CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

INFORME Nº 326 DEL CONSEJO DE CUENTAS

Seguimiento de la aplicación de las recomendaciones realizadas al Ayuntamiento de Astorga (León) sobre seguridad informática

■ El Consejo de Cuentas analiza la evolución experimentada desde la auditoría efectuada en el ejercicio 2021

La Conferencia de Presidentes de la Asociación de Órganos de Control Externo Autonómicos aprobó en noviembre de 2018 la guía práctica de fiscalización para la revisión de los controles básicos de ciberseguridad, basados en el Esquema Nacional de Seguridad (ENS), siendo el Consejo de Cuentas uno de los primeros en incluir este tipo de auditorías en su programación.

En 2021 el Consejo de Cuentas aprobó los informes correspondientes a siete ayuntamientos de tamaño intermedio de la Comunidad: Béjar, Ciudad Rodrigo y Santa Marta de Tormes de la provincia de Salamanca; Villaquilambre, Astorga y La Bañeza de la provincia de León; y Benavente de la provincia de Zamora. El Ayuntamiento de Astorga, con una población de 10.300 habitantes a fecha 1 de enero de 2025, tiene 148 empleados como media.

El tamaño de este tipo de municipios, que implica cierta complejidad de gestión, contrasta con las escasas dotaciones de recursos humanos y materiales dedicados a su área tecnológica. Sin embargo, han tenido que adaptarse necesariamente a las nuevas tecnologías, por la generalización de su uso como herramienta de trabajo, y también por la digitalización creciente impuesta por la normativa.

En definitiva, han sufrido una transformación digital que debe hacerse cumpliendo unos requisitos mínimos de seguridad en sus sistemas de información, al ser estos el soporte de los procesos básicos de gestión que el Ayuntamiento lleva a cabo, incluyendo algunos tan relevantes como la gestión contable y presupuestaria, la recaudación de tributos o la gestión del padrón municipal.

Además, el Consejo de Cuentas debe poder confiar en los datos contenidos en los sistemas de la entidad fiscalizada, como único soporte de la información económica y financiera. Para que un sistema de información sea fiable, es necesario, aunque no suficiente, que existan controles eficientes de ciberseguridad, siendo los que se detallan en el alcance de esta fiscalización los más básicos.

La presente auditoría, de carácter operativo, tiene como objetivo principal actualizar el análisis de la situación en el ejercicio 2025 de los controles básicos de ciberseguridad en relación con la revisión realizada en 2021 y comprobar la implantación de las medidas recomendadas en la fiscalización anterior. Para ello, se estudian las actuaciones, medidas y procedimientos adoptados desde la anterior auditoría para adoptar estas recomendaciones de manera que permitan garantizar la efectiva implantación de los ocho controles básicos de ciberseguridad analizados.

Las recomendaciones realizadas en el informe anterior precisaban para ser implementadas un impulso por parte de la corporación. Se ha revisado la aplicación de estas recomendaciones y, en concreto, si se han adoptado medidas para la aprobación de un plan estratégico en materia de tecnologías de la información que incluya planificación, dotación de recursos y plazos para la aprobación de las normativas en materia de seguridad obligatorias, la subsanación de las deficiencias de carácter técnico detectadas y la realización del proceso de certificación del ENS.

Las conclusiones de este nuevo informe reflejan que los avances en el establecimiento de una gobernanza de tecnologías de la información y seguridad se limitan a la elaboración de una política de seguridad, que se encuentra en tramitación. Este avance, siendo un primer paso importante, se valora positivamente, pero no permite afirmar que haya un impulso decidido del Ayuntamiento ya que debe traducirse en acciones concretas y, sobre todo, en un plan para dirigir de forma continuada la mejora de la ciberseguridad; en particular, con la adecuación al ENS.

También se ha incluido en la relación de puestos de trabajo, un puesto de personal técnico informático, lo que permite que el Ayuntamiento cuente con al menos un recurso especializado. No obstante, siendo una mejora, no es suficiente, especialmente si no se acompaña de un análisis de las necesidades reales en esta materia y se promueve su cobertura definitiva.

Se está tramitando la aprobación de la política de seguridad, pero no se han formalizado los roles exigidos por el Esquema Nacional de Seguridad (responsable de la información, del servicio y de la seguridad), ni se ha comenzado a trabajar en actuaciones concretas derivadas de esta política, por lo que todavía no hay un proceso de adaptación estructurado, documentado y sostenido en el tiempo.

El entorno tecnológico del Ayuntamiento implica la coexistencia de varios modelos para sus sistemas más relevantes, que van desde soluciones llave en mano proporcionadas por la Diputación, a sistemas instalados en una plataforma externalizada cuyo mantenimiento se contrata a otro proveedor. Hay una dependencia importante de terceros con los que, en algunos casos, falta formalizar la prestación. En el caso de la infraestructura principal, la ausencia de contrato en vigor introduce riesgos y limita la capacidad de asegurar la aplicación de controles.

Los controles básicos de ciberseguridad definidos se evalúan según un modelo de madurez de procesos que establece seis niveles (L0 a L5). Se considera que la actividad organizativa de los controles debe alcanzar como mínimo el nivel 3 de madurez (L3), que se corresponde con un índice de cumplimiento del 80%. En el caso del Ayuntamiento de Astorga el índice de cumplimiento global ha pasado del 18% (L1) en 2021 al 20% (L1) en 2024.

De forma global, la evolución 2021-2024 muestra ausencia de mejora significativa en la mayoría de controles y un mantenimiento del nivel de madurez agregado en L1. Para progresar hacia el nivel requerido (L3), resulta imprescindible culminar la aprobación de la Política de Seguridad, asignar responsabilidades y formalizar procedimientos, además de resolver las carencias contractuales y de recursos que condicionan la implantación efectiva de los controles.

El Consejo de Cuentas realiza cuatro nuevas recomendaciones orientadas a las actuaciones necesarias para que el Ayuntamiento alcance un nivel de ciberseguridad adecuado.