CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SEGOVIA

TRATAMIENTO DE ALEGACIONES

PLAN ANUAL DE FISCALIZACIONES 2024

ÍNDICE

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

I. EXPOSICIÓN PRELIMINAR 3
II. ALEGACIÓN PRIMERA 3
III. ALEGACIÓN SEGUNDA 4
IV. ALEGACIÓN TERCERA 5
V. ALEGACIÓN CUARTA 6
VI. ALEGACIÓN QUINTA 8

ACLARACIONES

El Ayuntamiento de Segovia ha presentado alegaciones al Informe provisional dentro del plazo para su presentación.

Entre las alegaciones se incluyen determinados aspectos con detalles propios de los papeles de trabajo, que no se han considerado alegaciones, sino que se les ha dado el tratamiento que contempla el Art. 26.5 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas.

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. EXPOSICIÓN PRELIMINAR

El presente informe recoge las alegaciones planteadas por el Ayuntamiento de Segovia al informe provisional emitido por el Consejo de Cuentas de Castilla y León, en el marco de la fiscalización que está llevando a cabo sobre el "Análisis de la seguridad informática del Ayuntamiento de Segovia", incluida dentro del Plan Anual de Fiscalizaciones para el ejercicio 2024, aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León del día 12 de febrero de 2024 (BOCyL n.º 44, de 1 de marzo de 2024).

II. ALEGACIÓN PRIMERA

Párrafo alegado

Apartado "*ENTORNO TECNOLÓGICO Y SISTEMAS DE INFORMACIÓN OBJETO DE LA FISCALIZACIÓN*"

- *Alegación relativa al punto 1 del apartado de conclusiones (página 21).*

"*La concejalía de Turismo; Innovación y Digitalización; Promoción Económica realiza todas las acciones necesarias para una dirección efectiva de la política de seguridad informática. No obstante, presenta carencias muy importantes en el ámbito de una adecuada relación de puestos de trabajo, del impulso de la cobertura de plazas y del nombramiento de los principales responsables de la gestión y seguridad informática."*

Alegación realizada

No consideramos que existan importantes carencias en el nombramiento de los principales responsables de la gestión y seguridad informática, según indicamos en el anexo

Contestación a la alegación

Si bien es cierto que los nombramientos efectuados en la Política de Seguridad de la entidad son correctos, es importante señalar que no consta que se ha efectuado el nombramiento del responsable de sistemas de manera inequívoca, lo cual evitaría cualquier ambigüedad. Por otro lado, es fundamental la participación tanto del responsable de sistemas como del de seguridad en la Comisión Técnica de Administración Electrónica (CTAE) y esta debe efectuarse como vocales y no como asesores o personal técnico.

En todo caso, se acepta la alegación a los efectos de mejorar el contenido del Informe, y se modifica el texto referente a la conclusión 1) en la página 21.

Donde dice:

1) "La concejalía de Turismo; Innovación y Digitalización; Promoción Económica realiza todas las acciones necesarias para una dirección efectiva de la

política de seguridad informática. No obstante, presenta carencias muy importantes en el ámbito de una adecuada relación de puestos de trabajo, del impulso de la cobertura de plazas y del nombramiento de los principales responsables de la gestión y seguridad informática."

Debe decir:

1) "La concejalía de Turismo; Innovación y Digitalización; Promoción Económica realiza todas las acciones necesarias para una dirección efectiva de la política de seguridad informática. No obstante, presenta carencias muy importantes en el ámbito de una adecuada relación de puestos de trabajo e impulso de la cobertura de plazas."

III. ALEGACIÓN SEGUNDA

Párrafo alegado

Apartado "*ENTORNO TECNOLÓGICO Y SISTEMAS DE INFORMACIÓN OBJETO DE LA FISCALIZACIÓN*"

- *Alegación relativa al punto 2 del apartado de conclusiones (página 21).*

"*Diversos cometidos relacionados con las Tecnologías de la Información se acumulan en pocas personas, incumpliendo la necesaria segregación de funciones derivada del principio de seguridad como función diferenciada."*

Alegación realizada

Consideramos que no es correcta la expresión "incumpliendo la necesaria segregación de funciones …', según indicamos en el anexo

Contestación a la alegación

Como se ha mencionado anteriormente, es necesario valorar y tener en cuenta los aspectos previamente referenciados en la alegación primera. Si bien esos puntos señalados, no suponen un incumplimiento de la necesaria segregación de funciones, tal y como se indica en la alegación.

