CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE ZAMORA

El ámbito temporal de la fiscalización alcanza a la situación existente en el año 2025. Se trata de una auditoría de operativa o de gestión cuyo objetivo principal es verificar el funcionamiento de los controles básicos de ciberseguridad implantados por la entidad fiscalizada y, en función de los resultados, proponer recomendaciones de mejora. Así, se analizan las actuaciones, medidas y procedimientos adoptados para la implantación de ocho controles básicos de ciberseguridad, así como el grado de efectividad alcanzado.

Según la información que aparece reflejada en el estado de liquidación del presupuesto del ejercicio 2024, el importe del presupuesto definitivo de gastos e ingresos del Ayuntamiento de Zamora se elevó a 125,3 millones de euros. De acuerdo con los datos económicos, cuenta con tamaño suficiente para disponer de una estructura de tecnologías de la información y de las comunicaciones de cierta complejidad. Esta estructura permite la realización de pruebas y la comprobación *in situ* de los aspectos que sean precisos.

Los controles básicos de ciberseguridad definidos por Asocex se evalúan según un modelo de madurez de procesos que establece seis niveles. Los órganos de control externo autonómicos consideran que la actividad organizativa de los controles debe alcanzar como mínimo el nivel 3 de madurez, que implica un proceso bien definido y estandarizado. Ello equivale en la evaluación global de los controles de ciberseguridad a un índice de cumplimiento del 80%. En el caso del Ayuntamiento de Zamora, alcanza un nivel 1 de madurez, que se corresponde con un índice de cumplimiento global del 45%.

El Ayuntamiento no dispone de un plan de adecuación al Real Decreto 311/2022 para la implantación progresiva de los requisitos del Esquema Nacional de Seguridad (ENS). Asimismo, carece de una política de seguridad formalmente aprobada, lo que limita el establecimiento de un marco de gobierno de la seguridad adecuado. Adicionalmente, no consta la existencia de comités de seguridad, ni de mecanismos organizativos que permitan una adecuada coordinación.

Recomendaciones. El Consejo de Cuentas realiza 10 recomendaciones al Ayuntamiento de Zamora. Entre ellas, en línea con las recomendaciones ya realizadas a los ayuntamientos de otras capitales de provincia ya auditados, con carácter general, el alcalde debería impulsar las actuaciones necesarias para solventar los incumplimientos normativos y las deficiencias de carácter técnico que se han constatado durante la revisión de los controles.

Para esta tarea, organismos como el Centro Criptológico Nacional, la Federación Española de Municipios y Provincias o la Agencia Española de Protección de Datos publican guías detalladas que ofrecen modelos completos para la adaptación de los ayuntamientos de características similares que pueden ser tomadas como referencia para facilitar el proceso.

Además, el alcalde debería asumir y promover un compromiso firme por parte del Pleno del Ayuntamiento con el cumplimiento de la normativa, elaborando una estrategia a largo plazo, que establezca una gobernanza de tecnologías de la información adecuada. Así, se debería regularizar y reforzar la cobertura de los puestos clave de la plantilla en el ámbito de las tecnologías de la información; dotar de los recursos necesarios a la Unidad de Tecnología de

la Información y Comunicaciones; y culminar el proceso mediante la realización de auditorías o autoevaluaciones de cumplimiento del ENS, valorándose su realización conjunta con las relativas a la protección de datos personales.

Sobre el entorno tecnológico del Ayuntamiento, el alcalde debería impulsar las acciones necesarias para dotar adecuadamente los puestos contemplados en la relación de puesto de trabajo para garantizar una estructura que cumpla los principios de seguridad como función diferenciada y que tenga capacidad de asumir las tareas requeridas para la gestión de sus sistemas de información.

Además, debería formalizar el nombramiento del responsable de seguridad, asegurando su adecuada inclusión en la política de seguridad. Asimismo, se recomienda garantizar la documentación suficiente y actualizada del entorno de tecnologías de la información, con el fin de preservar el conocimiento sobre los sistemas de información con independencia de las personas que formen el servicio.

Sobre el inventario y control de activos y el uso controlado de privilegios administrativos, el alcalde debería impulsar la implantación de un inventario integral y actualizado de activos que incluya todas las tipologías relevantes y garantice la calidad e integridad de la información. Asimismo, se recomienda establecer procedimientos y herramientas que permitan la actualización automatizada o sistemática de dichos inventarios, con el fin de mejorar su fiabilidad y asegurar un control efectivo sobre los activos de la entidad. Además, debería promover una planificación a medio y largo plazo de las necesidades de renovación tecnológica para evitar la obsolescencia del *hardware* y utilización de *software* sin soporte del fabricante, asegurando una dotación presupuestaria adecuada.

Sobre el proceso continuo de identificación y corrección de vulnerabilidades**,** el responsable de seguridad deberá asumir la coordinación con el responsable del sistema en las decisiones sobre el empleo de herramientas automatizadas. Además, el alcalde debería impulsar la inclusión en la contratación de los servicios informáticos de las cláusulas que permitan realizar un control de cómo se llevan a cabo los servicios y el uso y control de los privilegios de administración de acuerdo con lo especificado en el ENS.

Sobre el cumplimiento normativo**,** el Pleno del Ayuntamiento debería liderar las actuaciones aún no iniciadas, para dotar a la entidad de las medidas delimitadas en la normativa como aspectos claves, conforme al ENS y a la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

Además, debería aprobar una normativa que garantice que el registro de actividad de los usuarios se realiza conforme al ENS y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral.