



COMISIÓN DE ECONOMÍA Y HACIENDA

PRESIDENCIA

DON JOSÉ ALBERTO CASTRO CAÑIBANO

Sesión celebrada el día 2 de junio de 2025, en Valladolid

ORDEN DEL DÍA

1. Comparecencia del Excmo. Sr. Presidente del Consejo de Cuentas de Castilla y León para la presentación del Informe “Seguimiento de recomendaciones y actualización de la situación de seguridad informática del Ayuntamiento de Béjar (Salamanca)”, del Consejo de Cuentas de Castilla y León.
2. Comparecencia del Excmo. Sr. Presidente del Consejo de Cuentas de Castilla y León para la presentación del Informe “Seguimiento de recomendaciones y actualización de la situación de seguridad informática del Ayuntamiento de Ciudad Rodrigo (Salamanca)”, del Consejo de Cuentas de Castilla y León.
3. Comparecencia del Excmo. Sr. Presidente del Consejo de Cuentas de Castilla y León para la presentación del Informe “Seguimiento de recomendaciones y actualización de la situación de la seguridad informática del Ayuntamiento de Benavente (Zamora)”, del Consejo de Cuentas de Castilla y León.

SUMARIO

	Páginas
Se inicia la sesión a las diecisiete horas.	22889
El presidente, Sr. Castro Cañibano, abre la sesión.	22889
Intervención de la procuradora Sra. Gallego González (Grupo UPL-SORIA ¡YA!) para comunicar sustituciones.	22889
Intervención de la procuradora Sra. Suárez Villagrá (Grupo VOX Castilla y León) para comunicar sustituciones.	22889
Intervención del procurador Sr. Beltrán Martín (Grupo Popular) para comunicar sustituciones.	22889
El presidente, Sr. Castro Cañibano, comunica que, por acuerdo de los portavoces, se unifican los tres puntos del orden del día.	22889

**Páginas****Puntos primero, segundo y tercero del orden del día.**

La secretaria, Sra. Vallejo Quevedo, da lectura al primer, segundo y tercer puntos del orden del día.	22889
Intervención del Sr. Amilivia González, presidente del Consejo de Cuentas de Castilla y León, para informar a la Comisión.	22890
El presidente, Sr. Castro Cañibano, abre un turno para la formulación de preguntas u observaciones por parte de los portavoces de los grupos parlamentarios.	22896
En turno de portavoces, interviene la procuradora Sra. Gallego González (Grupo UPL-SORIA ¡YA!).	22896
En turno de portavoces, interviene la procuradora Sra. Suárez Villagrá (Grupo VOX Castilla y León).	22898
En turno de portavoces, interviene la procuradora Sra. Rubio Martín (Grupo Socialista).	22900
En turno de portavoces, interviene el procurador Sr. Beltrán Martín (Grupo Popular).	22903
Intervención del Sr. Amilivia González, presidente del Consejo de Cuentas de Castilla y León, para responder a las cuestiones planteadas.	22904
En turno de réplica, interviene la procuradora Sra. Gallego González (Grupo UPL-SORIA ¡YA!).	22906
En turno de réplica, interviene la procuradora Sra. Rubio Martín (Grupo Socialista).	22907
En turno de réplica, interviene el procurador Sr. Beltrán Martín (Grupo Popular).	22907
En turno de dúplica, interviene el Sr. Amilivia González, presidente del Consejo de Cuentas de Castilla y León.	22908
El presidente, Sr. Castro Cañibano, levanta la sesión.	22909
Se levanta la sesión a las dieciocho horas cinco minutos.	22909



[Se inicia la sesión a las diecisiete horas].

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Buenas tardes, señorías. Se abre la sesión. ¿Algún grupo parlamentario quiere comunicar alguna sustitución? ¿Por el Grupo Parlamentario UPL-Soria ¡Ya!?

LA SEÑORA GALLEGO GONZÁLEZ:

Sí. Gracias, presidente. Alicia Gallego en sustitución de José Ramón García.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

¿Por el Grupo Vox Castilla y León?

LA SEÑORA SUÁREZ VILLAGRÁ:

Sí. María Luisa Calvo sustituye a José Antonio Palomo.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

¿Por el Grupo Parlamentario Popular?

EL SEÑOR BELTRÁN MARTÍN:

Sí. Pablo Trillo-Figueroa Martínez-Conde sustituye a Noemí Rojo Sahagún y Antonio Mendoza Toribio sustituye a Rosa María Esteban Ayuso.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Tenemos el honor y el gusto hoy de estar nuevamente acompañados por el presidente del Consejo de Cuentas y todos los miembros que le acompañan, un nutrido grupo que siempre tiene el honor de venir a esta Comisión.

Se ha decidido, en... en comunicación con todos los portavoces, unificar, al ser temas semejantes, homólogos, en un único punto los tres. Por eso vamos a proceder a la lectura de los tres puntos seguidos. Seremos más flexibles en cuanto a... a la disposición del tiempo. Quedamos... para intentar, siendo homogéneos, siendo parecidos los temas, el presidente del Consejo de Cuentas no tiene tiempo y el resto de los portavoces, en este caso, tendrán como... más de quince minutos si quieren, sin ningún tipo de... de problema.

Tiene la palabra la señora secretaria para la lectura del orden del día.

Informes

LA SECRETARIA (SEÑORA VALLEJO QUEVEDO):

Gracias, presidente. Señorías, buenas tardes. Procedo a dar lectura de forma conjunta a los tres puntos del orden del día: **Comparecencia del excelentísimo señor presidente del Consejo de Cuentas de Castilla y León para presentación del Informe “Seguimiento de recomendaciones y actualización de la situación de seguridad informática del Ayuntamiento de Béjar (Salamanca)”**; **“Seguimiento**



de recomendaciones y actualización de la situación de seguridad informática del Ayuntamiento de Ciudad Rodrigo (Salamanca)”; “Seguimiento de recomendaciones y actualización de la situación de la seguridad informática del Ayuntamiento de Benavente (Zamora)”, del Consejo de Cuentas de Castilla y León. Muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Para la presentación de estos informes, tiene la palabra don Mario Amilivia González, sin límite de tiempo. Muchas gracias.

EL PRESIDENTE DEL CONSEJO DE CUENTAS DE CASTILLA Y LEÓN (SEÑOR AMILIVIA GONZÁLEZ):

Muy buenas tardes. Gracias, presidente, por sus palabras de bienvenida en nombre propio, en nombre del Pleno del Consejo de Cuentas y de los miembros del... del equipo que me... que me acompañan.

Esta es la octava comparecencia del año y voy a presentar tres fiscalizaciones en materia de ciberseguridad correspondientes al sector público local, departamento que –como saben sus señorías– dirige el consejero Emilio Melero, que en esta ocasión ha contado con la coordinación técnica de la auditora informática Marisol González, que también nos acompaña.

Se trata en los tres informes del seguimiento de las recomendaciones sobre seguridad informática realizadas en las auditorías llevadas a cabo en dos mil veintiuno en los Ayuntamientos de Béjar y de Ciudad Rodrigo en la provincia de Salamanca y Benavente, en Zamora, así como el análisis y evaluación de su situación actual. El primero de ellos fue aprobado el... el pasado veintiuno de noviembre; el segundo, el treinta de diciembre; y el tercero ya este año: el ocho de mayo. Como es habitual, seguidamente fueron remitidos a estas Cortes y publicados en la página web de la Institución.

Tras esta sesión, quedan nueve informes a la espera de ser presentados: dos de ellos fueron aprobados en los dos últimos meses de dos mil veinticuatro –Cuenta General y endeudamiento– y los otros siete corresponden al presente ejercicio. En estos momentos, la actividad de la Institución comprende 52 trabajos en diferentes estados de tramitación. Así, hasta la fecha, son 67 las comparecencias celebradas durante el actual mandato, con 144 informes de los 297 presentados por el Consejo de Cuentas en toda su serie histórica; es decir, el 48 % del total.

Entrando ya en el contenido de los informes, quiero recordar, en primer lugar, que la Conferencia de Presidentes de la Asociación de Órganos de Control Externo Autonómico aprobó, en noviembre de dos mil dieciocho, la Guía práctica de fiscalización para la revisión de los controles básicos de ciberseguridad, basados en el Esquema Nacional de Seguridad, recientemente objeto de actualización en el año dos mil veintidós, siendo el Consejo de Cuentas, en este sentido, uno de los primeros en incluir este tipo de auditorías en su programación.

