CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

PLAN ANUAL DE FISCALIZACIONES 2021

Análisis de la seguridad informática de los ayuntamientos de Castilla y León

■ El Consejo de Cuentas es uno de los primeros órganos de control externo autonómicos en realizar este tipo de auditoría

La Conferencia de Presidentes de la Asociación de Órganos de Control Externo Autonómicos (Asocex) aprobó en noviembre de 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 incluir este tipo de auditorías en su programación.

Se trata de una auditoría operativa cuyo objetivo principal es verificar el funcionamiento de los controles básicos de ciberseguridad implantados por las diferentes entidades fiscalizadas. Así, se han analizado las actuaciones, medidas y procedimientos adoptados para la efectiva implantación de dichos controles, así como el grado de efectividad alcanzado.

Complementariamente, las auditorías realizadas también proporcionan a los entes fiscalizados información relevante sobre su capacidad para continuar con la actividad en caso de padecer un ataque, así como propuestas sobre posibles acciones de mejora.

El desarrollo de la administración electrónica para facilitar servicios a los ciudadanos por parte de las administraciones públicas, debe ir acompañado de las medidas de seguridad necesarias para proteger los datos. La transformación digital de los ayuntamientos tiene que cumplir unos requisitos mínimos de seguridad en sus sistemas de información, al ser estos el soporte de procesos tan relevantes como la gestión contable y presupuestaria, la recaudación de tributos o el padrón municipal.

El tamaño de los municipios que han sido objeto de los informes implica cierta complejidad de gestión, que contrasta con las escasas dotaciones de recursos humanos y materiales dedicados a su área tecnológica.

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.

A cada ayuntamiento se le ha transmitido con carácter confidencial la situación detallada de los controles de seguridad auditados, con la debida prevención de la importancia de salvaguardar esa información. Por otra parte, y con carácter general, se les ha transmitido una serie de recomendaciones básicas para cualquier administración pública.

Los controles básicos de ciberseguridad definidos por Asocex se evalúan según el modelo de madurez de procesos, que define 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 este nivel 3 de madurez, se calcula el índice de cumplimiento que servirá de referencia para la evaluación global de los controles de ciberseguridad. El nivel mínimo de madurez se considera que es del 80%.

Entre las recomendaciones que realiza el Consejo de Cuentas, las principales van orientadas a obtener de los máximos órganos directivos una implicación en el fortalecimiento de la seguridad en sus ayuntamientos y, en concreto, el concejal competente por razón de la materia 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.

Por su parte, 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 que contemple las siguientes iniciativas:

- Aprobar una política de seguridad que defina claramente las responsabilidades sobre la seguridad de los servicios que ofrece y la información que maneja, permitiendo dar continuidad al esfuerzo de adaptación necesario para el cumplimiento normativo.

- Dotar de recursos al departamento de tecnologías de la información para solventar aquellos aspectos técnicos que precisan mejoras.

- Específicamente, se deberá culminar el proceso mediante la realización de auditorías o autoevaluaciones de cumplimiento del Esquema Nacional de Seguridad, valorándose su realización conjunta con las relativas a protección de datos personales.

Un aspecto básico que permitirá comenzar a estructurar y documentar el proceso de seguridad informática debería ser el nombramiento por parte del alcalde de los responsables en el Ayuntamiento de velar por la aplicación efectiva de la política de seguridad.