



## **La segunda revisión realizada a la seguridad informática de los ayuntamientos de Béjar, Ciudad Rodrigo y Benavente constata una mejora relativa gracias a las medidas adoptadas**

- **El presidente del Consejo de Cuentas presentó en las Cortes la actualización de los informes de ciberseguridad realizados en 2021. Los tres municipios han dado pasos importantes a raíz de las recomendaciones efectuadas, especialmente Benavente, que aprobó su Política de Seguridad, duplicando su puntuación global**
- **A la vista de los nuevos análisis, los tres ayuntamientos deberían impulsar su adecuación al Esquema Nacional de Seguridad, así como asegurar la dotación de recursos materiales y humanos imprescindibles para lograr un nivel de seguridad adecuado**

La segunda revisión sobre la seguridad informática de los ayuntamientos salmantinos de Béjar y Ciudad Rodrigo y del zamorano de Benavente ha venido a constatar, según los informes realizados por el Consejo de Cuentas tres años después de los primeros trabajos, que los tres han dado pasos importantes en ciberseguridad, especialmente el de Benavente, ya que duplicó su puntuación de madurez global en los controles básicos de seguridad.

No obstante, existe aún margen de mejora por parte de los tres ayuntamientos en un asunto -la seguridad informática- que es un proceso “continuo y fundamental” para cualquier organización en el contexto digital actual.

Las auditorías que viene realizando el Consejo ponen de manifiesto insuficientes dotaciones de medios, tanto humanos como materiales. En esta línea, el presidente de la institución, Mario Amilivia, destacó que las necesidades en todos los casos se podrían resumir en “compromiso y recursos. Compromiso por parte de los máximos órganos directivos, y recursos para alcanzar los objetivos comprometidos”.

En la que ha sido su octava comparecencia del año ante la Comisión de Economía y Hacienda de las Cortes, ha dado cuenta de los tres informes de seguimiento de las recomendaciones sobre seguridad informática realizadas en las auditorías llevadas a cabo en 2021 en dichos ayuntamientos, analizando y evaluando su situación actual.



Con estos nuevos informes, el Consejo de Cuentas pretende dar un nuevo impulso a la ciberseguridad de estos municipios, ya que el objetivo fundamental es “que todos alcancen y mantengan un nivel de seguridad mínimo”.

En este contexto, recordó que el nivel de seguridad mínimo requerido es cada vez más exigente. De hecho, el Esquema Nacional de Seguridad fue objeto de una actualización importante en 2022, elevando en muchos casos los requisitos. Además, una nueva directiva de la UE -ya en vigor- ha vuelto a subir el listón en esta materia en el ámbito comunitario.

Ante este panorama, resaltó que la cooperación y aunar esfuerzos son claves para superar las dificultades, porque son comunes en muchos casos. Por ello, las diputaciones provinciales, como administraciones que tienen entre sus competencias la asistencia técnica a los municipios, pueden ser un elemento clave para lograr el objetivo, destacó.

El Consejo aprobó en 2021, con carácter pionero en la materia, los informes de seguridad informática de 7 ayuntamientos de tamaño intermedio. Además de los tres citados, los referidos a Santa Marta de Tormes, Villaquilambre, Astorga y La Bañeza.

Además del seguimiento de las recomendaciones efectuadas entonces, se consideró oportuno realizar un seguimiento específico de estas siete primeras auditorías sobre ciberseguridad. Eso sí, una vez transcurrido un periodo suficiente para la implantación de las mejoras propuestas. Las de los cuatro municipios restantes están en elaboración.

Con carácter previo señaló que el Ayuntamiento de Béjar, con 12.021 habitantes (a 1 de enero de 2023) tenía una plantilla media de 262 empleados; el de Ciudad Rodrigo, 11.810 habitantes y una plantilla de 141; y el de Benavente, con 17.246 habitantes a 1 de enero de 2024, contaba con una plantilla de 214 empleados.

El tamaño de estos municipios implica cierta complejidad de gestión, lo que contrasta con las escasas dotaciones de recursos humanos y materiales dedicados a su área tecnológica. No obstante, han tenido que adaptarse necesariamente al uso de las nuevas tecnologías. 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 que llevan a cabo.

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. Para que un sistema de información sea fiable, es necesario, aunque no suficiente, que haya controles eficientes de ciberseguridad.

El objetivo principal de las tres auditorías presentadas es actualizar el análisis de los ocho controles más básicos de ciberseguridad llevados a cabo en la revisión de 2021, comprobando la implantación de las medidas que ya se recomendaron entonces.

Las recomendaciones realizadas en las anteriores auditorías precisaban para su implementación de un impulso por parte de las corporaciones respectivas.



A tal efecto, se ha revisado la aplicación efectiva de esas recomendaciones y, en concreto, si se adoptaron 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 obligatorias, la subsanación de las deficiencias técnicas detectadas y la realización del proceso de certificación del Esquema Nacional de Seguridad (ENS).

**Principales conclusiones.** El Ayuntamiento de Béjar 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 del primer informe se concretan en las siguientes mejoras:

- La creación de una plaza de técnico informático, actualmente sin cubrir. El personal responsable de tecnologías de la información se reduce a una persona contratada con carácter temporal.
- La adquisición de equipos y contratación de servicios que mejoran la seguridad de la red.
- Finalmente, la inclusión de cláusulas específicas en los contratos de servicios informáticos para cumplir determinadas medidas de seguridad.

