CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SANTA MARTA DE TORMES (SALAMANCA)

TRATAMIENTO DE ALEGACIONES

PLAN ANUAL DE FISCALIZACIONES 2021

ÍNDICE

ACLARACIONES

El contenido de las alegaciones figura en tipo de letra normal, reproduciéndose previamente el párrafo alegado en letra cursiva.

La contestación a las alegaciones presentadas se hace en tipo de letra negrita.

Las referencias de las páginas están hechas con relación al Informe provisional para alegaciones.

Se han numerado las alegaciones formuladas por el Ente fiscalizado a efectos de una mayor claridad en su exposición y tratamiento en la presente Propuesta.

I. ALEGACIÓN PRIMERA

Párrafos de referencia (páginas 24 y 25, conclusiones 1 a 10).

III.1. ENTORNO TECNOLÓGICO Y SISTEMAS DE INFORMACIÓN OBJETO DE LA FISCALIZACIÓN

1) *Las competencias del área de nuevas tecnologías recaen en el 4ª Teniente de Alcalde, que se responsabiliza de entre otras áreas, "nuevas tecnologías". De los trabajos realizados reflejados en las conclusiones siguientes no se deduce que esa concejalía ejecute una dirección política efectiva de la seguridad informática. (Apartado V.1.1)*

2) *Según la relación de puestos de trabajo aprobada en sesión ordinaria celebrada por el Pleno el día 23 de diciembre de 2019, el Ayuntamiento de Santa Marta de Tormes no dispone de personal dedicado a las tecnologías de la información. (Apartado V.1.1)*

3) *No se ha definido una estructura de TI en el Ayuntamiento para asumir las responsabilidades que le corresponden con respecto a la seguridad de los servicios que ofrece y la información que maneja, con independencia de si la gestión se asume con recursos propios o externalizados en empresas privadas o en otras administraciones. (Apartado V.1.1)*

4) *A efectos de esta fiscalización, la interlocución con el equipo auditor ha sido asumida por personal de la empresa "MT Comunicación" que realiza las tareas de gestión de TI en el Ayuntamiento de Santa Marta de Tormes, reconociendo así el Ayuntamiento que no ejerce un control sobre la prestación, toda vez que los detalles sobre ésta los desconoce, debiendo recurrir a la propia empresa para aportar la información solicitada. Se da la circunstancia de que el titular de esta empresa trabaja en el Ayuntamiento y ha incumplido el deber de colaboración para con el Consejo de Cuentas como se detalla en el apartado II.3 del presente Informe. (Apartado V.1.1)*

5) *No ha sido posible obtener los detalles de los servicios que presta la empresa al no existir una contratación unificada de éstos, sino que se trata de una serie de contratos menores que se realizan periódicamente y también para cubrir las necesidades puntuales que van apareciendo, de los que, por su carácter de contrato menor, no se dispone de un pliego de prescripciones técnicas para su revisión, ni ha aportado el ayuntamiento detalle de los servicios que incluyen. (Apartado V.1.1)*

6) *El Ayuntamiento carece de documentación detallada de sus sistemas y procesos de gestión, estando la única información existente en manos de terceros, y al carecer de personal de TI tampoco tiene la experiencia y el conocimiento que puede aportar el capital humano. (Apartado V.1.1)*

7) *El Ayuntamiento no ha realizado una identificación y categorización según el ENS de los sistemas de información de que dispone, tarea básica para definir correctamente el alcance de cualquier proceso de adecuación a la normativa en materia de seguridad de la información que se pretenda acometer. (Apartado V.1.2)*

8) *Se ha optado por un modelo mixto, utilizando para procesos muy relevantes los servicios ofrecidos por la Diputación de Salamanca (administración electrónica, padrón y contabilidad), estando los servicios y la información que se presta, en algunos casos en la nube (modalidad SaaS) y en otros en local. La utilización de modelos en la nube simplifica la implantación de medidas de seguridad, pero requiere un control sobre la prestación del servicio, al no eximir en modo alguno al Ayuntamiento de la responsabilidad última. Los modelos en local requieren de la aplicación de medidas de seguridad más complejas para lo que es necesario disponer de recursos, humanos y materiales, suficientes. (Apartado V.1.2)*

9) *Del examen de la estructura de la red del Ayuntamiento se concluye que en buena medida no existe una red corporativa como tal, sino un conjunto de equipos que comparte un acceso a internet y un grupo de trabajo, ya que no hay un servidor de ficheros o un dominio, únicamente recursos compartidos en un grupo de trabajo. (Apartado V.1.3)*

10) *El Ayuntamiento facilita el teletrabajo a su personal mediante acceso por VPN y también gracias al sistema de administración electrónica en la nube (SaaS), que permite acceder de igual forma con independencia de la ubicación física.(Apartado V.1.3)*

Alegación realizada

(1). Hacen referencia a la inexistencia de dirección política en la materia, cuestión que no es cierta ya que el concejal de Nuevas Tecnologías está informado constantemente de las líneas de trabajo del área. Además, se llevan a cabo reuniones de trabajo en las que propone cambios y mejoras para el servicio.

