



INFORME 275 DEL CONSEJO DE CUENTAS

Análisis de la seguridad informática del Ayuntamiento de Valladolid

- **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 el pasado año se abordan las relativas a las nueve capitales de provincia de la Comunidad**
- **Es el cuarto informe de capitales de provincia, después de los referidos a Ávila, Burgos y Palencia**

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 Valladolid. La Conferencia de Presidentes de la Asociación de Órganos de Control Externo Autonómicos (Asocex) 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 el pasado ejercicio 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 y Palencia, y se encuentran en elaboración los referentes a León y Salamanca.

Se trata de una auditoría operativa 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 los controles básicos de ciberseguridad, así como el grado de efectividad alcanzado por estos controles.

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.

Los ayuntamientos objeto de la presente fiscalización cuentan con tamaño suficiente para disponer de una estructura de tecnologías de la información y de las comunicaciones de cierta complejidad. Han 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, han sufrido una transformación digital que debe cumplir unos requisitos mínimos de seguridad en sus sistemas de información, al ser estos el soporte de los procesos básicos de gestión que los ayuntamientos llevan 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 las entidades fiscalizadas, como único soporte existente de la información económica y financiera, y para ello es necesario que existan unos controles eficientes de ciberseguridad, siendo los que se detallan en el alcance de esta fiscalización, los más básicos.

Teniendo en cuenta que la finalidad de estos informes de auditoría es promover un cambio positivo, antes de su publicación se deja transcurrir un cierto tiempo para facilitar que las entidades corrijan las debilidades puestas de manifiesto. En este sentido, 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. Por parte de los entes fiscalizados se ha obtenido una recepción muy positiva a lo largo de la ejecución de los trabajos, con la aplicación inmediata de mejoras.

Los controles básicos de ciberseguridad definidos por Asocex se evalúan según el 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. Sobre dicho nivel se calcula el índice de cumplimiento que servirá de referencia para la evaluación global de los controles de ciberseguridad. El índice mínimo de madurez se considera que es el 80%.

El Ayuntamiento está trabajando en la adaptación al nuevo Esquema Nacional de Seguridad que regula el Real Decreto 311/2022, siguiendo el plan de adecuación elaborado por la Oficina Técnica de Seguridad, con el perfil de cumplimiento para municipios de gran tamaño. El Ayuntamiento de Valladolid dispone de esta Oficina Técnica de Seguridad desde octubre de 2022.

Recomendaciones. El Consejo de Cuentas realiza 10 recomendaciones al Ayuntamiento de Valladolid. Entre ellas, en línea con las recomendaciones ya realizadas a los Ayuntamientos de Ávila, Burgos y Palencia, 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 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.



Asimismo, debería impulsar la adecuada dotación de las plazas contempladas en la relación de puestos 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 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.

También 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 Esquema Nacional de Seguridad.

Por su parte, el responsable de seguridad que se determine en la política de seguridad debería garantizar que existe una documentación suficiente del entorno de tecnologías de la información del ayuntamiento para asegurar que el conocimiento sobre los sistemas de información está disponible con independencia de las personas que formen el servicio. Además, debería valorar juntamente con el responsable del sistema, el empleo de herramientas automatizadas para la detección de vulnerabilidades.

Con carácter más específico, el Consejo de Cuentas recomienda al Ayuntamiento de Valladolid que el Pleno siga liderando las actuaciones ya iniciadas para dotar a la entidad de una adecuada política de seguridad y una declaración de aplicabilidad, de acuerdo con lo especificado en el Esquema Nacional de Seguridad.

El Pleno también debería aprobar una normativa que garantice que el registro de actividad de los usuarios se realiza de acuerdo con lo establecido en el Esquema Nacional de Seguridad, 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, el alcalde debería requerir al delegado de protección de datos que supervise el cumplimiento del Reglamento General de Protección de Datos.