El informe, que fue aprobado el pasado 21 de noviembre, revela que en estos más de 3 años transcurridos ha comenzado a tomar algunas medidas para revertir la situación, mejorando su calificación global. Las medidas son aún insuficientes, siendo imprescindible un impulso para conseguir un nivel de seguridad adecuada y garantizar el cumplimiento de la normativa.

Los controles básicos de ciberseguridad definidos se evalúan según un modelo de madurez de procesos que establece 6 niveles, de nivel cero o L0 a nivel 5 o L5. Se considera que la actividad organizativa de los controles debe alcanzar como mínimo el nivel 3 o L3, que se corresponde con un índice de cumplimiento del 80%. En el caso de Béjar el nivel de madurez global ha pasado del 5% en 2021, que suponía un nivel cero, al 20% en 2024, que se corresponde con nivel 1 o L1.

Por su parte, el Ayuntamiento de Ciudad Rodrigo también carece de una estrategia de tecnologías de la información y no ha establecido una gobernanza adecuada para poder afrontar con garantías el proceso de dotar a sus sistemas de información de un nivel de seguridad suficiente. Sus actuaciones a raíz de la auditoría de 2021 se concretaron en:

- 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.
- La mejora del proceso de copias de seguridad y contratación de un servicio de respaldo en la nube para copias de seguridad.
- El nombramiento del delegado de protección de datos.



Por otro lado, se mantiene la situación por la que el ayuntamiento 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 por la falta de aprobación de una política de seguridad como paso fundamental para iniciar el proceso de adaptación al ENS.

En estos tres años, el consistorio apenas ha mejorado su calificación global. Sigue siendo necesario impulsar 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, su puntuación global pasó del 3% en 2021 al 8% en 2024, en ambos casos dentro del nivel cero o L0.

Finalmente, el Ayuntamiento de Benavente, con la aprobación de la Política de Seguridad de la Información, dio un paso relevante para aprobar el proceso de dotar a sus sistemas de un nivel de seguridad suficiente. Aunque aun lejos del objetivo, el hecho de contar con un sistema de gobernanza hace previsible una evolución futura positiva.

Sigue careciendo, no obstante, 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. Sus actuaciones para cumplir con las recomendaciones que le fueron efectuadas en la primera fiscalización se concretaron en:

- La aprobación de la Política de Seguridad de la Información.
- La estabilización de una de las dos personas dedicadas a la tecnología de la información municipal. Sigue habiendo, sin embargo, un contexto de provisionalidad que no se ha abordado en su totalidad.
- La contratación de servicios y compra de equipamiento tecnológico, aunque la renovación no ha sido completa, quedando todavía elementos relevantes sin actualizar.
- La adecuación a la normativa de protección de datos.

Además, no se han realizado cambios relevantes en el entorno tecnológico, optando por un modelo donde las aplicaciones se instalan fundamentalmente en su propia infraestructura, sin utilizar tampoco el apoyo específico en materia de e-administración y soporte informático que ofrece la Diputación de Zamora.

Las actuaciones realizadas, pese a conseguirse hitos importantes, aun son puntuales e insuficientes ya que no existe una planificación estratégica de la tecnología de la información municipal que garantice una dotación de recursos ajustada a las necesidades actuales y futuras.

No obstante, en el periodo de tres años ha tomado medidas, algunas relevantes, pero todavía insuficientes. Precisa de un impulso importante para conseguir un nivel de seguridad adecuado y garantizar el cumplimiento de la normativa de aplicación. La puntuación global de los controles de seguridad se ha duplicado, pasando del 16% en 2021 al 32% en 2024, en ambos casos dentro del nivel 1 o L1.



**Nuevas recomendaciones.** A la vista de esta segunda revisión en los tres ayuntamientos, el Consejo de Cuentas realiza nuevas recomendaciones: 5 para Béjar; cuatro para Ciudad Rodrigo y 7 para Benavente, orientadas todas ellas a las actuaciones necesarias para que alcancen un nivel de ciberseguridad adecuado.

Hay dos recomendaciones comunes para las tres entidades:

- En primer lugar, el Ayuntamiento, en su caso el alcalde, debería impulsar las actuaciones para acometer 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 alcanzar de esta forma un nivel de ciberseguridad adecuado
- Asimismo, debería asegurar 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 éstas 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:

- Ambas corporaciones, o los alcaldes, en su caso, deberían, 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 procesos relevantes de gestión, especialmente la aplicación de nóminas, 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 toman medidas para garantizar la capacidad de reestablecer 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 disponen de copias y están adecuadamente protegidas.

Con carácter singular para el Ayuntamiento de Ciudad Rodrigo, como cuarta y última recomendación:



- El ayuntamiento o el alcalde, en su caso, dada la relevancia que las aplicaciones proporcionadas por 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.

Para finalizar, las recomendaciones dirigidas específicamente al Ayuntamiento de Benavente:

- De acuerdo con el modelo de gobernanza aprobado en 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 las funciones que le son propias, entre otras, de coordinación, planificación y seguimiento, para asegurar de esta forma que se realizan las tareas definidas en la política de seguridad.

En cuanto al proceso continuo de identificación y corrección de vulnerabilidades:

- 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 periódica de actuaciones como las que se han llevado a cabo desde la anterior auditoría.

Y en lo referente al uso controlado de los privilegios administrativos:

- El concejal competente debería impulsar la inclusión en todos los contratos de 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.

- 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 las contraseñas por defecto y la definición de políticas robustas y homogéneas para los sistemas de autenticación.

- Finalmente, 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 artículo 24 del 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 puede utilizarse como referencia la guía del Centro Criptológico Nacional sobre “Registro de la actividad de los usuarios”.