(2, 3 y 4). Efectivamente la RPT del Ayuntamiento no contempla personal técnico adscrito al área de Nuevas Tecnologías por lo que es la empresa adjudicataria del contrato la responsable de la prestación del servicio, subrayando que no existe vinculación laboral entre el responsable de la empresa y el Ayuntamiento.

La persona designada de contacto, por tanto, no tiene ninguna vinculación laboral, ni funcionarial, ni como personal eventual tal y como se puede acreditar con la correspondiente Relación de Puestos de Trabajo (publicada en el BOP N° 6 del 10-1-2020, modificada según anuncio publicado en el BOP N° 22 del 3-2-2021), así como en la Plantilla (BOP N° 13 del 18-1-2021).

La posible confusión puede deberse por aparecer dicha persona en algún correo electrónico en su calidad de "Jefe de Prensa del Ayuntamiento de Santa Marta de Tormes" (apartado II.3, pág. 22 del informe provisional), teniendo en cuenta que aquella

es adjudicataria de un contrato de asesoría de comunicación, protocolo y relaciones con la prensa del Ayuntamiento.

Con respecto a la falta de cumplimiento del deber de colaboración para con este Consejo de Cuentas (tal y como se detalla en el apartado II.3 del citado informe provisional), este Ayuntamiento lamenta profundamente que la persona designada haya podido incurrir en ese incumplimiento, del cual no era conocedor hasta el extremo en que se refiere en el apartado II.3 del informe antes citado, pues, en ningún momento ha existido ánimo o intencionalidad alguna de no colaborar con esta institución.

En cualquier caso, este Ayuntamiento ofrece la colaboración necesaria, así como la práctica de las actuaciones y pruebas pertinentes que este Consejo de Cuentas considere oportunas, para que, de manera inmediata, se puedan aclarar todas aquellas cuestiones pendientes, siendo la única intención de esta Corporación la máxima colaboración con el Consejo de Cuentas, como, por otra parte, es habitual en otros procedimientos seguidos con esta institución.

A tal efecto, facilitamos como persona de contacto para futuras actuaciones que resulten necesarias practicar, además de la persona designada, a Dª Esther Corchero Martín, Jefa de Contabilidad y Presupuestos de este Ayuntamiento (con correo electrónico: ecorchero@santamartadetormes.org) rogando sea también objeto de las comunicaciones oportunas.

(5, 6 y 7). En la actualidad el Ayuntamiento está trabajando para sacar a licitación, de acuerdo con la nueva ley de contratos, el servicio de Mantenimiento Informático. En este contrato estarán plasmados y definidos todos los servicios y sistemas de gestión en los que sí estarán registrados toda la información, servicios, necesidades, así como el pliego de prescripciones técnicas y las pautas marcadas por el ENS. También se recogerán en este pliego cuestiones como el inventario de activos de hardware.

(8, 9 y 10). El día 1 de agosto han comenzado los trabajos para sustituir la red física del Ayuntamiento por un sistema totalmente virtualizado que estará funcionando plenamente a mediados de la semana del 13 de septiembre corrigiendo y eliminando la mayoría de los problemas de seguridad. Todos los trabajadores del Ayuntamiento accederán a través de una vpn y podrán compartir los archivos con un Nas.

Contestación a la alegación

Con respecto a lo indicado sobre la conclusión (1), el Informe afirma que la dirección política no es efectiva, no que sea inexistente. El Ayuntamiento no aporta en su alegación ninguna justificación de la efectividad de la dirección política que realiza, más allá de señalar que el Concejal está informado de las actuaciones que realiza la empresa de mantenimiento, y realiza propuestas de cambio o mejoras, tareas que no suponen una dirección política efectiva, como se deduce de los siguientes hechos:

- **No se ha definido una estructura de TI en el Ayuntamiento para asumir las responsabilidades que le corresponden (conclusión 3)**

- **No se han realizado licitaciones planificadas en materia de servicios informáticos, sino que se ha recurrido a contrataciones menores sucesivas, evidenciando la falta de planificación del servicio (conclusión 5)**

- **El conocimiento sobre el entorno tecnológico no se encuentra en el Ayuntamiento, como pone de manifiesto el hecho de que la interlocución con el equipo auditor haya tenido que ser asumida por la propia empresa de mantenimiento, y no por personal del Ayuntamiento, que en todo caso podría ser asistido en las cuestiones más técnicas por la empresa de mantenimiento informático, pero que debería tener un mínimo conocimiento sobre sus sistemas de información (conclusiones 3, 4 y 6)**

Acerca de las alegaciones realizadas sobre las conclusiones (2, 3 y 4), el Ayuntamiento confirma lo expuesto en el Informe acerca de la falta de una estructura de TI en el Ayuntamiento.

Con respecto a la vinculación laboral de la persona responsable de la interlocución del Ayuntamiento el Consejo de Cuentas constata que se presenta como "jefe de prensa" del ayuntamiento, con correo del ayuntamiento y el escudo del ayuntamiento en su firma. En caso de no ser efectivamente un trabajador, el Ayuntamiento deberá tomar las medidas necesarias para aclarar la situación y evitar el uso de su correo o de sus símbolos por personas ajenas al mismo.

