CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

Nota informativa | 11 marzo 2024

Las auditorías de ciberseguridad de los ayuntamientos de Salamanca y León recogen un total de 17 recomendaciones para promover un "cambio positivo" y "mitigar los ataques más comunes"

- **El presidente de Consejo de Cuentas, Mario Amilivia, constata que ambos ayuntamientos están poniendo ya en marcha diversas medidas para el cumplimiento de las recomendaciones**
- **En la presentación de los dos informes en las Cortes, subraya la disponibilidad de la Comisión de Economía y Hacienda para mantener la mayor actualidad posible de los trabajos**
- **Amilivia llega al medio centenar de comparecencias en el presente mandato de la institución de control externo, iniciado en 2019, en las que ya ha presentado un total de 124 informes**

El presidente del Consejo de Cuentas de Castilla y León, Mario Amilivia, presentó hoy en su sexta comparecencia del año ante la Comisión de Economía y Hacienda del Parlamento autonómico dos informes, los de análisis de la seguridad informática de los ayuntamientos de Salamanca y de León. Dos auditorías que fueron aprobadas en octubre y diciembre del año pasado, respectivamente, y que, como recordó, ya fueron mencionadas en el debate suscitado en esta Comisión el pasado 29 de enero con ocasión de la presentación del análisis referido a la seguridad informática del Ayuntamiento de Valladolid.

Con esta son ya 50 las comparecencias de Amilivia en el actual mandato, prácticamente la mitad de las 104 que han tenido lugar en toda la serie histórica. En este medio centenar de sesiones ha expuesto un total de 124 informes, representando el 44% de todos los aprobados en los 21 años de la institución autonómica de control externo.

En este sentido, solo restan 8 informes pendientes de comparecencia y, por otro lado, hay 59 trabajos en diferentes fases de tramitación, "lo que da cuenta del constante volumen de actividad de la institución", remarcó.

La revisión de los controles básicos de ciberseguridad según la más actual metodología internacional en esta materia sitúa al Consejo de Cuentas a la vanguardia en estas auditorías. En 2021 se publicó una primera serie de siete ayuntamientos de tamaño intermedio para después abordar los análisis de las capitales de provincia por el impacto de esta materia en la vida de los ciudadanos.

En esta línea, ya se han presentado los de Ávila, Burgos, Palencia y Valladolid, y la serie de completará con los previstos en el Plan de Fiscalizaciones de este año

para los ayuntamientos de Segovia, Soria y Zamora. Trabajos que, subrayó, "proponen recomendaciones de mejora, es decir, promover un cambio positivo". Añadió que se trata de "recomendaciones fundamentales a la hora de servir de guía y acicate a los ayuntamientos auditados, que pueden ser tomadas como punto de partida por otras entidades que quieran mejorar se seguridad informática".

Como resumen general de las presentaciones de las auditorías de Salamanca y León, Amilivia destacó que "ambos ayuntamientos están poniendo en marcha medidas para el cumplimiento de las recomendaciones". Son, añadió, dos informes de carácter operativo con la finalidad fundamental de "mejorar la situación previa".

Análisis de ciberseguridad del Ayuntamiento de Salamanca. En primer lugar, precisó que la auditoría se circunscribió a la verificación de las actuaciones, medidas y procedimientos adoptados para la implantación de los controles básicos de ciberseguridad y su grado de eficacia. La entidad presentó alegaciones, destacando literalmente "la precisión y el rigor con el que se han llevado a cabo los trabajos de auditoría, así como el alto nivel de competencia y profesionalidad que han demostrado los auditores para plasmar una visión clara de la situación actual de la seguridad informática del Ayuntamiento".

Resumidamente, se realizaron 45 conclusiones tras el análisis. Con relación al entorno tecnológico y sistemas de información, se subraya, por ejemplo, que la concejalía que tiene atribuidas las competencias en materia de informática realiza acciones para una dirección efectiva de la política de seguridad informática, pero presenta carencias importantes, especialmente en el ámbito de impulso a la aprobación de una política de seguridad y del nombramiento de los principales responsables de la gestión y seguridad en esta materia.

El ayuntamiento tiene 20 puestos relacionados con las tecnologías de la información, estando cubiertos 15, y con varios procesos selectivos para cubrir las vacantes. Por otro lado, dispone de documentación de sus sistemas y procesos de gestión y ha realizado una identificación y categorización según el Esquema Nacional de Seguridad (ENS) de los sistemas de información de que dispone.

Los equipos son controlados por la propia entidad, excepto la página web. Respecto a la estructura de la red corporativa, tiene en general, dada su dimensión, un sistema con una adecuada protección perimetral, redundancia en los accesos a internet, equipamiento y configuración de la red local. También dispone de soluciones de teletrabajo y acceso remoto permitiendo un nivel de seguridad adecuado.

