CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SALAMANCA

TRATAMIENTO DE ALEGACIONES

PLAN ANUAL DE FISCALIZACIONES 2022

ÍNDICE

ALEGACIONES PRESENTADAS AL INFORME PROVISIONAL DEL "ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SALAMANCA"

ACLARACIONES

El Ayuntamiento de Salamanca ha presentado con fecha 5 de octubre de 2023, alegaciones al Informe de referencia, dentro del plazo para su presentación.

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

El apartado V al que hace referencia forma parte de los papeles de trabajo.

Entre las alegaciones se incluyen determinados aspectos con detalles propios de los papeles de trabajo, a los que se les ha dado el tratamiento que contempla el Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

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. EXPOSICIÓN PRELIMINAR

El presente documento recoge las alegaciones planteadas por el Ayuntamiento de Salamanca, como respuesta al Informe provisional para alegaciones, emitido por el Consejo de Cuentas de Castilla y León, sobre el "*Análisis de la seguridad informática del Ayuntamiento de Salamanca, ejercicio 2022"*, recibido por registro de entrada de fecha 22 de septiembre de 2023 (nº 2023054923). Dicha fiscalización está incluida en el Plan Anual de Fiscalizaciones para el ejercicio 2022, el cual fue aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León el 13 de junio de 2022 (BOCyL n.º 123, de 28 de junio de 2022).

El Ayuntamiento de Salamanca, con carácter general, es conforme con dicho informe provisional y quiere destacar la precisión y el rigor con el que se han llevado a cabo los trabajos de auditoría, así como el alto nivel de competencia y profesionalidad que han demostrado los auditores para plasmar una visión clara de la situación actual de la seguridad informática del Ayuntamiento. Las alegaciones abordadas a continuación, tratan de matizar o aclarar algunas cuestiones técnicas en apartados muy concretos del informe provisional, que son citados en el presente documento en cursiva.

Contestación

No se trata propiamente de una alegación, sino que se trata de una exposición preliminar realizada por parte del Ayuntamiento de Salamanca al Informe provisional.

El Consejo valora las mejoras que el Ayuntamiento lleva realizando y ha puesto en marcha en lo que se refiere a la ciberseguridad durante este tiempo y que deben tener su continuidad en el tiempo. Por otro lado, tal y como se señaló en el apartado *II.3 "Limitaciones y Deber de colaboración"* y se vuelve a remarcar en este momento, ha existido siempre una gran profesionalidad, disponibilidad y colaboración del personal encargado de las funciones de TI de la entidad.

II. ALEGACIÓN PRIMERA

Párrafo alegado

Apartado "ENTORNO TECNOLÓGICO Y SISTEMAS DE INFORMACIÓN OBJETO DE LA FISCALIZACIÓN". Conclusión 20

Alegación 1

En el Apartado III.4. PROCESO CONTINUO DE IDENTIFICACIÓN Y CORRECCIÓN DE VULNERABILIDADES (CBCS 3 punto 20) figura lo siguiente:

"Sin embargo, una vez recibida la alerta, las acciones concretas para su priorización y resolución están atribuidas al Departamento de Tecnologías de Información y Comunicaciones. Se ha verificado que estas actuaciones se realizan, pero no se cuenta con un procedimiento formalizado. Se concluye que el proceso depende de la actitud proactiva y profesionalidad de los técnicos del Ayuntamiento, que además tienen como condicionantes de su actuación […]"

El Ayuntamiento de Salamanca dispone de los Procedimientos de Gestión de Incidentes de Ciberseguridad y Gestión de Incidentes Críticos de Ciberseguridad incorporados en la documentación aportada dentro del apartado 5.8, documentos 3 y 4.

En el citado apartado III.4 se menciona también lo siguiente:

"La necesidad de establecer cauces formales de coordinación con terceros para que las responsabilidades a la hora de solucionar las vulnerabilidades detectadas queden bien establecidas. (Apartados V.4.2 y V.4.3) […]

En el Anexo II del Protocolo Gestión de Incidentes Críticos de Ciberseguridad figuran los Acuerdos de Nivel de Servicio (ANS) que tiene el Ayuntamiento con las empresas colaboradoras de apoyo a la resolución de incidencias técnicas:

- Datos de contacto.
- Parámetros de calidad.
- Protocolo.
- Escalado de incidencias.

En el protocolo antes mencionado se establece, en función de la categoría de la incidencia, la empresa colaboradora que debería actuar en caso de necesidad.

Contestación a la alegación

La conclusión hace referencia al proceso continuo de identificación y resolución de vulnerabilidades, entendiendo como vulnerabilidades tanto aquellas

que se detectan de manera reactiva, como consecuencia de un incidente, como aquellas que se detectan de manera proactiva.