Respecto a que es adjudicataria de un contrato de *"asesoría de comunicación, protocolo y relaciones con la prensa del Ayuntamiento",* en realidad según la Plataforma de Contratos del Sector Público, dicho contrato quedó desierto la primera vez que se licitó en marzo de 2021, y tras publicarse por segunda vez la licitación en agosto de 2021, está ahora en fase de evaluación, luego, de la documentación que obra en poder del Consejo, esa afirmación no sería precisa. Es cierto que en los menores publicados en el portal de transparencia (en la Plataforma de Contratos del Sector Público no se pudo encontrar) hay uno con el siguiente contenido: "*723 Asesoría de Comunicación, protocolo y relaciones con la prensa. 4 13332,99 02/03/2021 MARTIN TAPIA FRANCISCO JAVIER 002242730N SLNE*"

Con respecto a lo indicado sobre las conclusiones (5, 6 y 7), la alegación ratifica el contenido del Informe.

Finalmente, en las alegaciones sobre las conclusiones (8, 9 y 10), el Ayuntamiento informa de los cambios realizados con posterioridad a la emisión del Informe Provisional, y que según el Ayuntamiento suponen un cambio sustancial en la seguridad de la red y en el entorno tecnológico del Ayuntamiento.

Dado que el Ayuntamiento en esta primera alegación solicitó, además, la realización de las pruebas adicionales necesarias, se han llevado éstas a cabo y se ha evaluado su impacto, realizándose las siguientes modificaciones que se han incorporado al Informe en aplicación del Art. 26.5 del Reglamento del Consejo de Cuentas:

En la página 25, conclusión 12), donde dice "*No se han implantado medidas para impedir la conexión de dispositivos físicos no autorizados en la red cableada y las que existen en la red inalámbrica no se han podido verificar",* debe decir *"No se han implantado medidas efectivas para impedir la conexión de dispositivos físicos no autorizados".*

En la página 26, conclusión 15) donde dice "*El Ayuntamiento utiliza para sistemas de información muy relevantes, aplicaciones cuya contratación realiza la Diputación de Salamanca (a través de CIPSA) sin que se hayan previsto los medios de control que el ENS establece para el uso de proveedores externos."* Debe decir *"El Ayuntamiento utiliza para sistemas de información muy relevantes, aplicaciones cuya contratación realiza bien Diputación de Salamanca (a través de CIPSA), bien el propio Ayuntamiento directamente, sin que se hayan previsto los medios de control que el ENS establece para el uso de proveedores externos".*

En la página 26, conclusión 18) donde dice "*El Ayuntamiento hace uso del software ofrecido por la Diputación en una parte relevante de sus sistemas de información, sin que por parte del Ayuntamiento se hayan previsto mecanismos que aseguren que se realiza el proceso de identificación y corrección de vulnerabilidades en tiempo y forma.",* debe decir *"El Ayuntamiento hace uso del software ofrecido por la Diputación en una parte relevante de sus sistemas de información, sin que por parte del Ayuntamiento se hayan previsto mecanismos que aseguren que se realiza el proceso de identificación y corrección de vulnerabilidades en tiempo y forma. Tampoco se introducen cláusulas en este sentido en las contrataciones que el Ayuntamiento realiza directamente".*

En la misma conclusión donde dice *"Con respecto al resto de elementos que el Ayuntamiento mantiene directamente, no realiza ningún proceso de identificación y corrección de vulnerabilidades. El riesgo de que una vulnerabilidad crítica permanezca sin corregir en sus sistemas y cree una ventana de oportunidad para un ataque es elevado",* debe decir *"Con respecto al resto de elementos que el Ayuntamiento mantiene directamente, no realiza un proceso de identificación y corrección de vulnerabilidades sistemático, dependiendo únicamente de actuaciones puntuales de los técnicos. El riesgo de que una vulnerabilidad crítica permanezca sin corregir en sus sistemas y cree una ventana de oportunidad para un ataque es elevado".*

En la página 27, se introduce una nueva conclusión, numerada como 21), *"Hay un cierto control de las cuentas con privilegios administrativos de los sistemas más relevantes, aunque con un amplio margen de mejora (Apartado V.5)".* Como

consecuencia, todas las conclusiones de la 21) en adelante se renumeran incrementándose una unidad.

En la página 27, conclusión 22) (renumerada como 23), donde dice ***"No consta que se hayan establecido contractualmente o por convenio mecanismos que permitan asegurar el buen uso y gestión de las cuentas de administración controladas por proveedores externos",*** **debe decir** ***"No se han establecido contractualmente o por convenio mecanismos que permitan asegurar el buen uso y gestión de las cuentas de administración controladas por proveedores externos".***