Con relación a la implantación de los controles básicos de ciberseguridad definidos por la Asociación de Órganos de Control Externo autonómicos, estos se evalúan según el modelo de madurez de procesos estableciendo seis niveles (de 0 a 5). De esta manera, se considera que la actividad organizativa de los controles debe alcanzar como mínimo el nivel 3 de madurez, lo que implica un "proceso bien definido y estandarizado".

Los controles abordaron el inventario y control de dispositivos físicos: inventario y control de software autorizado y no autorizado: proceso continuo de identificación y corrección de vulnerabilidades: uso controlado de privilegios administrativos; configuraciones seguras del software y hardware de dispositivos y equipos; registro

de la actividad de los usuarios; copias de seguridad de datos y sistemas y cumplimiento normativo.

A la vista de los resultados, la situación global de los controles básicos de ciberseguridad de la entidad presenta un nivel de madurez L2. A su vez, el índice de cumplimiento es del 79%, alcanzando prácticamente el nivel de madurez L3, que se corresponde con una puntuación del 80% como objetivo mínimo deseable.

Las cinco recomendaciones del Consejo van dirigidas, con carácter general, a que el alcalde debería impulsar las actuaciones necesarias para solventar los incumplimientos normativos y las deficiencias de carácter técnico constatadas durante la revisión de los controles.

Asimismo, este debería asumir y promover un compromiso firme por parte del Pleno con el cumplimiento de la normativa, elaborando una estrategia a largo plazo, que establezca una gobernanza de tecnologías de la información adecuada.

Por otra parte, con relación al inventario y control de activos y el uso controlado de privilegios administrativos, el alcalde debería impulsar una planificación a largo plazo de las necesidades de renovación tecnológica; y sobre el proceso continuo de identificación y corrección de vulnerabilidades, debería impulsar en la contratación de los servicios informáticos cláusulas que permitan controlar 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.

En cuanto al cumplimiento normativo, se recomienda que el Pleno debe seguir liderando las actuaciones ya iniciadas en lo referido a dotar a la entidad de una adecuada política de seguridad y una estructura del departamento de tecnologías de la información acorde y que permita cumplir el principio de “seguridad como responsabilidad diferenciada”.

Análisis de la seguridad informática del Ayuntamiento de León. A continuación, presentó este informe, que fue remitido al Parlamento autonómico el pasado 10 de enero.

Al igual que el anterior, se trata de una auditoría operativa cuyo objetivo central es verificar el funcionamiento de los controles básicos de ciberseguridad implantados por la entidad y, en función de los resultados, proponer recomendaciones de mejora, que fueron en este caso doce. Desde el punto de vista temporal se analiza la situación existente hasta el ejercicio 2023, sin perjuicio de las comprobaciones sobre actuaciones anteriores. Además de señalar la disponibilidad y colaboración del personal encargado de las funciones TIC del ayuntamiento, resaltó, de acuerdo con las evidencias aportadas tras los trabajos de campo, la voluntad y trabajo de la entidad en la mejora y desarrollo de un ámbito tan específico y complejo como es el de la seguridad informática.

Del análisis realizado, se extraen 52 conclusiones, precisó Amilivia. Entre ellas, que la concejalía que tiene atribuidas las competencias no realiza las acciones necesarias para una dirección efectiva de la política de seguridad informática, especialmente en el ámbito de impulso de la cobertura de plazas y del nombramiento de los principales responsables. Existen 23 puestos relacionados con las TICs, estando cubiertos 14 de ellos.

El ayuntamiento carece de documentación detallada de sus sistemas y procesos de gestión, sin un plan de actuación ante un cambio en el equipo de trabajo. Tampoco ha realizado una identificación y categorización adecuada según el ENS de los sistemas de información de que dispone.

Además, se ha optado en su mayor parte por un modelo mixto de gestión, con una parte de los servicios y de la información residenciada en equipos controlados por la propia entidad e instalados físicamente en sus dependencias, y otra parte externalizada en el Centro de Supercomputación de Castilla y León.

Del examen de la estructura de la red corporativa, se concluye que tiene en general, dada su dimensión, un sistema con una adecuada protección perimetral, redundancia en los accesos a internet, equipamiento y configuración de la red local. Aunque se observan algunas carencias referidas a la ubicación de cierto equipamiento ante posibles contingencias. La conexión inalámbrica es adecuada en líneas generales, aunque en algunas localizaciones carece de las medidas de seguridad necesarias para gestionar los accesos y su trazabilidad.