El protocolo al que se refiere la alegación hace referencia exclusivamente a la resolución de incidentes críticos, y por tanto a las vulnerabilidades asociadas al incidente. No se refiere a aquellas que se detectan de manera proactiva y para cuya resolución únicamente se indica en el protocolo de resolución de incidentes de seguridad que: "El DTIC recibirá periódicamente boletines con posibles vulnerabilidades provenientes de la división de ciber inteligencia del SOC o de las sondas Nessus instaladas en los servidores del ayuntamiento. Estos boletines contribuyen a reforzar la infraestructura tecnológica del ayuntamiento proporcionando información que debe ser analizada por el DTIC para determinar el riesgo y las acciones de mitigación a realizar."

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

III. ALEGACIÓN SEGUNDA

Alegación realizada

En el apartado V.1.2. SISTEMAS DE INFORMACIÓN figura lo siguiente:

"Para delimitar el alcance de la presente revisión, se tendrá en cuenta que el Ayuntamiento ya ha realizado una categorización de sus sistemas de información, definidos de manera amplia como "Los sistemas de información propiedad del Ayuntamiento de Salamanca, que dan soporte a los servicios de Administración Electrónica", de tal manera que incluye los siguientes servicios e informaciones como esenciales: […]"

Se considera que, en lugar de los servicios de Administración Electrónica, debería decir los servicios que presta el Ayuntamiento de Salamanca.

En el citado apartado V.1.2, dentro del Cuadro 6 Elementos transversales, figura lo siguiente:

"Teletrabajo Terminador de túneles […] basado en tecnología […]"

Esta información no es acorde con lo que figura en el apartado V.1.3.3 del informe provisional de auditoría. Se desea aclarar que el Ayuntamiento tiene contratada una solución tecnológica que proporciona de manera íntegra el túnel para el acceso remoto. Adicionalmente, para aumentar la seguridad del tráfico procedente del túnel del proveedor del acceso remoto, se incorpora una capa adicional de seguridad mediante dos cortafuegos en el acceso a la infraestructura municipal.

Contestación

El apartado V al que hace referencia forma parte de los papeles de trabajo.

Con respecto a la definición del ámbito de aplicación del ENS se transcribe literalmente lo indicado respecto al alcance en el "Informe Diagnóstico en relación con el grado de adecuación a la normativa del ENS Nivel MEDIO" realizado en noviembre de 2022 por el Ayuntamiento.

Lo anterior no es contradictorio con las modificaciones a este alcance que el Ayuntamiento considere necesarias en futuras actuaciones de mejora de la ciberseguridad o más en concreto, de adaptación a la normativa del ENS.

En ambos casos, al estar las precisiones realizadas contenidas en detalles propios de los papeles de trabajo, han sido tratadas según el procedimiento que contempla el Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

IV. ALEGACIÓN SEGUNDA (BIS)

Párrafo alegado

Apartado IV RECOMENDACIONES.

Alegación realizada

En diversos puntos del apartado IV de "RECOMENDACIONES" se hace alusión al Alcalde como responsable y autoridad en los temas objeto de esta auditoría, por decreto de alcaldía de fecha 20 de junio de 2023, delegó las competencias en materia de Régimen Interior, de quien depende orgánicamente el Departamento TIC y por ende los aspectos en materia de ciberseguridad, al Cuarto Teniente de Alcalde.

Se sugiere que se tengan en cuenta estos términos en el informe de Auditoría

Contestación a la alegación

Dado que las delegaciones de competencias se realizan por decreto de Alcaldía y están sujetas por tanto a cambios discrecionales, se considera más adecuado hacer referencia al responsable final con respecto a la seguridad de la información del Ayuntamiento que es, justamente su máximo representante, es decir, el Alcalde.

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

V. ALEGACIÓN TERCERA

Alegación realizada

En el apartado V.1.3.1. Acceso a internet figura lo siguiente:

"El Ayuntamiento de Salamanca mantiene una Red de Datos corporativa que conecta las sedes municipales a través de diferentes tipos de conexiones:

• Conexiones de fibra propia del Ayuntamiento.

• Conexiones a través de red privada virtual proporcionada por el operador.

• Conexiones a través de una VPN propia del Ayuntamiento establecida a través de los equipos de seguridad perimetral soportándose la conexión en la sede concreta mediante una línea ADSL/FTTH. Esta funcionalidad es mantenida por técnicos municipales con el soporte del contrato de seguridad perimetral. […]"

Respecto al último punto, el Ayuntamiento de Salamanca no dispone de conexiones a través de VPN propia, sino de entradas controladas a través de un portal cautivo soportado por los cortafuegos perimetrales, disponibles para empresas de soporte y funcionarios aislados en otras administraciones.

Contestación a la alegación

El apartado V al que hace referencia forma parte de los papeles de trabajo.