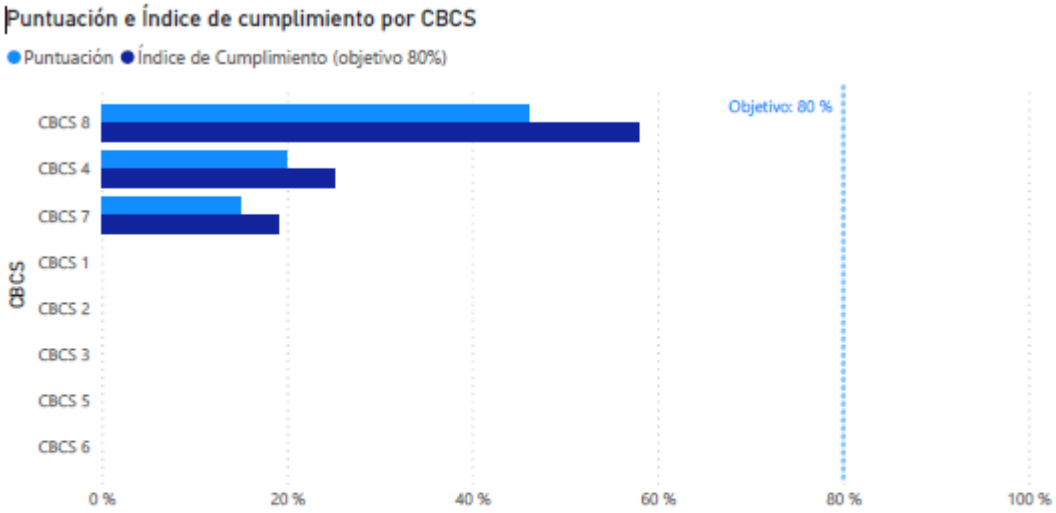
En la página 27, conclusión 23) (renumerada como 24), donde dice ***"No se ha podido verificar la existencia de un proceso de control del uso de privilegios administrativos, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos"",*** **debe decir "*****En el proceso para el control del uso de privilegios administrativos el Ayuntamiento alcanza un índice de madurez L1, en el que "el proceso existe, pero no se gestiona"."***

En la página 28, conclusión 30) (renumerada como 31), donde dice ***"No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento si describe una sistemática para su realización. Sin embargo, no se ha podido verificar que se estén realizando",*** **debe decir** ***"No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento sí describe una sistemática para su realización y se realizan en parte de los sistemas relevantes, disponiendo de herramientas para ello".***

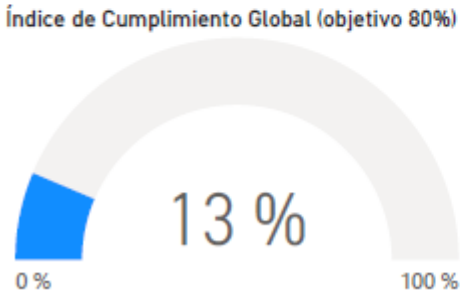
En la página 28, conclusión 32) (renumerada como 33) donde dice ***"No se ha podido verificar que se aplican medidas suficientes para la protección de las copias de seguridad",*** **debe decir** ***"Se aplican medidas insuficientes para la protección de las copias de seguridad, siendo de especial relevancia la carencia de mecanismos de control en la contratación de las copias de seguridad en infraestructuras de terceros".***

En la página 28, conclusión 33) (renumerada como 34), donde dice ***"No se ha podido verificar la existencia del proceso para la realización de copias de seguridad, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos"",*** **debe decir** ***"De acuerdo con las conclusiones de esta área, el proceso de realización de copias de seguridad de datos y sistemas por el Ayuntamiento alcanza un índice de madurez L1, en el que en el que "el proceso existe, pero no se gestiona"."***

En la página 29, apartado "III.10", donde dice ***"El Ayuntamiento de Santa Marta de Tormes no ha implantado ninguno de los subcontroles revisados, o bien, dada la falta de disposición para la realización de pruebas, o para aportar la documentación requerida, no ha podido demostrar su efectividad."*** **debe decir** ***"La situación global de los controles básicos de ciberseguridad se puede resumir en el siguiente gráfico donde se indica la puntuación alcanzada y el objetivo de cumplimiento para cada uno de ellos.", y se introduce a continuación el siguiente gráfico, numerado como "1":***



CBCS	Descripción	Puntuación	Índice de Cumplimiento (objetivo 80%)
CBCS 8	Cumplimiento normativo	46 %	58 %
CBCS 4	Uso controlado de privilegios administrativos	20 %	25 %
CBCS 7	Copias de seguridad de datos y sistemas	15 %	19 %
CBCS 1	Inventario y control de dispositivos físicos	0 %	0 %
CBCS 2	Inventario y control de software autorizado y no autorizado	0 %	0 %
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	0 %	0 %
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	0 %	0 %
CBCS 6	Registro de la actividad de los usuarios	0 %	0 %
Total			**13 %**



El nivel de madurez alcanzado globalmente por la entidad corresponde al nivel **L1**

El índice de cumplimiento (sobre un objetivo de madurez L3 que corresponde a una puntuación del 80%) es del **13%**.

Como consecuencia, se renumeran los gráficos del 1 en adelante, incrementándose en una unidad.

En cuanto a la falta de colaboración que el Consejo reflejó en el Informe Provisional, una vez que ha sido subsanada por parte del Alcalde, el Consejo solo puede destacar la necesidad de una adecuada valoración del trabajo de las Instituciones de la Comunidad, especialmente cuando el beneficiario del Informe es el Ayuntamiento, en tanto recibe una visión objetiva de su situación en este ámbito junto con propuestas claras para mejorarla.