El Plan Estratégico del Consejo de Cuentas estableció el objetivo de acercar sus informes a las inquietudes sociales, y, en dicho sentido, parece incuestionable que la seguridad informática ha pasado a formar parte de las preocupaciones presentes y ordinarias en la sociedad actual. Así, en dos mil veintiuno, el Consejo



de Cuentas aprobó los informes correspondientes a siete ayuntamientos de tamaño intermedio de la Comunidad: Béjar, Ciudad Rodrigo y Santa Marta de Tormes, en la provincia de Salamanca; Villaquilambre, Astorga y La Bañeza, de la provincia de León; y Benavente, de la provincia de Zamora.

Con independencia del informe de seguimiento de recomendaciones a los entes fiscalizados que el Consejo de Cuentas realiza en su informe anual, se consideró oportuno llevar a cabo un seguimiento específico de estas siete primeras auditorías informáticas, eso sí, una vez transcurrido un período de tiempo suficiente para la implantación de las mejoras propuestas. Las que hoy presentamos son las tres ya aprobadas, mientras las cuatro restantes se encuentran en elaboración y será mi propósito también, en su día, presentarlas conjuntamente.

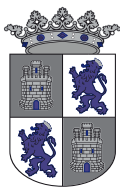
Con carácter previo, señalar que el Ayuntamiento de Béjar, con una población de 12.021 habitantes a fecha de uno de enero de dos mil veintitrés, tiene una plantilla media de 262 empleados. Por su parte, el de Ciudad Rodrigo tiene 11.810 habitantes y dispone de una plantilla de 141 empleados. En cuanto a Benavente, municipio con 17.246 habitantes a fecha uno de enero de dos mil veinticuatro, su ayuntamiento cuenta con una plantilla compuesta por 214 empleados.

El tamaño de este tipo de municipios, que implica cierta complejidad de gestión, contrasta, no obstante, con las escasas dotaciones de recursos humanos y materiales dedicados a su área tecnológica. No obstante, estas limitaciones 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 inevitable digitalización impuesta por la normativa.

En definitiva, los ayuntamientos fiscalizados han sufrido una transformación digital que debe hacerse cumpliendo unos requisitos mínimos de seguridad en sus sistemas de información, al ser estos el soporte de los procesos básicos de gestión; procesos básicos de gestión tan importantes y relevantes como la gestión contable y presupuestaria, la recaudación de tributos o la gestión del padrón municipal.

Además, el Consejo de Cuentas, desde el punto de vista de su función fiscalizadora, debe poder confiar en los datos contenidos en los sistemas de la entidad fiscalizada como único soporte de su información económica y financiera. Y 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 este informe los más básicos.

Estas tres auditorías, de carácter operativo, tienen como objetivo principal actualizar el análisis de la situación de los controles básicos de ciberseguridad en relación con la revisión realizada en dos mil veintiuno y comprobar la implantación de las medidas recomendadas en la fiscalización anterior, de manera que permitan garantizar la efectiva implantación de los 8 controles básicos de ciberseguridad analizados. Recordar que dichos controles analizan los siguientes aspectos: primero, inventario y control de dispositivos físicos; segundo, inventario y control de *software* autorizado y no autorizado; proceso continuo de identificación y corrección de vulnerabilidades; uso controlado de privilegios administrativos; configuraciones seguras de *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores; registro de la actividad de los usuarios; copias de seguridad de datos y sistemas; y, finalmente, cumplimiento normativo.



Las recomendaciones realizadas en el informe anterior precisaban para su ejecución de un impulso por parte de las respectivas corporaciones municipales. En ese sentido, se ha revisado la aplicación efectiva de estas recomendaciones y, en concreto, si se han adoptado medidas para la aprobación de un plan estratégico en materia de tecnologías de la información que incluya planificación, dotación de recursos y plazos para la aprobación de las normativas en materia de seguridad obligatoria, la subsanación de deficiencias de carácter técnico detectadas y la realización del proceso de certificación del Esquema Nacional de Seguridad.

Antes de abordar el resultado de las auditorías, quiero dejar constancia de que no han existido limitaciones y que, en tal sentido, el Consejo de Cuentas quiere destacar la disponibilidad y colaboración del personal municipal, independientemente de las incidencias detectadas. También dejar patente que en ningún caso las conclusiones ponen en cuestión la capacidad o profesionalidad de dichos trabajadores, considerándose que las conclusiones aluden a problemas de diseño o de inversión en medios humanos y materiales. En cuanto al trámite de alegaciones, no hubo alegaciones. Solo las presentó Benavente, pero realmente no fue considerada como tal.

A continuación, procedo a exponer ya sintéticamente las principales conclusiones relativas a cada uno de los ayuntamientos.

Comienzo por Béjar. El ayuntamiento sigue careciendo de una estrategia de tecnologías de la información y no ha establecido una gobernanza adecuada que le permita afrontar con garantías el proceso de dotar a sus sistemas de información de un nivel de seguridad suficiente.

Las actuaciones realizadas para cumplir con las recomendaciones en su primer informe se concretan en las siguientes mejoras. En primer lugar, creación de una plaza de técnico informático, aunque actualmente sin cubrir; el personal responsable de tecnologías de la información del ayuntamiento se reduce a una persona contratada con carácter temporal. En segundo término, la adquisición de equipos y contratación de servicios que mejoran la seguridad de la red. Y, finalmente, la inclusión de cláusulas específicas en los contratos de servicios informáticos para cumplir determinadas medidas de seguridad.

El Ayuntamiento de Béjar, como se puso de manifiesto en la anterior auditoría, se encontraba en una situación muy vulnerable frente a riesgos informáticos. En los tres años transcurridos -quiero manifestar- ha comenzado a tomar algunas medidas para revertir la situación, mejorando su calificación global; aunque tengo también que manifestar que estas medidas aún... aún son insuficientes, siendo imprescindible un impulso para conseguir un nivel de seguridad adecuado y garantizar el cumplimiento de la normativa.

Los controles básicos de ciberseguridad -como recordarán sus señorías- se evalúan según un modelo de madurez de procesos que establece 6 niveles, del nivel 0 o L... LO, L0, a nivel 5 o L5. Se considera que la actividad organizativa de los controles debe alcanzar como mínimo el nivel 3 de madurez o L3, que se corresponde con una... con un índice de... una puntuación del 80 %. En el caso del Ayuntamiento de Béjar, el nivel de madurez global ha pasado del 5 % en dos mil veintiuno, que suponía nivel 0 o L0, al 20 % en dos mil veinticuatro, que se corresponde con nivel 1 o L1; es decir, ha comenzado a tomar medidas para revertir la situación, mejorando su calificación y su puntuación global.



Este ayuntamiento carece de una estrategia de tecnologías de la información y tampoco ha establecido una gobernanza adecuada que le permita afrontar con garantías el proceso de dotar a sus sistemas de información de un nivel de seguridad suficiente. Las actuaciones realizadas para cumplir con las recomendaciones efectuadas por el Consejo de Cuentas en la auditoría de dos mil veintiuno se han concretado en los siguientes aspectos... Quiero advertirles que me estoy refiriendo a Ciudad Rodrigo, que no lo he dicho; por tanto, lo repito.

El Ayuntamiento de Ciudad Rodrigo carece de una estrategia de tecnologías de la información y no ha establecido la gobernanza, a diferencia del... adecuada. Y las actuaciones realizadas para cumplir con las recomendaciones se han concretado en los siguientes aspectos en relación a Ciudad Rodrigo. En primer lugar, la adquisición de equipamiento para la instalación centralizada de aplicaciones que proporciona la Diputación de Salamanca a través del Organismo Autónomo Centro Informático Provincial de Salamanca. En segundo término, mejora del proceso de copias de seguridad y contratación de un servicio de respaldo en la nube para copias de seguridad. Y, finalmente, el nombramiento del delegado de protección de datos.

Por otra parte, se mantiene la situación por la que el Ayuntamiento de Ciudad Rodrigo cuenta con apoyo específico en materia de Administración electrónica, nóminas, padrón y gestión presupuestaria a través del Centro Informático Provincial de Salamanca.

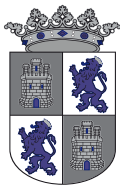
Aun así, las actuaciones realizadas, a juicio del informe, no son suficientes como consecuencia de la falta de aprobación de una política de seguridad como paso fundamental para iniciar el proceso de adaptación al Esquema Nacional de Seguridad.