Al estar las precisiones realizadas contenidas en detalles propios de los papeles de trabajo, han sido tratadas según el procedimiento que contempla el Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

VI. ALEGACIÓN CUARTA

Alegación realizada

En el apartado V.1.3.3. Teletrabajo figura lo siguiente:

"El Ayuntamiento de Salamanca dispone de una solución de teletrabajo que consiste […]. Se emplea doble factor de autenticación […], pero no se ejecuta ningún tipo de aplicación del tipo […] que permita revisar la configuración del equipo que accede.[…]"

Se desea aclarar que el servicio contratado por el Ayuntamiento para el acceso remoto proporciona un acceso mediante portal cautivo a las máquinas internas de la organización. En ningún momento la máquina origen desde la que se inicia la conexión se integra en la red corporativa interna. Por este motivo, no se ha considerado necesaria la ejecución de ninguna aplicación que establezca requisitos adicionales de seguridad para la conexión, más que la entrada al portal mediante doble factor de autenticación. La seguridad del servicio está garantizada y certificada por el proveedor del servicio.

Contestación a la alegación

El apartado V al que hace referencia forma parte de los papeles de trabajo.

Al estar las precisiones realizadas contenidas en detalles propios de los papeles de trabajo, han sido tratadas según el procedimiento que contempla el

Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

VII. ALEGACIÓN QUINTA

Alegación realizada

En el apartado V.4.3. RESOLUCIÓN DE VULNERABILIDADES (CBCS-3.3) figura lo siguiente:

"Se han revisado algunas de las vulnerabilidades descritas en los informes del SOC y el Ayuntamiento aporta evidencias de las acciones tomadas para su resolución, que si bien son efectivas dado que las vulnerabilidades por las que se preguntan están resueltas, dependen en buena medida de la actitud proactiva de los técnicos del DTIC al no existir una asignación formal de roles y responsabilidades que permitan garantizar que las actuaciones se hacen en tiempo oportuno y que queda constancia de su realización. […]"

Se reitera lo incluido en la alegación primera haciendo mención especial al apartado 5 ROLES EN LA GESTION DE CIBERSEGURIDAD del Procedimiento de Gestión de Incidentes de Ciberseguridad aportado en el apartado 5.8 de la documentación".

Contestación a la alegación

El apartado V al que hace referencia forma parte de los papeles de trabajo.

De igual forma que en la alegación primera, el protocolo al que hace referencia esta alegación es muy detallado en lo que se refiere a la gestión de incidentes y por tanto a la resolución de vulnerabilidades relacionadas con estos incidentes, pero trata la resolución de vulnerabilidades detectadas de manera proactiva con menor detalle.

No obstante, sí que se indican, tal y como refiere el Ayuntamiento, una asignación de roles y responsabilidades a esta tarea.

Al estar las precisiones realizadas contenidas en detalles propios de los papeles de trabajo, han sido tratadas según el procedimiento que contempla el Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

VIII. ERRATA

Se solicita que se subsane una errata en las páginas 99 a 101 donde debería aparecer Ayuntamiento de Salamanca.

Contestación a la alegación

El apartado V al que hace referencia forma parte de los papeles de trabajo.

Al estar las precisiones realizadas contenidas en detalles propios de los papeles de trabajo, han sido tratadas según el procedimiento que contempla el Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

IX. CONCLUSIONES

El Ayuntamiento quiere agradecer al Consejo de Cuentas el esfuerzo, cooperación y cordialidad durante todo el proceso de auditoría y reconoce la importancia de los resultados de la misma para continuar el proceso de adecuación y mejora en la seguridad informática que lleva acometiéndose desde hace varios años.

Por último, cabe mencionar que el Ayuntamiento de Salamanca sigue trabajando con la finalidad de aportar los recursos organizativos, humanos y materiales necesarios para realizar avances en materia de seguridad informática y ratificar su compromiso con la misma.

En esta dirección se han finalizado los dos procesos selectivos para incorporar personal en el Departamento TIC de acuerdo con las ofertas de empleo. Por otro lado, estos procesos han permitido generar las correspondientes bolsas de empleo para la cobertura de necesidades urgentes, especialmente aquellas señaladas en el informe de auditoría. En el caso de que alguno de los contenidos incluidos en las alegaciones formuladas debiera ser acreditado, existe completa disponibilidad para aportar la información correspondiente.

Contestación a la alegación

No se trata propiamente de una alegación, sino que se trata de una conclusión final realizada por parte del Ayuntamiento de Salamanca al Informe provisional.

El Consejo valora las mejoras que el Ayuntamiento lleva realizando y ha puesto en marcha en lo que se refiere a la ciberseguridad durante este tiempo y que deben tener su continuidad en el tiempo. Por otro lado, tal y como se señaló en el apartado *II.3 "Limitaciones y Deber de colaboración"* y se vuelve a remarcar en este momento, ha existido siempre una gran profesionalidad, disponibilidad y colaboración del personal encargado de las funciones de TI de la entidad.