Como consecuencia de la alegación presentada se modifica el apartado II.3 LIMITACIONES que pasa a tener la siguiente redacción:

"El Ayuntamiento designó como persona de contacto para la remisión de la información que se solicitara, así como para la realización de las pruebas pertinentes, a D. Javier Martín Tapia. El Consejo de Cuentas intentó repetidamente obtener la información por todos los medios disponibles sin éxito, siendo finalmente en el periodo de alegaciones cuando el Alcalde del Ayuntamiento solicitó que se realizaran las pruebas que hasta el momento no se habían podido realizar, dando las instrucciones oportunas dentro de su organización."

Se modifica la conclusión 4 que pasa a tener la siguiente redacción:

"A efectos de esta fiscalización, la interlocución con el equipo auditor ha sido asumida por personal de la empresa "MT Comunicación" que realiza las tareas de gestión de TI en el Ayuntamiento de Santa Marta de Tormes, reconociendo así el Ayuntamiento que no ejerce un control sobre la prestación, toda vez que los detalles sobre ésta los desconoce, debiendo recurrir a la propia empresa para aportar la información solicitada."

Se elimina la recomendación 1.

Como consecuencia, se renumeran las siguientes recomendaciones decrementándose en una unidad.

II. ALEGACIÓN SEGUNDA

Párrafos de referencia conclusiones apartado III.2.

III.2. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

11) No existe un inventario que permita un control adecuado de los activos hardware. (Apartado V.2.1)

12) No se han implantado medidas para impedir la conexión de dispositivos físicos no autorizados en la red cableada y las que existen en la red inalámbrica no se han podido verificar. (Apartado V.2.2)

13) No existe el proceso de gestión de inventario y control de hardware, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.2.3)

Alegación realizada

(11 y 13). Actualmente el Ayuntamiento no tiene un inventario actualizado de los activos de hardware. Esta situación será corregida en las próximas fechas ya que se han iniciado los trabajos para comenzar a inventariar todos los elementos de hardware que permitan un mayor control.

(12). Es cierto que no hay medidas específicas para conectar dispositivos físicos a no autorizados, aunque solamente están activas las "bocas" de la red a la que están conectados los equipos del consistorio. El resto de bocas están deshabilitadas y determinados equipos tiene bloqueados los puertos usb para que a los equipos no puedan conectarse dispositivos no autorizados.

Contestación a la alegación

Sobre lo señalado acerca de las conclusiones (11 y 13), la alegación ratifica el contenido del Informe.

Para dar respuesta a la alegación al contenido de la conclusión (12), tal y como se ha detallado con anterioridad, se realizaron las pruebas adicionales pertinentes para comprobar si en efecto se encontraban deshabilitadas, concluyéndose tras solicitar aclaración al Ayuntamiento durante la sesión de pruebas, que la medida aplicada consiste en no parchear los puertos de red que no se están utilizando.

Se modifica en consecuencia el memorándum detallado enviado al Ayuntamiento y una vez evaluadas nuevamente las medidas que se aplican en su conjunto, se estima que esta medida, es insuficiente, y no se aplican otras adicionales que puedan complementarla, por lo que no se modifican las conclusiones sobre la aplicación del control.

No se acepta la alegación toda vez que no modifica en contenido del Informe.

III. ALEGACIÓN TERCERA

Párrafos de referencia Conclusiones apartado III.3.

III.3. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO Y NO AUTORIZADO (CBCS 2)

14) *El Ayuntamiento de Santa Marta de Tormes no dispone de un inventario de activos software, ni ha adoptado medidas efectivas para impedir el uso de software no autorizado, por lo que no existe control sobre qué software se utiliza, ni del estado de sus licencias ni del soporte del software. (Apartado V.3.1)*

15) *El Ayuntamiento utiliza para sistemas de información muy relevantes, aplicaciones cuya contratación realiza la Diputación de Salamanca (a través de CIPSA) sin que se hayan previsto los medios de control que el ENS establece para el uso de proveedores externos. (Apartado V.3.2)*

16) *No existe un plan de mantenimiento de software ni de compra o adquisición de licencias, delegando por completo en la empresa de mantenimiento cualquier control, sin que el Ayuntamiento disponga al menos de un inventario de licencias, asumiéndose riesgos importantes asociados a la falta de soporte y uso inadecuado*

de licencias de software, con impacto potencial importante para el funcionamiento de la organización. (Apartado V.3.2.3)

17) *No existe el proceso de gestión de inventario de software autorizado, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.3.4)*

Alegación realizada

(14 y 17) Como dice en este punto las conclusiones del informe provisional, el Ayuntamiento no dispone de inventario formalizado y estandarizado de software aunque sí existe una relación de las aplicaciones utilizadas por los usuarios dependiendo del puesto que desempeñan.

(15) También está previsto la contratación, de cara al próximo año, del servicio que permita el control y seguimiento de las pautas y estándares fijadas por el ENS.