En los tres años transcurridos no se han tomado todas las medidas necesarias para revertir la situación del ayuntamiento, mejorando apenas su calificación global. Sigue siendo necesario, por lo tanto, un impulso importante para conseguir un nivel de seguridad adecuado y garantizar el cumplimiento de la normativa de aplicación.

En cuanto al análisis y evaluación de los controles básicos de... de ciberseguridad en el Ayuntamiento de Ciudad Rodrigo, la puntuación global ha pasado del 3 % en dos mil veintiuno al 8 % en dos mil veinticuatro, en ambos casos, dentro del nivel 0 o L0.

Finalmente, me referiré -para completar las conclusiones- al Ayuntamiento de Benavente. El ayuntamiento, con la aprobación de la política de seguridad de la información, ha dado un paso relevante para afrontar el proceso de dotar a sus sistemas de un nivel de seguridad suficiente. No obstante, sigue careciendo de una estrategia como herramienta para planificar las necesidades de tecnologías de la información municipales a largo plazo, garantizando así que se alcanza y se mantiene el nivel de seguridad adecuado.

Las actuaciones para cumplir con las recomendaciones realizadas por el Consejo en la primera fiscalización se han concretado en los siguientes aspectos. En primer lugar, la... la aprobación de una política de seguridad de la información. En segundo término, la estabilización de una de las dos personas dedicadas a la tecnología de la información municipal. Sin embargo, sigue habiendo un contexto de provisionalidad que no se ha abordado en su totalidad. En tercer lugar, la contratación



de servicios y compra de equipamiento tecnológico, aunque la renovación no ha sido completa y quedan todavía elementos relevantes sin actualizar. Y, finalmente, la adecuación a la normativa de protección de datos.

Por otra parte, no se han realizado cambios relevantes en el entorno tecnológico y se mantiene la situación por la que el Ayuntamiento de Benavente opta por un modelo donde las aplicaciones se instalan fundamentalmente en su propia infraestructura, sin utilizar tampoco el apoyo específico en materia de Administración electrónica y soporte informático que ofrece la Diputación de Zamora.

Las actuaciones realizadas, aunque han supuesto la consecución de hitos importantes, aún son puntuales e insuficientes, ya que no permiten la continuidad de los esfuerzos realizados al no existir una planificación estratégica de la tecnología de la información municipal que garantice una dotación de recursos ajustada a las necesidades actuales y futuras.

El Ayuntamiento de Benavente, como se puso de manifiesto en la anterior auditoría, se encontraba en una situación muy... muy vulnerable frente a riesgos informáticos. No obstante, en el período de tres años transcurridos ha comenzado a tomar algunas medidas para revertir la situación, mejorando ostensiblemente su calificación global. Pero estas medidas, siendo algunas -como ya he mencionado- de gran relevancia, son, a juicio del Consejo de Cuentas, todavía insuficiente... insuficientes, siendo preciso un impulso importante para conseguir un nivel de seguridad adecuado y garantizar el cumplimiento de la normativa de aplicación.

En cuanto al análisis y evaluación de los controles básicos de ciberseguridad en el Ayuntamiento de Benavente, la puntuación global se ha duplicado, pasando del 16 % en dos mil veintiuno al 32 % en dos mil veinticuatro, en ambos casos, dentro del nivel 1 o L1.

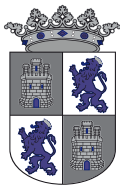
A la vista de esta segunda revisión efectuada en los tres ayuntamientos, el Consejo de Cuentas realiza nuevas recomendaciones (cinco para Béjar, para Ciudad Rodrigo cuatro y siete para Benavente), orientadas todas ellas a las actuaciones necesarias para que estos ayuntamientos alcancen un nivel de seguridad... de ciberseguridad -perdón- adecuado.

Hay dos recomendaciones comunes para las tres entidades: en primer lugar, el alcalde debería impulsar, de manera decidida y continuada, las actuaciones para acometer inmediatamente la adecuación del ayuntamiento al Esquema Nacional de Seguridad y a la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, para que el ayuntamiento alcance un nivel de ciberseguridad adecuado -en este caso, los ayuntamientos-.

Asimismo, debería asegurarse... deberían asegurarse la dotación de recursos materiales y humanos imprescindibles para conseguir un nivel de seguridad apropiado.

En concreto, en Ciudad Rodrigo se debería asegurar que la relación de puestos de trabajo y el organigrama del ayuntamiento, al menos, contemple las funciones de tecnologías de la información, de acuerdo con la importancia que estas tienen para el ayuntamiento.

En el caso de Benavente, la Diputación de Zamora dispone de un servicio de asistencia a municipios, y específicamente en materia de Administración electrónica, al que el ayuntamiento podría recurrir.



Los Ayuntamientos de Béjar y Ciudad Rodrigo comparten una tercera recomendación: el alcalde debería, por una parte, asignar los roles y responsabilidades implantando una gobernanza de ciberseguridad que garantice que el proceso de adaptación se llevará a cabo en un plazo determinado y tendrá la continuidad imprescindible para garantizar que se alcanza el objetivo y que se mantiene a largo plazo; y, por otra parte, aprobar la normativa en materia de seguridad de la información y protección de datos personales necesaria.

De forma específica, como cuarta y quinta recomendaciones para el Ayuntamiento de Béjar, el alcalde debería asegurar que las actuaciones a emprender o puestas en marcha por el propio ayuntamiento o con apoyo específico de la Diputación de Salamanca se apliquen a todos los sistemas de información que dan soporte a los procesos relevantes de gestión, sin que existan áreas que no estén bajo el control de los responsables de la tecnología de la información municipal.

Y, finalmente, debería asegurar que se tomen medidas para garantizar la capacidad de restablecer la prestación de los servicios fundamentales del ayuntamiento en un tiempo determinado, especialmente mediante la mejora en el proceso de copias de seguridad, y, en concreto, asegurando que todos los sistemas de información relevantes dispongan de copias y estén adecuadamente protegidos.

Con carácter singular para el Ayuntamiento de Ciudad Rodrigo, como cuarta y última recomendación, el alcalde, dada la relevancia que las aplicaciones proporcionadas por el Centro Informático Provincial de Salamanca y las contrataciones externas tienen para la gestión municipal, debería asegurar que los convenios y contratos en los que se basa su utilización contienen las previsiones que exige el Esquema Nacional de Seguridad para estos casos.

Finalizo ya contemplando las recomendaciones dirigidas específicamente al Ayuntamiento de Benavente.

En primer lugar, de acuerdo con el modelo de gobernanza aprobado por su política de seguridad, los responsables de la información y de los servicios correspondientes deberían establecer y aprobar los requisitos de seguridad, encargándose a su vez de su aplicación y verificación. Por su parte, el Comité de Seguridad debería ejercer sus funciones que les son propias, entre otras, de coordinación, planificación y seguimiento, para asegurar de esta forma que se realizan las tareas definitivas en la política de seguridad.

En cuanto al proceso continuo de identificación y corrección de... de vulnerabilidades, el responsable de seguridad debería valorar, junto con el responsable de sistemas, el empleo de herramientas automatizadas para la detección de vulnerabilidades y la realización periódica de actuaciones como las que se han llevado a cabo desde la anterior auditoría.

Y para concluir, en lo referente al uso controlado de los privilegios administrativos, el concejal competente, en su caso, debería impulsar la inclusión en todos los contratos de servicios informáticos de cláusulas que permitan realizar un control de cómo se llevan a cabo los servicios y el uso y control de los privilegios de la Administración, de acuerdo con lo especificado en el Esquema Nacional de Seguridad.

Además, es urgente que el responsable de seguridad defina un procedimiento para la realización de tareas como la gestión de usuarios administradores, haciendo



uso de la política de mínimo privilegio, el cambio de contraseñas por defecto y la definición de políticas robustas y homogéneas para los sistemas de autenticación.

Finalmente, el Pleno del ayuntamiento debería aprobar una normativa que garantice que el registro de actividad de los usuarios se realiza de acuerdo con lo establecido en el Artículo 24 del Esquema Nacional de Seguridad, en concreto, con plenas garantías del derecho al honor, a la intimidación 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 puede utilizarse como referencia la guía del Centro Criptológico Nacional sobre registro de la actividad de los usuarios. Eso es todo por mi parte. Muchas gracias por su atención.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Muchas gracias. Abrimos un turno de intervenciones. Empezamos por el Grupo Parlamentario UPL-Soria ¡Ya! Para su intervención tiene... por un tiempo... aunque en el Reglamento pone diez minutos, vamos a dar quince por la unificación de los tres, si es necesario. No hace falta que lo gaste en totalidad si no quiere, pero tiene quince minutos a su disposición la procuradora doña Alicia Gallego González.

