CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

Nota informativa | **5 junio 2023**

El Consejo de Cuentas constata proyectos en marcha en los ayuntamientos de Ávila, Burgos y Palencia que fortalecen sus políticas de ciberseguridad

■ Amilivia presenta las auditorías de seguridad informática de los consistorios, que recogen un total de 31 recomendaciones

"Los ayuntamientos de Ávila, Burgos y Palencia están avanzando en el refuerzo de sus políticas de ciberseguridad con la puesta en marcha de proyectos gracias a la financiación propiciada por los fondos europeos". Así lo afirmó hoy el presidente del Consejo de Cuentas de Castilla y León, Mario Amilivia, en su comparecencia ante la Comisión de Economía y Hacienda del Parlamento autonómico para presentar los informes relativos al análisis de la seguridad informática de los citados ayuntamientos.

"Proyectos que, además de permitir que las administraciones realicen un uso más eficiente de las nuevas tecnologías en favor de los ciudadanos, es decir, progresando en transparencia, contribuyen decisivamente a hacer frente a las constantes amenazas y brechas de seguridad en internet", valoró.

Teniendo en cuenta que la finalidad de las auditorías realizadas a los tres ayuntamientos citados es promover un cambio positivo, se dejó transcurrir un cierto tiempo antes de su publicación para facilitar que las entidades corrigieran las debilidades que se pusieron de manifiesto.

En esta línea, Amilivia afirmó que el Consejo de Cuentas es uno de los primeros órganos de control externo autonómicos en programar este tipo de auditorías. Tras una primera serie publicada en 2021 sobre siete ayuntamientos de tamaño intermedio, se están abordando en la actualidad las capitales de provincia de Castilla y León atendiendo al impacto que esta materia puede tener en la vida de las personas. Así, además de los tres informes presentados hoy, se encuentran en elaboración los referentes a los ayuntamientos de León, Salamanca y Valladolid.

El Consejo de Cuentas, explicó, ha analizado las actuaciones, medidas y procedimiento 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", apuntó.

Ayuntamientos como Ávila, Burgos y Palencia 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. 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, lo que hace necesaria la existencia de controles eficientes de ciberseguridad, siendo los que se detallan en el alcance de estas tres fiscalizaciones referidas al ejercicio 2022 los más básicos.

Las 31 recomendaciones recogidas por el Consejo de Cuentas en las tres auditorías (12 al Ayuntamiento de Ávila; 8 al de Burgos y 11 al de Palencia) se han demostrado “fundamentales” a la hora de servir de guía y acicate a los consistorios auditados, pudiendo ser tomadas como punto de partida por otras entidades que quieran mejorar su seguridad informática. Destaca, por ser común a los tres ayuntamientos, la necesidad de implicación de los máximos órganos directivos como único camino para obtener resultados efectivos, desterrando la idea de la seguridad como una responsabilidad del personal de tecnologías de la información exclusivamente.

El Consejo, significó, “quiere destacar la disponibilidad y colaboración del personal encargado de las funciones de las nuevas tecnologías de la información, independientemente de las incidencias detectadas en los respectivos informes”. “Quiero dejar constancia -prosiguió- de que en ningún caso las conclusiones ponen en cuestión su capacidad o profesionalidad, considerándose que las conclusiones se dirigen a problemas de diseño o de inversión en medios humanos y materiales”.

Ocho controles básicos

Las auditorías se refieren a la verificación de las actuaciones, medidas y procedimientos adoptados para la implantación de los controles básicos de ciberseguridad y su grado de eficacia. Así, se realizaron 8 controles verificando, por un lado, si se gestionan activamente todos los dispositivos hardware de la red; el inventario y control de software autorizado y no autorizado; la disposición de un proceso para obtener información sobre nuevas vulnerabilidades, reduciendo así la ventana de oportunidad a los atacantes; y, por otro, el chequeo a la disposición de herramientas control, prevención y corrección del uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones; la configuración de seguridad de dispositivos; el análisis sobre registros de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque; la verificación sobre la realización de copias de seguridad de la información crítica y, por último, el cumplimiento normativo.