(16) En cuanto a las licencias, están en poder del Ayuntamiento y pueden comprobarse las correspondiente a los sistemas antivirus de equipos y correo, así como de otras aplicaciones que se van incorporando como son Adobe DC, Photoshop o Autocad. En el futuro está previsto continuar con la compra e implantación de licencias.

Contestación a la alegación

Sobre lo indicado acerca de las conclusiones (14 y 15), la alegación ratifica el contenido del Informe, dado que el Ayuntamiento confirma la inexistencia de inventario, y sobre la relación de aplicaciones por usuario, solicitada esta al Ayuntamiento, únicamente se proporciona un listado de tres aplicaciones, con indicación del número de puestos en que se encuentran instaladas, y por tanto no implica ningún cambio sobre las conclusiones del Informe.

No obstante, para una mayor precisión y como consecuencia de la documentación aportada por el Ayuntamiento en la fase de alegaciones, se realiza el cambio en la redacción de la conclusión 15) que ya se ha detallado en la respuesta a la alegación primera.

Sobre lo indicado acerca de la conclusión 16) no se ha aportado documentación que sustente la afirmación del Ayuntamiento, por lo que la alegación presentada no modifica el contenido del Informe.

IV. ALEGACIÓN CUARTA

Párrafos de referencia Conclusiones apartado III.4

III.4. PROCESO CONTINUO DE IDENTIFICACIÓN Y CORRECCIÓN DE VULNERABILIDADES (CBCS 3)

18) *El Ayuntamiento hace uso del software ofrecido por la Diputación en una parte relevante de sus sistemas de información, sin que por parte del Ayuntamiento se hayan previsto mecanismos que aseguren que se realiza el proceso de identificación y corrección de vulnerabilidades en tiempo y forma. (Apartado V.4.1)*

19) *Con respecto al resto de elementos que el Ayuntamiento mantiene directamente, no realiza ningún proceso de identificación y corrección de vulnerabilidades. El riesgo de que una vulnerabilidad crítica permanezca sin corregir en sus sistemas y cree una ventana de oportunidad para un ataque es elevado. (Apartado V.4.1)*

20) *No existe el proceso de identificación y corrección de vulnerabilidades, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.4.2)*

Alegación realizada

(18) Como dicen el Ayuntamiento utiliza una herramienta externa, Gestiona, facilitada por Diputación de Salamanca para una de las partes más relevantes de sus sistemas de información. Esto se debe a que el Ayuntamiento de Santa Marta, como la gran mayoría de los Ayuntamientos de su tamaño y población no cuenta con los recursos necesarios ni suficiente para poder desarrollar este tipo de aplicaciones de gestión interna de expedientes o sede electrónica. Tampoco se cuenta con los recursos necesarios para tener mecanismo de vigilancia del correcto funcionamiento del servicio ni de la corrección de vulnerabilidades. Es otro de los motivos de la contratación de este servicio con una empresa especializada que ofrece todas las garantías y asesoramiento para la identificación de vulnerabilidades y su posterior corrección.

En cuanto al resto de sistemas, es cierto que ese proceso no está procedimentado y descrito pormenorizadamente, pero existe. El Ayuntamiento revisa periódicamente los procedimientos para corregir esas posibles vulnerabilidades.

(19) El anterior punto se deduce que la identificación y corrección de vulnerabilidades no es un procedimiento que actualmente no se esté llevando a cabo en el Consistorio. En primer lugar se está haciendo por la empresa EsPúblico, propietaria y prestadora de la plataforma de gestión de expedientes y también por parte del Ayuntamiento, aunque no esté formalizado y procedimentado.

Contestación a la alegación

La falta de recursos que impiden realizar un correcto seguimiento del servicio prestado por proveedores externos ya sea mediante el convenio con la

Diputación, o por contrataciones realizadas, no exime al Ayuntamiento de sus obligaciones, y refuerza el sentido de la recomendación que señala la necesidad de dotar con recursos suficientes a su departamento de TI.

Con respecto a la afirmación de que la contratación de una empresa especializada ofrece todas las garantías, sólo puede aceptarse como cierta en caso de que se apliquen los requisitos mínimos que exige en ENS acerca del uso de recursos externos, lo que no se da para la contratación de las empresas *"MT Comunicación"* y "*Wurth*", ni para el uso de los recursos que proporciona la Diputación.

En las pruebas realizadas en la fase de alegaciones, el Ayuntamiento detalla cómo realiza la gestión de vulnerabilidades, deduciéndose que no existe una sistemática, dependiendo en todo caso de actuaciones individuales de los técnicos de la empresa mantenedora y con las limitaciones que implica la falta de control sobre el software instalado, que no permite conocer en detalle las aplicaciones, versiones, niveles de parcheo, etc. y por tanto realizar un proceso de gestión de vulnerabilidades adecuado.

Se procede a aclarar en el memorándum detallando las actuaciones que realiza el Ayuntamiento y se modifica la conclusión 18) en el sentido ya detallado en la contestación a la alegación primera.

V. ALEGACIÓN QUINTA

Párrafos de referencia Conclusiones apartado III.5.