También, dispone de una plataforma de teletrabajo teóricamente capaz de proporcionar un nivel suficiente de seguridad.

Con relación a la implantación de los controles básicos de ciberseguridad (se establecen 6 niveles, de 0 a 5), se considera que el ayuntamiento, en 7 de los 8 controles registra un índice de madurez L1, lo que significa que "*el proceso existe, pero no se gestiona. El éxito del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una emergencia*".

Solo en el control 7, que revisa las copias de seguridad de datos y sistemas, el consistorio alcanza un índice de madurez L2, en el que *"existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias, pero es impredecible el resultado si se dan circunstancias nuevas*".

A la vista de los resultados, la situación global de los controles básicos de ciberseguridad presenta un nivel de madurez L1 (se considera que la actividad organizativa de los controles debe alcanzar como mínimo el nivel 3 de madurez, que implica un proceso bien definido y estandarizado), con un índice de cumplimiento del 47%, siendo el 80% el objetivo mínimo deseable.

El ayuntamiento está trabajando en la adaptación a la nueva regulación del ENS, siguiendo el plan de adecuación elaborado, alineado con el perfil de cumplimiento para ayuntamientos de gran tamaño. En esta línea, la propia entidad destaca la creación de un Centro de Operaciones de Seguridad.

Las recomendaciones del Consejo pasan, en primer lugar, porque el alcalde impulse las actuaciones necesarias para solventar los incumplimientos normativos y las deficiencias técnicas constatadas durante la revisión de los controles.

También, este 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, solventando la situación en cuanto a plazas relevantes como son las de responsable de seguridad o jefe de servicio; dotar de los recursos necesarios al Servicio de Recursos para la Información y las Comunicaciones, y

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.

En segundo lugar, con relación al entorno tecnológico del ayuntamiento el alcalde debería impulsar las acciones necesarias para dotar adecuadamente los puestos contemplados 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 según el modelo mixto adoptado. Por su parte, el responsable de seguridad debe garantizar que existe una documentación suficiente del entorno de tecnologías de la información del ayuntamiento.

En tercer lugar, 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, asegurando una dotación presupuestaria adecuada.

En cuarto lugar, en cuanto al 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 para la detección de vulnerabilidades.

Por su parte, 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.

En quinto lugar, en lo referido a copias de seguridad de datos y sistemas, la recomendación es que el responsable de seguridad debe impulsar de forma inmediata las acciones necesarias para que se firme por parte del ayuntamiento un instrumento jurídico en el que se detallen las obligaciones de las partes, el régimen aplicable y el procedimiento de actuación en relación con la fundación Supercomputación de Castilla y León.

Finalmente, en cuanto al cumplimiento normativo, el Pleno municipal debe seguir liderando las actuaciones en lo referido a dotar a la entidad de una declaración de aplicabilidad, de acuerdo con lo especificado en el ENS.

El alcalde, por su parte, debería requerir al delegado correspondiente la supervisión del cumplimiento del Reglamento General de Protección de Datos.

El Pleno debería aprobar una normativa que garantice que el registro de actividad de los usuarios se realiza de acuerdo con lo establecido en el ENS y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral.

Por último, la Intervención municipal debería realizar la auditoría anual de sistemas de registro contable de facturas.

En el transcurso del debate suscitado en la Comisión tras la exposición de las recomendaciones de ambos análisis, Amilivia apuntó que el Consejo de Cuentas tiene constancia de que el Ayuntamiento de Salamanca ha convocado 5 plazas (3 de

auxiliares y 2 de analistas programadores) para el refuerzo de este área y que en relación con el Ayuntamiento de León se han convocado también las plazas para los nombramientos de un Jefe de Servicios Informáticos y de un Responsable de Seguridad en esta materia.

También, en el ámbito del Ayuntamiento de León, el Consejo tiene constancia de la reciente adjudicación de un contrato de infraestructura "MAN segura" que tiene por objeto el suministro, instalación y puesta en servicio de los equipos de electrónica de red necesarios para renovar la red corporativa, así como los servicios asociados a los mismos.

El Consejo de Cuentas también es conocedor del propósito del Ayuntamiento de León de seguir invirtiendo y mejorando en esta materia. Así, "hemos podido constatar el propósito de invertir una cantidad superior a los 2,6 millones de euros con cargo a los remanentes de tesorería para gastos generales en el área de Informática. Acuerdo que, en su caso, se incluirá en un próximo Pleno". Con ello, "manifestamos esa voluntad de mejora, que es la que persigue el informe", concluyó.

www.consejodecuentas.es

+INFO 649979174

Para ampliar la información, aquí los informes:

➔ Ayto de Salamanca

➔ Ayto León