LA SEÑORA GALLEGO GONZÁLEZ:

Gracias, presidente. Yo creo que por las razones técnicas no lo agotaré. Pero, bueno, dar la bienvenida y agradecer las explicaciones al presidente del Consejo de Cuentas, a su equipo. Porque, evidentemente, es una... bueno, esta materia siempre es bastante, bueno, pues poco... poco buena para... para manejar, para tratar y, sobre todo, dadas las circunstancias en las que se encuentran los ayuntamientos. Las entidades locales pues tienen unas limitaciones o unas... una situación de... de pocos recursos económicos, financieros, de tal manera que muchas veces esas limitaciones son las que impiden pues el ponerse al día -entiendo yo- en toda esta materia tan importante como es la ciberseguridad.

Claro, se habla de ayuntamientos de un tamaño medio como puede ser Béjar, Ciudad Rodrigo, en Salamanca, o Benavente, en Zamora, en la que, bueno, sus presupuestos ya estamos hablando de cierta entidad, pero seguramente tan agobiados y asfixiados para poder solventar sus necesidades que muchas veces les imposibilitará el dar solución, o yo entiendo que serán más razones de... de tipo presupuestario los que les impiden adaptar su plantilla a las necesidades existentes; una plantilla que pues exige pues un personal cualificado, como se ha puesto aquí de relieve -pues desde informáticos hasta responsables de protección de datos-, y con la importancia, la cualificación y la responsabilidad que asume y que en sus recomendaciones pues vienen a... a indicar la... la necesidad de... de que tengan pues todo lo que es ese Esquema, esa normativa aprobada por los propios órganos, y luego la responsabilidad que asume en la gestión del mismo.

Es evidente lo que se pone de manifiesto en... en la documentación adjunta de que los recursos que deberían de ser utilizados para tener pues normalizada esta situación están por debajo de lo necesario, si bien se... se apunta de que es un 1,34 % de los recursos ordinarios. Con lo cual, difícil, difícil el... el solventar estas necesidades, estas recomendaciones que se le da.



También se ha puesto de manifiesto pues esas plantillas –como digo– que no acaban de actualizarse con las necesidades, donde no se convocan las plazas de... de informáticos, donde, además, se da una cierta temporalidad. Con lo cual, en una materia tan importante como esta, pues parece evidente que esas soluciones sí que tienen que adaptarse, tienen que... que tomarse para dar... dar finalización a... a lo que es ese Esquema y, por lo tanto, la necesidad que los ciudadanos y los propios datos que tiene el ayuntamiento pues no generen un problema pues, como muchas veces se ve, cuando, bueno, pues hay esa... esa fuga, esa roba de... de datos; y con ello los problemas que se genera pues tanto para el propio ciudadano, como se ha puesto aquí de relieve en uno de los ayuntamientos, por el honor, la intimidad y también por la sensibilidad de que son cuentas bancarias u otro tipo de... de datos que pudieran afectar de una forma todavía más... más importante.

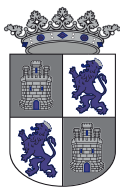
Es verdad que hay una... –o se ha puesto de relieve aquí– una cierta posibilidad de convenios con diputaciones, pero sí que es verdad que debería de abordarse quizá más el tema de cómo los ayuntamientos pueden acceder pues por distintas vías a nuevos equipos, a ese tipo de... de actualizaciones en *software*, en *hardware* y que, además, pues tengan la posibilidad de no estar tan limitados a lo que hoy nos afecta tanto, que son las reglas fiscales, y que muchas veces imposibilitan el dar cumplimiento a cosas tan importantes como pudiera ser esta.

Sin entrar en más detalle de... de los datos que se nos han expuesto aquí y que en la Memoria aparecen de forma clara, tanto las recomendaciones como los seguimientos y... y, en su caso, bueno, pues evidencia muchos de los incumplimientos. Después de tres años sí que es verdad que quizá habría que adoptar algún tipo de medidas o... o algún tipo de... o esa es la opinión que a mi modo se desprende de... de todo este análisis de sus datos, en que a lo mejor habría que incidir en algún tipo de política autonómica que ayudara de una manera más intensa a los ayuntamientos a solventar todas estas deficiencias tecnológicas; que muchas veces, ahogados por la falta de recursos o bien, en su caso, por una incapacidad de no poder solventar una materia tan técnica, necesitarían no solamente del apoyo de las diputaciones a través de los convenios, sino también de forma más directa e intensa por parte de... de esta Administración, como al final pues solventaría el problema ciudadano.

Creo que los ayuntamientos muestran voluntad, pero sí que es verdad que, aparte de eso, hay que marcar plazos, hay que marcar retos como son las normativas. El cumplimiento de esa política es importante, las responsabilidades que se asumen por parte –muchas veces– de los propios políticos de estas Administraciones y que necesitan –reitero– una ayuda económica para solventar esas deficiencias.

Me gustaría, eso, saber si... si, bueno, si esto son, bueno, pues meros ejemplos simplemente por falta de... de una apuesta que hacen pues más o menos porque no tienen unas consecuencias luego legales o incumplimiento, o bien, en su caso, se achaca más a una falta de... de recursos lo que generaría esta falta de cumplimiento después de tres años. Y insistir nuevamente, como parece que... que se deduce de los estudios, en que las recomendaciones siguen estando ahí vigentes sin que se hubiera cumplido.

Finalizo en esta primera intervención. Y simplemente sería esa la duda que se me ha generado después de... del estudio de estos informes. Gracias.

**EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):**

Muchas gracias. Tiene la palabra, en representación del Grupo Parlamentario Vox Castilla y León, la procuradora doña Susana Suárez Villagrà, por un tiempo máximo de quince minutos.

LA SEÑORA SUÁREZ VILLAGRÀ:

Muchas gracias, presidente. Gracias, señor Amilivia, por estos informes sobre el seguimiento de recomendaciones y actualización de la situación de seguridad informática en estos tres ayuntamientos respecto al año dos mil veintiuno.

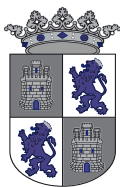
En la era de la digitalización, la Administración pública se enfrenta a desafíos cada vez más grandes en el ámbito de la ciberseguridad. Las Administraciones públicas –en este caso, los ayuntamientos– manejan una gran cantidad de datos personales de los ciudadanos, datos sensibles como son la formación... la información personal, registros financieros, etcétera. Por ello, se hace fundamental proteger esos datos sensibles para mantener la confianza de los ciudadanos en la Administración pública.

Esa información que almacenan los ayuntamientos resulta ser un objetivo atractivo para los ciberdelincuentes y los ciberataques. El robo de datos en las Administraciones y las infiltraciones en sistemas críticos o ciberataques pueden tener consecuencias muy graves. La exposición de datos sensibles como información personal no solo puede llevar a fraudes y robos de identidad que afectan a los ciudadanos. A nivel operativo, un ciberataque puede interrumpir gravemente los servicios públicos esenciales como oficinas virtuales, recaudación de impuestos y servicios de emergencia, paralizando funciones críticas.

En dos mil veintiuno ya vimos como varios portales del Estado sufrieron ataques que afectaron a servicios clave como los del SEPE, paralizando su funcionamiento durante días. Además de los ciberataques, hay que tener en cuenta que puede caerse el sistema por fallos en la red, en los servidores, en los discos duros de estos, simplemente con un corte de luz como hemos vivido hace unas semanas. Los que conocemos bien el ámbito informático porque nos hemos dedicado a ello laboralmente sabemos que con un simple corte de luz se puede estropear un disco duro o una fuente de alimentación, y para eso hay que tener equipos de respaldo, lo que quiere decir que hay que estar preparados y hay que invertir en otros equipos. Hay que tener mecanismos que nos garanticen estos servicios si hay una caída del sistema por el motivo que sea, porque se pueden perder datos.

Cuando alguno de estos casos se da –intrusismo en los equipos, robo de datos, pérdida de estos– y la Administración no responde porque no ha sido responsable, el daño reputacional para ese ayuntamiento puede ser tremendo. La imagen de vulnerabilidad es muy mala porque genera desconfianza e ineficacia hacia la gestión municipal.