III.5 USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS (CBCS 4)

21) *No existe un procedimiento para la realización de tareas como la gestión de usuarios administradores, el cambio de las contraseñas por defecto, ni se han definido políticas homogéneas para los sistemas de autenticación, ni para el uso dedicado de las cuentas de administración. Esta carencia propicia fallos de seguridad potencialmente relevantes. (Apartado V.5)*

22) *Los usuarios son administradores de sus equipos sin que se justifique la necesidad de tener esa condición. (Apartado V.5.1.1)*

23) *No consta que se hayan establecido contractualmente o por convenio mecanismos que permitan asegurar el buen uso y gestión de las cuentas de administración controladas por proveedores externos. (Apartado V.5.1.2)*

24) *No se ha podido verificar la existencia de un proceso de control del uso de privilegios administrativos, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.5.6)*

Alegación realizada

(20, 21, 22 y 23) Actualmente en el Ayuntamiento las labores que desempeñan la mayoría de los trabajadores prácticamente se ciñen al uso de Gestiona. Esta aplicación tiene la seguridad suficiente y periódicamente se realiza un cambio obligatorio de las contraseñas de acceso.

Además, la herramienta Bitdefender asegura el uso de navegación según establecen círculos de privilegios en función de las necesidades de cada puesto. Hay permisos para navegar en cualquier url o permisos para acceder a un grupo de url's determinado.

Los proveedores externos son habitualmente empresas reconocidas que ofrecen las garantías necesarias de profesionalidad y seguridad. En cualquier caso es otro de los puntos que se establecerá de cara a un futuro para incluir la firma de este tipo de convenios o contratos que aseguren el buen uso de estas cuentas.

Contestación a la alegación

Lo indicado sobre las conclusiones (20, 21, 22 y 23) sobre el uso prácticamente exclusivo de la aplicación Gestiona, siendo este un sistema de información en la nube, en la modalidad "*software como servicio o SaaS, Software as a Servicie*" implica que precisamente el proceso de gestión de privilegios administrativos adquiere aún mayor relevancia, dado que el uso inadecuado de usuarios administradores es uno de los riesgos que la *"Guía Práctica de Fiscalización de los Órganos de Control Externo (GPF-OCEX) 1403, Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube"* identifica como derivado o acentuado por el uso de soluciones en la nube. Dicha guía indica que *"habrá administradores ajenos a la entidad cuya existencia no será "visible" (en la mayoría de los casos) ni para los auditores ni para la propia entidad auditada. A veces las entidades con servicios cloud contratados confían, sin verificar, en la buena gestión de los usuarios realizada por el CSP incurriendo en riesgos importantes".*

En el caso de Santa Marta de Tormes, se produce esta circunstancia, al carecer de los mecanismos de control mínimos exigidos por el ENS.

Tras la realización de las pruebas correspondientes, se verificó que la herramienta BitDefender no realiza ninguna función relativa a la gestión de usuarios administradores.

Finalmente, como ya se ha indicado, la contratación de servicios a proveedores de prestigio reconocido en el sector, y con certificaciones de cumplimiento del ENS al nivel requerido, es condición necesaria pero no suficiente como se ha puesto de relieve en el Informe.

No se acepta la alegación toda vez que no modifica el contenido del Informe.

VI. ALEGACIÓN SEXTA

Párrafos de referencia Conclusiones apartado III.6.

III.6 CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE DE DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES (CBCS 5)

25) *El Ayuntamiento no realiza un proceso de configuración segura en los sistemas que administra directamente, lo que incluye todos los equipos de usuario y los servidores donde se instalan las aplicaciones del fabricante Wurth (Wintask SICAL y Padrón). (Apartado V.6.1)*

26) *No se ha podido verificar la existencia de mecanismos que impidan cambios no autorizados o erróneos de la configuración, ni permitan su detección y su corrección en un periodo de tiempo oportuno. (Apartado V.6.2)*

Alegación realizada

(24 y 25) La seguridad en todos los equipos aumentará y mejorará notablemente con el cambio y la virtualización que está realizando en estos momentos. Los dos servidores que están actualmente en funcionamiento y que albergan las bases de datos de Padrón, Contabilidad, Gestión Tributaria, Tasas.... pasarán a ser un servicio cloud y este problema se corregirá en gran medida.

Contestación a la alegación

La alegación refuerza el contenido del Informe toda vez que el Ayuntamiento reconoce la necesidad de realizar cambios para poder implantar este proceso de configuración segura.

No se acepta la alegación toda vez que no modifica el contenido del Informe.

VII. ALEGACIÓN SÉPTIMA

Párrafos de referencia Conclusiones apartado III.7.

III.7. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS (CBCS 6)

27) *El Ayuntamiento no realiza ninguna acción específica para recoger, recopilar, proteger o analizar los registros de actividad de los usuarios, contando únicamente con los logs que por defecto o por parte de los proveedores externos, se encuentren activados en los sistemas. (Apartado V.7.1)*

Alegación realizada

(27) Por el tamaño y número de empleados del Ayuntamiento no se ha considerado necesario, hasta el momento, hacer una relación de los logs del Ayuntamiento, cuestión que será subsanada con la firma del próximo contrato de

"Mantenimiento de Sistemas Informáticos". Esta opción será incluida dentro de los servicios exigidos.

