CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

INFORME 314 DEL CONSEJO DE CUENTAS

Análisis de la seguridad informática del Ayuntamiento de Soria

- **El Consejo de Cuentas es uno de los primeros órganos de control externo autonómicos en realizar este tipo de fiscalización**
- **Tras las auditorías realizadas en 2021 a siete ayuntamientos de tamaño intermedio, desde 2022 se abordan las relativas a las nueve capitales de provincia de la Comunidad**
- **Es el octavo informe de capitales, después de los referidos a Ávila, Burgos, Palencia, León, Salamanca, Segovia y Valladolid**

El Consejo de Cuentas ha entregado en las Cortes de Castilla y León el informe relativo al análisis de la seguridad informática del Ayuntamiento de Soria. La Asociación de Órganos de Control Externo Autonómicos aprobó en 2018 la guía práctica de fiscalización para la revisión de los controles básicos de ciberseguridad, siendo el Consejo de Cuentas uno de los primeros en programar este tipo de auditorías.

Tras una primera serie publicada en 2021 correspondiente a siete ayuntamientos de tamaño intermedio, desde 2022 se abordan las capitales de provincia de la Comunidad, pensando en el impacto que esta materia puede tener en la vida de los ciudadanos. Además del presente informe, ya se han aprobado los relativos a los Ayuntamientos de Ávila, Burgos, Palencia, León, Salamanca, Segovia y Valladolid.

El ámbito temporal de la fiscalización alcanza a la situación existente en el año 2024. Se trata de una auditoría 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 han analizado las actuaciones, medidas y procedimientos adoptados para la efectiva implantación de ocho controles básicos de ciberseguridad, así como el grado de efectividad alcanzado.

Dada la importancia adquirida por la administración electrónica, es fundamental que las entidades locales, especialmente las de mayor tamaño, tengan un adecuado sistema de seguridad para evitar riesgos de pérdida de datos o de imposibilidad de prestación de servicios en el caso de ataque informático.

Según la información que aparece reflejada en el estado de liquidación del presupuesto del ejercicio 2023, el importe del presupuesto definitivo de gastos e ingresos se elevó a 81,6 millones de euros. De acuerdo con los datos económicos, el Ayuntamiento 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.

El Ayuntamiento ha tenido que adaptarse necesariamente al uso de 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, ha sufrido una transformación digital que debe cumplir unos requisitos mínimos de seguridad en sus sistemas de información, al ser éstos 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.

Por otra parte, en el ejercicio de su función fiscalizadora, el Consejo de Cuentas debe poder confiar en los datos contenidos en los sistemas de la entidad fiscalizada, como único soporte existente de la información económica y financiera y para ello es necesario que existan unos controles eficientes de ciberseguridad, siendo los contemplados en esta fiscalización los más básicos.

Teniendo en cuenta que la finalidad de estos informes de auditoría es promover un cambio positivo, las recomendaciones son fundamentales a la hora de servir de guía y acicate a los ayuntamientos auditados, y pueden ser tomadas como punto de partida por otras entidades que quieran mejorar su seguridad informática.

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 Soria, alcanza un nivel 2 de madurez, que se corresponde con un índice de cumplimiento global del 61%.

El Ayuntamiento está trabajando en la adaptación al nuevo Esquema Nacional de Seguridad siguiendo el plan de adecuación elaborado y preparando la aprobación de la normativa necesaria. Asimismo, avanza en otros aspectos como la designación por parte de los proveedores de un punto o persona de contacto con el fin de analizar y supervisar los requisitos de seguridad del servicio, así como en la gestión y monitorización por parte de un centro de operaciones en seguridad o en la utilización de un sistema de gestión de información y eventos de seguridad. Es necesario continuar avanzando en la adaptación de los sistemas de información y en la implementación de las medidas definidas en el nuevo ENS.

Recomendaciones. El Consejo de Cuentas realiza 11 recomendaciones al Ayuntamiento de Soria. Entre ellas, en línea con las recomendaciones ya realizadas a los ayuntamientos de otras capitales de provincia ya auditadas, 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. Específicamente, se debería culminar el proceso mediante la realización de auditorías o autoevaluaciones de cumplimiento del ENS, valorándose su realización conjunta con las relativas a 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.

Por su parte, el responsable de seguridad debe garantizar que existe una documentación suficiente del entorno de tecnologías de la información del Ayuntamiento para asegurar que el conocimiento de los sistemas de información está disponible 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 realización de una planificación a largo plazo de las necesidades de renovación tecnológica para evitar la obsolescencia del *hardware* y utilización de *software* sin soporte del fabricante.

Sobre el proceso continuo de identificación y corrección de vulnerabilidades, el responsable de seguridad debe participar juntamente con el responsable del sistema, en las decisiones que conllevan el empleo de herramientas automatizadas.

Además, al 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 la seguridad de datos y sistemas, el Ayuntamiento debería firmar un instrumento jurídico en el que se detallen las obligaciones de las partes, el régimen aplicable y el procedimiento de actuación en relación con los servicios prestados relativos a las copias de seguridad.

En cuanto al cumplimiento normativo, el Pleno del Ayuntamiento debe seguir liderando las actuaciones ya iniciadas en lo que se refiere a llevar a cabo auditorías de seguridad periódicas sobre los sistemas de información de la entidad, de acuerdo con lo especificado en el ENS.

Además, debería aprobar una normativa que garantice que el registro de actividad de los usuarios se realiza de acuerdo con el ENS, en concreto con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral.

Finalmente, la Intervención municipal debería realizar la auditoría anual de sistemas del registro contable de facturas. Para facilitar su cumplimiento, la Intervención General de la Administración del Estado, publicó una guía marco que contiene una serie de orientaciones.