Si hablamos en términos económicos, también resulta relevante, ya que la recuperación y la restauración de sistemas y datos suele ser costosa, además de la pérdida de ingresos por inactividad y posibles sanciones por incumplimiento normativo, como las posibles multas por parte de la Agencia Española de Protección de Datos si se vulnera el Registro General de Protección de Datos.



Para reducir los riesgos de un ciberataque es importante tomar algunas medidas como son capacitar a los empleados de manera continua en las mejoras en las prácticas de... de ciberseguridad y en cómo identificar amenazas; utilizar sistemas avanzados para monitorear y detectar problemas que permitan identificar y responder rápidamente a posibles incidentes; desarrollar y mantener políticas de seguridad claras y actualizadas asegura que la organización esté preparada para enfrentar las amenazas cibernéticas en constante evolución. Y las Administraciones públicas deben seguir actualizándose y adaptándose a nuevas amenazas, porque cada vez, además, son... son mayores. Muchos de los ayuntamientos optan por la opción de subcontratar el servicio con empresas externas. Pero también estas empresas deben cuidar su seguridad, porque puede ocurrir lo sucedido en el mes de marzo de este año en Benavente y en otros ayuntamientos, que fueron atacados a través de la empresa que le da soporte a la página web del ayuntamiento.

Respecto al análisis de los cumplimientos por parte de los ayuntamientos citados, de Béjar y Ciudad Rodrigo, ambos de... de similar población, cuentan con el escaso... con escaso personal y destinan un porcentaje muy pequeño a las tecnológicas informáticas, tal como pone de manifiesto el informe según los datos aportados... según los datos aportados.

Son ayuntamientos que han tenido que adaptarse a los nuevos retos digitales, como todas las Administraciones públicas, a una velocidad muy rápida en una cuestión tan relevante como es la seguridad informática. Y esto, en muchos casos, no se está haciendo con el debido rigor -como usted muy bien ha dicho-, como ocurre con los ayuntamientos en los que estamos haciendo seguimiento en el día de hoy, incluido también el de Benavente. Los tres ayuntamientos no llegan ni siquiera al aprobado; algo tan básico como es hacer una copia de seguridad, como tener un plan de seguridad o nombrar a alguien como responsable informático no se hace.

Desde Vox creemos que es fundamental proteger la intimidad personal y familiar de los ciudadanos, fortalecer la ciberseguridad de las empresas y de las Administraciones públicas españolas frente al espionaje industrial o ataques por parte de potencias hostiles.

Algo tan importante como la normativa sobre el deber de la información y la protección de datos, según recoge el referente legal para la Administración local en... en materia de seguridad... ciberseguridad, que es el Esquema Nacional de Seguridad (ENS), tampoco se cumple por algunos ayuntamientos, y esto da aspecto de dejadez y desidia.

Señorías, es importante invertir en seguridad informática y hay que insistir en ello, es una inversión en seguridad para los ayuntamientos y para los ciudadanos. Creemos que aún falta mucho por hacer en este campo para modernizar digitalmente España, aunque en un país donde se va la luz un día y nadie da explicaciones poco podemos esperar. Lo más probable es que vayamos para atrás, en vez de ir hacia adelante. Muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Muchas gracias. Tiene la palabra, en representación del Grupo Parlamentario Socialista, la procuradora doña Rosa María Rubio Martín, por un tiempo máximo de quince minutos.



LA SEÑORA RUBIO MARTÍN:

Muchas gracias, señor presidente. Buenas tardes a todas y a todos, señorías. En primer lugar, dar la bienvenida a esta Comisión al presidente del Consejo de Cuentas, el señor Amilivia; a los consejeros que le acompañan; y a todo el equipo técnico. Gracias por la exposición que ha hecho, señor presidente, sobre los informes que debatimos esta tarde. Hoy traemos a esta Comisión tres informes de tres ayuntamientos –Béjar, Ciudad Rodrigo y Benavente–, sobre el seguimiento de las recomendaciones y actualización de la situación de la seguridad informática.

Antes de entrar en el fondo del asunto, sí conviene saber a qué nos estamos refiriendo cuando hablamos de ciberseguridad. La ciberseguridad se ha convertido en algo más que una palabra de moda, se trata de una necesidad, ya que con la creciente dependencia de la tecnológica, tanto las empresas como los particulares resultan más vulnerables que nunca a las amenazas informáticas. La ciberseguridad se refiere a la práctica de proteger los sistemas, las redes y los datos de las amenazas digitales, creando un entorno seguro al tiempo que garantiza la integridad, confidencialidad y disponibilidad de la información.

Los ciberataques pueden provocar accesos no autorizados, violaciones de datos, incluso pérdidas económicas. Este ámbito es tan amplio y abarca desde la protección de la información personal en dispositivos individuales hasta la aplicación de protocolos de seguridad sólidos para, por ejemplo, como es el caso de hoy, los ayuntamientos.

Los consistorios manejan una cantidad importante de información personal y privada de los ciudadanos particulares; por eso es tan necesario que exista un plan de seguridad informática y un delegado de protección de datos; por eso es tan necesario que los ayuntamientos se pongan al día en este tema y que cumplan la normativa existente para ello con guías, protocolos, personal y medios.

La importancia de la ciberseguridad es innegable en un mundo en el que se requiere proteger los datos, ya que constituyen la nueva moneda, porque sin las medidas adecuadas es posible acceder fácilmente a la información sensible, robarla o manipularla, lo que puede tener consecuencias sustanciales.

Hace unos días conocíamos la noticia de un posible ataque a la web del sistema educativo de Castilla y León, Educacyl. Según se publicaba en medios de comunicación, el presunto ladrón informático o jáquer afirmaba estar vendiendo acceso a datos sensibles del sistema educativo de la Comunidad. Estamos hablando de acceder ilegalmente a una base de datos que contiene más de 1.000.000 de registros personales de estudiantes y sus padres, incluidos nombres completos, números de identificación, números de teléfono, direcciones de correo electrónico, direcciones físicas, edades y fechas de nacimiento.

Esta noticia apuntala aún más la necesidad de contar con un sistema informático seguro y protegido de cualquier posible ataque o filtración. Esta misma mañana, la consejera de Educación ha asegurado que no ha existido ataque y que ningún jáquer ha accedido a la base de datos de la Consejería; cuestión que nos alegra enormemente, aunque haya generado preocupación –como es lógico– entre los castellanos y leoneses.



Y, entrando en el fondo del asunto de hoy, los tres informes que traemos esta tarde tienen muchos puntos en común, tanto de análisis como de conclusiones y recomendaciones; pero voy a juntar los dos informes de Béjar y Ciudad Rodrigo, por un lado, y separadamente el Ayuntamiento de Benavente, por otro.

Como se ha expuesto por el presidente de Cuentas, en el año dos mil veintiuno, se pusieron en contacto con los ayuntamientos para realizar la auditoría, recabar datos y poder elaborar el informe, del que se extrajeron conclusiones y recomendaciones que se comunicaron a los ayuntamientos con la intención de mejorar aquello que ya tuviera puesto en marcha y de instalar lo que ni siquiera existía, relativo a la seguridad... seguridad informática de estos ayuntamientos. Tanto en Béjar como en Ciudad Rodrigo la carencias eran bastante importantes.

En el año dos mil veinticuatro, se ha realizado el seguimiento de las recomendaciones efectuadas y se plasmó en el informe que debatimos hoy la realidad actual de la seguridad informática de estos consistorios. En el año dos mil veintiuno, las recomendaciones se dirigían a los concejales delegados; en este informe del año dos mil... dos mil veinticuatro se personaliza en la figura del alcalde la obligación de aprobar la normativa, de cumplir con la legislación al respecto y de implantar las medidas necesarias para que los sistemas informáticos de los consistorios tengan el nivel de seguridad adecuado y correcto para proteger y protegerse.

Resusta... resulta -perdón-, resulta especialmente llamativo que tanto el Ayuntamiento de Béjar como el Ayuntamiento de Ciudad Rodrigo, a pesar de seguir teniendo bastantes carencias -Béjar ni siquiera ha nombrado un delegado de protección de datos-, a pesar de esto, de las carencias tan importantes que tenían en seguridad informática, ninguno de los dos ayuntamientos ha presentado alegaciones para, por lo menos, intentar justificar o aclarar el por qué no había aplicado las recomendaciones que se les hicieron llegar procedentes de la auditoría del año dos mil veintiuno.