Contestación a la alegación

La alegación refuerza el contenido del Informe toda vez que el Ayuntamiento reconoce la necesidad de subsanar esta carencia.

VIII. ALEGACIÓN OCTAVA

Párrafos de referencia Conclusiones apartado III.8.

III.8. COPIAS DE SEGURIDAD DE DATOS Y SISTEMAS (CBCS 7)

30) *No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento si describe una sistemática para su realización. Sin embargo, no se ha podido verificar que se estén realizando. (Apartado V.8.1)*

31) *No se realizan pruebas de recuperación completas y periódicas por lo que no es posible asegurar que las copias serán válidas en caso de necesitar una recuperación. (Apartado V.8.2)*

32) *No se ha podido verificar que se aplican medidas suficientes para la protección de las copias de seguridad. (apartado V.8.3)*

33) *No se ha podido verificar la existencia del proceso para la realización de copias de seguridad, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.8.4)*

Alegación realizada

(30, 31, 32 y 33) Se realizan copias de seguridad en el interior de las instalaciones municipales, en los servidores físicos y se esa copia de seguridad también sale hacia servidores, a un centro de datos que cuenta con todas las medidas de seguridad y protección. Además, periódicamente se revisan que las copias de validez son válidas y pueden ser restauradas en caso de ser necesario. El sistema a de copias de seguridad está pasando a servidores virtuales en estos momentos.

Contestación a la alegación

En las pruebas complementarias que se realizan en la fase de alegaciones, se verifican aquellos aspectos que no se pudieron comprobar en su momento, y siempre teniendo en cuenta que ha habido un cambio tecnológico posterior a la emisión del Informe, se realizan los cambios necesarios en el memorándum detallado.

Adicionalmente, se modifican las conclusiones del Informe en el sentido ya detallado en la respuesta a la alegación primera.

IX. ALEGACIÓN NOVENA

Párrafos de referencia Conclusiones apartado III.9.

III.9. CUMPLIMIENTO NORMATIVO

34) El Ayuntamiento de Santa Marta de Tormes no aporta documentación que permita verificar que cumple con ninguno de los aspectos del ENS y de la normativa en materia de protección de datos personales revisados, con excepción del nombramiento del DPD. (Apartados V.9.1 y V.9.2)

35) No se ha podido verificar el cumplimiento de lo establecido en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas al no realizar la auditoría de sistemas anual del Registro Contable de Facturas. (Apartado V.9.3)

Alegación realizada

(34) Efectivamente el Ayuntamiento no está siguiendo las recomendaciones de ENS aunque ya se están dando los pasos para que todas las pautas y normativa está establecida y presente en un nuevo contrato para el año 2022.

(35) El consistorio tiene adjudicado, tal como exige la ley, el servicio de protección de datos del que hay nombrado a delegado. Igualmente el Ayuntamiento cuenta con un Registro Contable de Facturas.

En conclusión:

1. El Ayuntamiento muestra toda su disposición para colaborar tanto en este como en cualquier otro procedimiento.

2. Que en la actualidad se está trabajando para sacar a licitación pública el contrato de Mantenimiento de Sistemas Informáticos.

3. El Ayuntamiento está realizando el cambio de la red física a una red virtual que conseguirá una mayor seguridad ya que los elementos dejarán de ser físicos y estarán en un entorno más seguro.

4. El Ayuntamiento nunca ha recibido recomendaciones expresas, ni formación, ni plazos de adaptación para cumplir con las diferentes normativas regionales, nacionales ni europeas.

5. A pesar de los continuos ataques que se reciben en las ip´s diariamente el Ayuntamiento no ha tenido en los últimos 5 años ningún problema de vulneración de datos ni seguridad.

Contestación a la alegación

Lo indicado sobre la conclusión 34) refuerza el contenido del Informe.

Sobre lo alegado a la conclusión 35), con relación al nombramiento del DPD, debe señalarse que la conclusión 34) ya recoge este hecho y ha sido valorado para el cálculo del nivel de madurez del control.

Sobre la realización de la auditoría de sistemas anual exigida en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas, el Ayuntamiento ha aportado el informe correspondiente en la fase de alegaciones, hecho que se refleja en el memorándum detallado y se procede a valorar para obtener el nivel de madurez alcanzado en este control.

Se realizan las siguientes modificaciones:

- **En la página 28, conclusión 35), donde dice "*No se ha podido verificar el cumplimiento de lo establecido en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas al no realizar la auditoría de sistemas anual del Registro Contable de Facturas",* debe decir *"El Ayuntamiento cumple con lo establecido en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas, al realizar la preceptiva auditoría anual de sistemas del Registro Contable de Facturas".***

- **En la página 28, conclusión 36), donde dice "*El resultado de la evaluación del control es un nivel de madurez L0, que implica la "existencia de incumplimientos generalizados de la normativa y la carencia de actuaciones en marcha o con una planificación firme dirigidas a corregir la situación",* debe decir, "*El resultado de la evaluación del control es un nivel de madurez L2, que implica que aunque existen incumplimientos significativos en aspectos relativos al ENS y, en menor medida, la LOPDGDD, se alcanza el objetivo en lo relativo al registro contable de facturas."***