reciben los diferentes responsables de su política a través del curso obligatorio de seguridad de la información es genérica. Existen actividades de formación y concienciación relacionadas con sus funciones de forma ocasional. El Comité de Seguridad de la Información desempeña sus funciones de forma efectiva y con la periodicidad semestral establecida.

Compromiso de la dirección. 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, donde 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. La dirección impulsa la formación y concienciación en seguridad de la información mediante un curso de ciberseguridad obligatorio para todos los miembros del organismo pagador y actividades de concienciación en sus planes anuales de formación, que cumplen las medidas contempladas por el ENS. Además, la dirección 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.

Gestión de riesgos. 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 en esta materia. Este aspecto cumple la medida sobre análisis de riesgos del ENS.

Cumplimiento legal. El organismo pagador contempla un marco normativo básico en su política de seguridad y mantiene un registro normativo con la legislación aplicable. Sin embargo, no existe un procedimiento formal de gestión de dicho registro acorde con los estándares de su documentación de seguridad. En cumplimiento de la legislación comunitaria para organismos pagadores responsables de la gestión y control de un gasto de la Unión Europea anual superior a 400 millones, ha certificado su Sistema de Gestión de Seguridad de la Información con la Asociación Española de Normalización. Sus sistemas de información cumplen con los requisitos exigidos por el ENS de acuerdo con el Perfil de Cumplimiento Específico de Organismos Pagadores, como muestra su certificado de conformidad publicado en la sede electrónica de la Administración autonómica.

El organismo pagador cumple con la normativa de protección de datos personales en cuanto al delegado de protección de datos, el Registro de Actividades de Tratamiento y el análisis y gestión de los riesgos que afectan a este tipo de datos. El procedimiento de gestión de incidentes de seguridad tiene en cuenta las particularidades de aquellos que involucren datos personales, pero no recoge 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.

Recursos del departamento TIC y de seguridad. El organismo pagador dispone 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 forma parte de los servicios corporativos y son compartidas con toda la Administración autonómica. El personal TIC recibe formación regular en seguridad mediante cursos de la Escuela de Administración Pública de Castilla y León, del Centro Criptológico Nacional, de empresas externas y del propio organismo pagador. Los gastos TIC del organismo pagador en 2022 ascendieron a 4,2 millones, de los cuales un 0,45% se destinaron a seguridad (19.112 euros). En 2023 los gastos TIC se incrementaron un 14% hasta los 4,8 millones, pero los destinados a seguridad (6.304 euros) disminuyeron un 67%, siendo un 0,13% del total de gastos TIC.

El Consejo de Cuentas realiza **seis recomendaciones** orientadas a contribuir a la mejora de la gobernanza en materia de ciberseguridad.