Me consta que, precisamente Béjar, tenía unas carencias enormes en seguridad informática, y no se había hecho absolutamente nada en el tema hasta el año dos mil veintiuno que se realizó la auditoría. Se dieron los pasos para cumplir con las alertas que contenía el informe, como, por ejemplo, crear una plaza de técnico informático del Grupo C1, que estuvo cubierta de manera interina hasta el año dos mil veintitrés en el que hubo un cambio de Gobierno. Se establecieron las bases para cambios de contraseña y se instaló una estructura perimetral de seguridad infrainformática. Desde el año dos mil veintitrés, con la celebración de elecciones municipales, no se ha avanzado absolutamente nada en seguridad informática por parte del ayuntamiento y del alcalde.

De las cuatro recomendaciones solamente ha aplicado una, y de manera parcial. Y no se ha implando un marco de gobernanza que garantice la continuidad y consistencia que requiere una estrategia de seguridad sólida. Para el Ayuntamiento de Béjar emanan ahora cinco recomendaciones, una más que en el año veintiuno, y que compartimos plenamente.

Muy paralelo es el análisis que hacemos del Ayuntamiento de Ciudad Rodrigo, aunque sí es cierto que este consistorio ha nombrado ya al delegado de protección de datos. Pero también de las cuatro recomendaciones, solo ha aplicado una y de manera parcial.



Como decía, llama poderosamente la atención que ni siquiera se hayan molestado en presentar alegaciones al informe para intentar justificar la falta de aplicación de medidas. Entendemos que se autoconvencerán con excusas presupuestarias, pero no es de recibo no dar la importancia que tiene el tema de seguridad informática, poniendo en riesgo los datos que poseen como ayuntamiento.

Al alcalde de Ciudad Rodrigo se le recomienda que dote de recursos materiales y humanos imprescindibles para alcanzar un nivel de seguridad acorde al uso intensivo y la relevancia que suponen los sistemas de información como soporte de los procesos fundamentales en la gestión municipal.

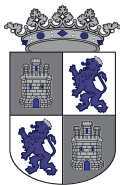
Este ayuntamiento no ha tenido cambio de Gobierno en el período desde que comenzó la auditoría, así que el responsable es el mismo desde el año dos mil veintiuno de los incumplimientos y falta de adaptación normativa en materia de seguridad informática. No dice nada bueno de un regidor que no le dé la importancia necesaria que tiene el tema que abordamos hoy. Se dictan cuatro recomendaciones que, desde el Grupo Parlamentario Socialista, compartimos y las hacemos nuestras.

Respecto al Ayuntamiento de Benavente, municipio con entidad, que –como dice el informe con los datos económicos y de población– estamos hablando de 17.246 habitantes, según los datos del INE a uno de enero del dos mil veinticuatro, con 214 empleados, puede disponer de una estructura de tecnologías de la información y de las comunicaciones de cierta complejidad. Me consta que el ayuntamiento hasta el año dos mil veintitrés, que hubo cambio de Gobierno, se esforzó y dio los pasos para cumplir con las recomendaciones que efectuó el Consejo de Cuentas. Dado que el técnico informático es el mismo desde el año dos mil veintiuno, la responsabilidad, lógicamente, es exclusivamente política.

El ayuntamiento presenta en el trámite de audiencia alegaciones, pero –como bien dice el informe– no se trata realmente de alegaciones, sino de una exposición acerca de las actuaciones que se han realizado y las que están planificadas para la elaboración y aprobación de los procedimientos. En el documento del ayuntamiento se valora positivamente el informe del Consejo de Cuentas, pero no influye en ninguna de las recomendaciones que ha elaborado el Consejo de Cuentas. En este punto, el Ayuntamiento de Benavente ya no puede excusarse en comunicar que tiene planificadas actuaciones si realmente ha tenido tres años para aplicar medidas y no lo ha hecho.

Respecto al seguimiento de las diez recomendaciones, ha cumplido totalmente una, pero no han establecido ni el cambio de contraseñas siquiera; ni un sistema de cumplimiento para aplicar a los proveedores de servicios informáticos externos; no hay un sistema continuo de detección de vulnerabilidades; no se ha realizado una planificación adecuada del inventario y los activos, teniendo algunos obsoletos. Esta es la situación real que plasma el informe año dos mil veinticuatro. Del informe de hoy emanan siete recomendaciones que el Grupo Parlamentario Socialista también las hace suyas.

Entendemos también que pareciera que los tres ayuntamientos auditados no han prestado la importancia necesaria al tema que tratamos, que es la seguridad informática. Es necesario tener seguridad en la red, seguridad en la información, centrada en proteger los datos sensibles de acceso no autorizado, la divulgación, la alteración y la destrucción. La seguridad de la información es crucial para mantener la confidencialidad, integridad y disponibilidad de dichos datos.



Hoy, desde el Grupo Parlamentario Socialista, les queremos mandar un mensaje a los alcaldes en general, y a los regidores de Béjar, Ciudad Rodrigo y Benavente en especial: que, en el mundo de la ciberseguridad, prevenir siempre es mejor que curar. Nada más por ahora, y muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Muchas gracias. Tiene la palabra, en representación del Grupo Parlamentario Popular, el procurador don David Beltrán Martín, por un tiempo máximo de quince minutos.

EL SEÑOR BELTRÁN MARTÍN:

Muchas gracias, presidente. Pues, desde el Grupo Parlamentario Popular, agradecemos la comparecencia del presidente del Consejo de Cuentas, así como el trabajo técnico y riguroso que hoy se nos presenta.

Los informes de seguimiento sobre la situación de la seguridad informática en los Ayuntamientos de Béjar, Ciudad Rodrigo y Benavente son un valioso instrumento para comprobar no solo la implantación de recomendaciones anteriores, sino también la evolución de estas entidades ante un desafío que afecta directamente a la calidad, continuidad, legalidad de la gestión pública y la protección de nuestros datos.

Como ha manifestado el señor Amilivia, la conclusión general de los tres informes es clara: existen deficiencias relevantes en materia de ciberseguridad, a pesar de algunos avances puntuales. Especialmente llamativo es el caso de Béjar, que pasa de un cumplimiento del 5 al 20 % en tres años; y el de Ciudad Rodrigo, que apenas mejora del 5 al 8 %. En cambio, en Benavente se observa una evolución más significativa: del 16 al 32 %, pero aún muy por debajo del umbral mínimo del 80 % -nivel L3- que marca el modelo de madurez exigible.

Entre las principales carencias señaladas por el Consejo de Cuentas destaca la ausencia de una política integral de seguridad de la información; la falta de planificación estratégica en tecnología a medio y largo plazo; la insuficiente dotación de personal técnico estable y cualificado; la no utilización de servicios de apoyo ofrecidos por diputaciones -en el caso de Benavente-; y la escasa implantación de controles básicos como inventarios de dispositivos, gestión de vulnerabilidades o protocolos de configuración segura.

En el plano normativo también se constata que no se han completado los procesos de adecuación al Esquema Nacional de Seguridad ni se han implementado todas las recomendaciones del Consejo en materia de protección de datos. Estos hechos evidencian que seguimos ante una situación muy vulnerable, que compromete no solo la seguridad de los sistemas, sino también la fiabilidad de los datos económicos, administrativos y financieros imprescindibles para el control público y la toma de decisiones.

Pero desde el Grupo Parlamentario Popular no nos quedamos en la crítica. Reivindicamos también el papel que está jugando el Gobierno autonómico para apoyar y acompañar a los ayuntamientos en su proceso de modernización digital. La Junta de Castilla y León ha sido pionera en impulsar programas: programas como Territorio Rural Inteligente, con soluciones tecnológicas en más de 200 municipios;



el despliegue de la herramienta Administracyl, que facilita a los ayuntamientos cumplir con el Esquema Nacional de Seguridad y avanzar en interoperabilidad; la red de soporte TIC local, en coordinación con diputaciones, para prestar asistencia a municipios sin medios propios; y la formación continua a empleados públicos en competencias digitales y protección de datos, en colaboración con el Instituto Nacional de Administración Pública. Todo ello ha sido posible sin ruido, sin titulares grandilocuentes, pero con resultados concretos. Porque en el Partido Popular entendemos la transformación digital no como un eslogan, sino como una tarea seria y sostenida en el tiempo.