Conclusiones

Varias de las conclusiones se refieren a asuntos como la dotación de puestos relacionados con las TIC, la gestión de los equipos, la estructura y dimensión de los sistemas o las conexiones y plataformas. Con relación a la implantación de los controles básicos de ciberseguridad, los resultados reflejan deficiencias generalizadas en la mayoría de los controles, no alcanzando ninguno de los 3 ayuntamientos un nivel de seguridad adecuado en el momento de realizarse la auditoría. Los controles básicos de ciberseguridad definidos por la Asociación de

Órganos de Control Externo Autonómicos se evalúan según el modelo de madurez de procesos, que establece 6 niveles, de cero a cinco.

De esta manera, 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. Los ayuntamientos de Burgos y Palencia reflejan un nivel de madurez 2, quedándose el de Ávila en un nivel 1.

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%, pues bien, el ayuntamiento de Burgos alcanza un 67%, el de Palencia un 65% y el de Ávila un 43%.

De los controles revisados destaca como el mejor implantado en los 3 ayuntamientos el número 7, que corresponde a las copias de seguridad, solo superado en el caso de Burgos por el control 8, dedicado a aspectos normativos que, por contra, es el que peor resultado obtiene en los consistorios de Ávila y Palencia.

Recomendaciones

En primer lugar, dos recomendaciones generales están dirigidas a los tres ayuntamientos. 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, comenzando por:

- 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 Tecnología de la Información para solventar aquellos aspectos técnicos que precisan mejoras, no cubriendo las necesidades mediante personal sin vinculación laboral.

- Específicamente, se debería 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.

Por otro lado, se deberían 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.

También como recomendaciones generales, en los casos de los ayuntamientos de Ávila y Palencia, un aspecto básico para comenzar a estructurar y documentar el proceso de seguridad informática debería ser el nombramiento por parte del alcalde del responsable de la información, del responsable del servicio y del responsable de la seguridad. Con estos nombramientos y el apoyo y concienciación política al más alto nivel se podrá proceder al desarrollo de la estructura y procedimientos necesarios.

Finalmente, también en los ayuntamientos de Ávila y Palencia, el responsable de seguridad que se determine, en coordinación con el responsable del sistema para cada proceso de gestión de Tecnología de la Información, debería elaborar y elevar a su aprobación formal el procedimiento que describe cada proceso en concreto, detallando el alcance, tareas a realizar, responsabilidades, registros o documentación que se genere, así como cualquier otro aspecto relevante.

Acciones específicas para cada una de las áreas:

Sobre el entorno tecnológico del Ayuntamiento:

-En los tres ayuntamientos, se 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.

-También en los tres ayuntamientos, el responsable de seguridad que se determine 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.

Sobre el inventario y control de activos (hardware y software) y el uso controlado de privilegios administrativos:

-En los tres ayuntamientos, se 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.

Sobre el proceso continuo de identificación y corrección de vulnerabilidades:

-También en los tres ayuntamientos, el concejal competente 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 debería valorar junto con el responsable del sistema, el empleo de herramientas automatizadas para la detección de vulnerabilidades y la realización de pruebas que simulan ataques reales.

Sobre el cumplimiento normativo en materia de protección de datos:

-En el caso de los ayuntamientos de Ávila y Burgos, el Pleno debe liderar la adopción de todas aquellas medidas aún no iniciadas y que están delimitadas como aspectos claves en la normativa sobre el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en la de Protección de Datos Personales y garantía de los derechos digitales. Entre otras, el llevar a cabo una adecuada política de seguridad y una declaración de aplicabilidad.

-En el caso del Ayuntamiento de Palencia, el Pleno debe seguir liderando estas actuaciones ya iniciadas.

-Como recomendación única para el Ayuntamiento de Ávila, 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 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. Para ello podría utilizarse como referencia la guía del Centro Criptológico Nacional, relativa al Registro de la actividad de los usuarios.

-Por último, en los ayuntamientos de Ávila y Palencia 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 a efectos de su realización.