Señorías, garantizar la seguridad de la información no es una opción, es una obligación ética, jurídica y técnica. Y desde el Grupo Popular vamos a seguir defendiendo que todos los municipios de Castilla y León, con independencia de su tamaño, tengan los medios necesarios para estar protegidos. Por ello, celebramos que Castilla y León haya sido pionera, a través del Consejo de Cuentas, en fiscalizar estos aspectos y que la Junta haya puesto en marcha programas útiles y realistas para apoyar a los municipios en su proceso de adaptación. Sin más, muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

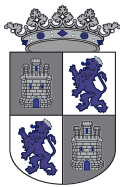
Para contestar a todas estas intervenciones, tiene de nuevo la palabra el presidente del Consejo de Cuentas, don Mario Amilivia.

EL PRESIDENTE DEL CONSEJO DE CUENTAS DE CASTILLA Y LEÓN (SEÑOR AMILIVIA GONZÁLEZ):

Muchas gracias, presidente. Más que entrar en una contestación precisa a cada una de sus intervenciones, me gustaría hacer una... una intervención más de carácter general.

En primer lugar, recordar que... que este es un informe de seguimiento de recomendaciones; es decir, ya ha habido un primer informe donde hubo una serie de recomendaciones que debían haber cumplido los ayuntamientos en su caso. Posteriormente, se llevó a cabo el informe de seguimiento de recomendaciones específico sobre esas recomendaciones establecidas en los primeros informes. Y este ya es un informe podemos decir recurrente, es decir, es un informe sobre el seguimiento de las recomendaciones tras el informe de seguimiento de las recomendaciones; es decir, es un informe que... que realmente destaca por su carácter operativo de rendimiento de gestión.

Debemos recordar que las recomendaciones –como siempre les señalo a sus señorías– no son vinculantes. Por lo tanto, su cumplimiento para el Consejo de Cuentas es un reforzamiento de nuestra *auctoritas*, del sentido que tiene la propia Institución. Y el cumplimiento de las mismas por parte de los entes fiscalizados pues manifiesta la... la voluntad de mejorar la gestión y, en este caso, que han comprendido o que han aceptado y que están impulsando el cumplimiento de nuestros informes, con recomendaciones que han de estar fundamentadas en las propias conclusiones y que deben añadir valor; es decir, deben abordar las debilidades, las deficiencias de una determinada gestión, evitando obviedades y permitiendo al ente fiscalizado libertad de gestión; y, además, deben ser relevantes o significativas, convincentes y comprensivas, finalmente prácticas, claras y concisas.



Los tres ayuntamientos auditados podemos... podemos señalar que han tenido una mejora relativa; es decir, es cierto que el nivel mínimo de madurez exigible es el 80 %. Es... es también reseñable que ninguna capital de provincia en Castilla y León, de los informes que hemos llevado a cabo, alcanzó ese nivel del 80 %. Pero sí es cierto que se ha producido, aunque sea una leve mejoría, en los tres ayuntamientos: Béjar, del 5 al 20 %; Ciudad Rodrigo, del... del 5 al 20 %; Ciudad Rodrigo, del 3 al 8 %; y Benavente, del 16 al 32 %. Obviamente insuficiente, pero sí se permite atisbar una mejora relativa y un cierto efecto espejo de estos informes en relación con otros... otros ayuntamientos.

¿Qué considera el Consejo? Que no se termina de asimilar, por parte de los responsables de la gestión, que la seguridad, en este caso, es... debe ser esencial, y que forma parte de una organización que debe tener un plan estratégico integral; es decir, no es una ocurrencia. La ciberseguridad es una necesidad de la... de la política de organización de cualquier entidad, en este caso local, esencial y debe estar, por lo tanto, de esa manera contemplada en su organización y con un plan estratégico.

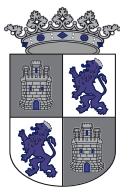
¿Qué pone también de manifiesto el informe? Que el proceso debe ser continuo y fundamental. Alguna de sus señorías han puesto de manifiesto como se puede interrumpir la... la política de seguridad o la política de ciberseguridad con ocasión de interrupciones de... de corporaciones. Pues bien, no. El informe manifiesta y pone de... de relieve que el proceso debe ser continuo y fundamental, y también pone de manifiesto la insuficiencia... -en los tres ayuntamientos, y me imagino que... que va a ocurrir lo mismo con los cuatro restantes- insuficiencia de dotación de medios materiales y humanos. Y también que las decisiones políticas no se trasladan a los presupuestos, es decir, que las distintas corporaciones municipales no consideran la ciberseguridad como una prioridad. Se considera mucho más prioritario acometer una determinada obra en el municipio del tipo que sea que acometer una... un esfuerzo presupuestario en materia de ciberseguridad, lo que, desde mi punto de vista, es un gravísimo error.

¿Ha habido avances irrelevantes? Quizá el más... el más relevante es cuando se aprueba una política de seguridad -como hemos dicho en relación a uno de los ayuntamientos auditados-, porque significa o manifiesta un compromiso ya de futuro.

Sí me gustaría, también, señalar que los controles básicos de seguridad, porque parece que estamos hablando de algo que ya agota en sí mismo la ciberseguridad, son necesarios pero no suficientes; es decir, cuando un ayuntamiento cumple con todos controles básicos de... de seguridad no significa que tenga garantizada la ciberseguridad, significa que tiene un nivel de madurez mínimo, que es ese 80 %.

Y, ahí, tenemos que ser conscientes que el nivel de inseguridad o el nivel de seguridad cada vez es más exigente y que está... y que está cambiando. Como me decía ayer un experto en esta materia, está cambiando el paradigma, es decir, lo que... lo que era el Esquema Nacional de Seguridad ha sido modificado en el año veintidós con mayores exigencias. Ahora viene una nueva Directiva europea, la NIS2, que va a establecer nuevas exigencias, pero también -esto es muy... muy importante- va a establecer responsabilidades; responsabilidades para las corporaciones municipales, que posiblemente ahí comience la solución.

Y, como no... no pueden obviar sus señorías, también tiene que ver mucho la... la ciberseguridad del futuro con la propia inteligencia artificial. Es decir, porque hoy los jáquer ya están utilizando la inteligencia artificial para atacar a los propios



entes fiscalizados, y estos se tienen que dotar de medios similares de defensa para poder... para poder compensar o... o neutralizar esos ataques. Es decir, falta personal cualificado, faltan medios presupuestarios suficientes y falta una voluntad también por parte de las corporaciones.

Coincido en la importancia de la cooperación entre Administraciones, en este caso especialmente la Comunidad Autónoma, la Junta de Castilla y León; y también reivindico -como lo hace el informe- los papeles de las diputaciones en su fundamental papel de asistencia técnica a los ayuntamientos.

Y resumiría todo diciendo que esto es un problema de compromiso y también de recursos para muchos ayuntamientos. Por mi parte, nada más. Y muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Abrimos un turno de réplicas. Tiene la palabra, en representación de Grupo Parlamentario UPL-Soria ¡Ya!, la procuradora doña Alicia Gallego González, por un tiempo máximo de diez minutos.

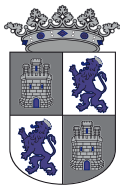
LA SEÑORA GALLEGO GONZÁLEZ:

Gracias, presidente, de nuevo. Bueno, pues no voy a agotar el tiempo evidentemente porque creo que las últimas conclusiones son las más esclarecedoras. Es decir, empiezo por el final, la falta de voluntad política creo que es la razón de que después de tres años pues ayuntamientos de este tipo pues no... no hayan tomado ninguna medida efectiva para solucionar los problemas que la ciberseguridad puede generar tanto para la propia entidad local como para los ciudadanos; y que es verdad que las Administraciones superiores, tanto la diputación como la Junta, sí que tendrían que hacer ese esfuerzo mayor.

Porque a veces es triste el... el que muchas veces siempre funcione el... el tema del palo y zanahoria como medida para cumplir la normativa. Es decir, sean las directivas que van a llegar o sea lo que obliga hoy el Esquema Nacional de... de Seguridad y la falta de cumplimiento de políticas claras que lleven a cabo por parte de estas Administraciones.

Creo muy importante que, dado los datos sensibles con los que trabajan estas entidades locales, esto es un ejemplo, las tres hoy mencionadas (Béjar, Ciudad Rodrigo y Benavente), pero que seguramente pues habría muchos más ejemplos en los que podríamos basarnos en... en la falta, yo creo, de... de conciencia, de que... de que estamos hablando de un tema muy importante por todos los datos que se manejan y que hay cuestiones sencillas, como las copias de seguridad, en las que sí que se podría plantear su cumplimiento.

Sí que es verdad también que, bueno, pues que la... el personal que tienen las Administraciones tiene que ser el adecuado. Muchas veces nos vamos a... a otro tipo de políticas, y aquí pues tanto los responsables informáticos como los responsables de datos personales hoy debería de ser uno más dentro de las plantillas municipales, puesto que todos los que son contratos de prestación de servicios exige ese cuidado en cuanto todo lo que se ofrece por parte del ciudadano a la Administración, se gestione de forma directa o indirecta, y por ello hay una responsabilidad por parte de quien gestiona los mismos.



Yo insisto en que quizá hay que incidir más en esa cooperación, en esa obligatoriedad, ayudada con los medios necesarios para que, bueno, pues evitemos problemas de futuro, tanto para los ciudadanos como para las propias Administraciones gestoras de los mismos. Agradeciendo las informaciones, pues finalizo mi exposición. Gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Tiene la palabra, en representación del Grupo Parlamentario Socialista, la procuradora doña Rosa María Rubio Martín.

LA SEÑORA RUBIO MARTÍN:

Nada, con brevedad. Yo creo que... -por algunas afirmaciones que se han hecho aquí esta tarde- yo creo que el... el apoyo de la Junta a los ayuntamientos se debería de plasmar en dinero y... y más presupuesto y en transferencias finalistas. Se alegaba aquí que, lejos del ruido, se veía que la efectividad en... en los ayuntamientos, respecto a la seguridad informática, gracias a la Junta de Castilla y León había mejorado. Y, bueno, pues ruido no lo sé si ha habido, pero efectividad, viendo los informes, se ve que... que poca. Se han analizado tres ayuntamientos; pero, si se analizaran más ayuntamientos, seguramente el... el resultado sea... sea el mismo.

Yo creo que es un tema -como ya hemos dicho aquí- de falta de voluntad política, además de... de un problema de recursos. Los recursos son vía dinero y vía transferencias finalistas que debe de hacer la Junta de Castilla y León; la voluntad política la pone cada regidor en su ayuntamiento. En este caso, además, coincide que los tres regidores son del mismo partido político, pero pudiera no coincidir. Estamos hablando de que son ayuntamientos con plantillas de más de 200 trabajadores y se está pidiendo un técnico informático. Pues miren, eso yo creo que lo... que lo dice... que lo dice todo.

Y un matiz: no se debe confundir el Legislativo con el Ejecutivo. La fiscalización de estos informes no tiene absolutamente nada que ver con las decisiones que se toman en la Junta de Castilla y León. Porque la... la fiscalización de estos informes emana de aquí, de esta Comisión de las Cortes de Castilla y León, que somos el Legislativo y no tiene nada ver con la Junta. Entonces, que veo que es un error de bulto que no... no se debe cometer por parte de... de ninguno de sus señorías.

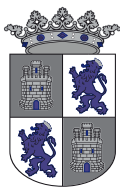
Y, nada, ya finalizando, agradecemos el trabajo del... del Consejo de Cuentas, y -como les dije en la primera intervención- compartimos las resoluciones y las hacemos nuestras. Nada más y muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

En el turno de réplica, por el Grupo Parlamentario Popular, tiene la palabra el procurador don David Beltrán Martín.

EL SEÑOR BELTRÁN MARTÍN:

Muchas gracias, presidente. Quiero finalizar agradeciendo de nuevo la labor del Consejo de Cuentas y la reflexión compartida en torno a estos tres informes. Hay un leve mejoría, pero falta de voluntad política para abordar una cuestión



de enorme trascendencia para el presente y futuro de nuestras Administraciones locales: la seguridad informática como garantía de calidad institucional y servicio público; compartiendo que la ciberseguridad debe ser una política esencial en cada entidad local, que requiere de un plan estratégico que nos lleve a un proceso continuo y fundamental.

Y más allá de los matices políticos, aunque siempre molesta a algún grupo político que se citen las políticas reales de la Junta de Castilla y León, creo que todos coincidimos en la necesidad de seguir avanzando juntos para que nuestros ayuntamientos cuenten con los medios, los conocimientos y el respaldo necesarios para afrontar los desafíos tecnológicos con solvencia.

Desde el Grupo Parlamentario Popular defendemos que la transformación digital de las entidades locales debe ser una tarea compartida, que combine la supervisión rigurosa con la cooperación institucional y el cumplimiento normativo con el apoyo técnico.

¿Nos queda camino por recorrer? Sin duda. Y más con el avance que se está produciendo... que está produciendo la inteligencia artificial -se ha citado que ya la utilizan los jáquer- o el cambio de paradigma que producirá la nueva normativa europea que establecerá responsabilidades, lo que generará -y estoy de acuerdo ahí con el señor Amilivia- un verdadero cambio. Pero también hay avances, compromisos y buenas prácticas sobre los que construir, y ese es el enfoque que hoy queremos remarcar, el de mejora continua, el aprendizaje institucional y la responsabilidad compartida. Muchas gracias.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Para finalizar, tiene de nuevo la palabra el presidente del Consejo de Cuentas, don Mario Amilivia.

EL PRESIDENTE DEL CONSEJO DE CUENTAS DE CASTILLA Y LEÓN (SEÑOR AMILIVIA GONZÁLEZ):

Pues muy bien. Muchas gracias a todas sus señorías por sus intervenciones. Recordar que el Consejo de Cuentas, que ha sido uno de los Consejos de España pioneros en esta materia, va a continuar haciendo fiscalizaciones en materia de ciberseguridad. Actualmente llevamos 27 fiscalizaciones en materia de ciberseguridad, que comenzamos en dos mil veintiuno: 18 informes han sido ya aprobados y otros 9 se encuentran en... en elaboración; 24 informes corresponden al sector público local y 3 al autonómico.

Los 24 informes del sector público local son 7 -que acabo de mencionar- de ayuntamientos intermedios; 7 en seguimiento o recomendaciones; 9 fiscalizaciones en capitales de provincia, las cuales se han aprobado ya todas menos Soria; y una fiscalización de seguimiento a las recomendaciones a la capital de provincia... en este caso es una capital de provincia: Palencia.

Y los 3 informes del sector público autonómico, en línea en la que estamos continuando, es el informe ya aprobado, que no presentado ante esta Comisión, sobre la Consejería de Agricultura, Ganadería y Desarrollo Rural como organismo pagador. Y 2 informes en elaboración sobre la Gerencia Regional de Salud y sobre la Universidad de Burgos.



Reiterar –como he dicho antes– que, desde nuestro punto de vista, lo más importante es constatar la falta de compromiso, en este caso de las distintas corporaciones, no la falta de cualificación del personal que existe, sino la falta de compromiso de las corporaciones locales, la decidida voluntad de... de acometer como algo esencial la política de seguridad, y la asignación de recursos presupuestarios; es decir, las decisiones no se trasladan a los presupuestos. También –como hemos dicho y todos creo que hemos coincidido– la necesidad de colaborar entre Administraciones, y actuar también... y la actuación también fundamental de las diputaciones, desde el punto de vista de su asistencia técnica.

Reiterar que, en materia de ciberseguridad, las exigencias van a ser cada vez más elevadas, porque los riesgos lo van a ser también cada vez más importantes. Luego la oportunidad de estos informes yo creo que se manifiesta por sí misma. Muchas gracias a todas sus señorías. Y por mi parte, nada más.

EL PRESIDENTE (SEÑOR CASTRO CAÑIBANO):

Finalizado el debate, de conformidad con lo establecido en la norma cuarta de la Resolución de la Presidencia de las Cortes de Castilla y León de siete de abril del dos mil nueve, se abre un plazo de cinco días para que los grupos parlamentarios puedan presentar ante la Mesa de la Comisión propuestas de resolución relativas a los informes de fiscalización que acaban de ser examinados. Dicho plazo finalizará, de conformidad en el Artículo 94 del Reglamento de la Cámara, el nueve de junio del dos mil veinticinco a las catorce horas.

Concluido el debate, agradeciendo al presidente del Consejo de Cuentas y todos los que le acompañan, se levanta la sesión. Muchísimas gracias.

[Se levanta la sesión a las dieciocho horas cinco minutos].