Por ello, se acepta la alegación, y se modifica el texto referente a la conclusión 2) en la página 21.

Donde dice:

2) "Diversos cometidos relacionados con las TI se acumulan en pocas personas, incumpliendo la necesaria segregación de funciones derivada del principio de seguridad como función diferenciada."

Debe decir:

2) "Diversos cometidos relacionados con las TI se acumulan en pocas personas. Asimismo, si bien la definición de los roles en la política de seguridad es correcta, no consta el nombramiento inequívoco del responsable del sistema. Por otro lado, la participación tanto del responsable de sistemas como del de seguridad en la Comisión Técnica de Administración Electrónica (CTAE) no se efectúa como vocales de la misma tal y como se referencia en la política de seguridad, sino como asesores o personal técnico."

IV. ALEGACIÓN TERCERA

Párrafo alegado

Apartado "*INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS (CBCS 1)*"

- *Alegación relativa al punto 10 del apartado de conclusiones (página 22).*

"La información del inventario de hardware se encuentra dispersa ya que cuenta con varias herramientas que pueden utilizarse a estos efectos en determinadas categorías de activos."

Alegación realizada

La expresión '…ya que cuenta con varias herramientas …' puede interpretarse de manera errónea, realmente sólo se utiliza una herramienta de inventario (GLPI) y dos métodos de actualización (reconocimiento automático y carga manual), tal como se explica en el anexo.

Contestación a la alegación

La conclusión precisamente hace referencia a lo trasladado en la alegación: la utilización de dos métodos o sistemas para la actualización del inventario. Por un lado, se menciona el reconocimiento automático, y por otro, la carga manual realizada por el técnico informático correspondiente. La combinación de ambos métodos, que convergen en la herramienta de inventario GLPI, es la causa de que el inventario no sea robusto.

En todo caso se acepta la alegación a los efectos de mejorar el contenido del Informe, y se realiza la siguiente precisión.

Donde dice:

10) "La información del inventario de hardware se encuentra dispersa ya que cuenta con varias herramientas que pueden utilizarse a estos efectos en determinadas categorías de activos. No es posible establecer una relación inmediata entre ambas herramientas porque no están adecuadamente actualizadas ni tampoco se encuentran

sincronizadas entre ellas. Esto implica una disminución de la fiabilidad. Todo ello resta utilidad a ese inventario."

Debe decir:

10) "La información del inventario de hardware se encuentra dispersa ya que cuenta con dos métodos de gestión de la información de inventario, que pueden utilizarse a estos efectos en determinadas categorías de activos. No es posible establecer una relación inmediata entre ambos métodos de gestión porque no están adecuadamente actualizados ni tampoco se encuentran sincronizados. Esto implica una disminución de la fiabilidad. Todo ello resta utilidad a ese inventario."

V. ALEGACIÓN CUARTA

Párrafo alegado

Apartado *"USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS (CBCS 4)*"

- *Alegación relativa al punto 27 del apartado de conclusiones (página 25).*

"*No se utilizan identificadores diferentes para poder acceder como usuario o administrador en función de las tareas que se quieran realizar. Por tanto, no se produce la elevación de permisos si se tienen que realizar tareas concretas para luego volver al perfil de usuario, lo cual supone un riesgo de seguridad importante."*

Alegación realizada

Sí utilizamos identificadores diferentes para poder acceder como usuario o administrador, según se indica en el anexo.

Contestación a la alegación

Si bien la entidad manifestó que no hacía elevación de permisos durante el trabajo de campo, se ha constatado lo expuesto por la entidad en lo referente a la utilización de identificadores diferentes, en el apartado de "Administradores" de directorio activo y, por tanto, se acepta la alegación modificando la conclusión 27).

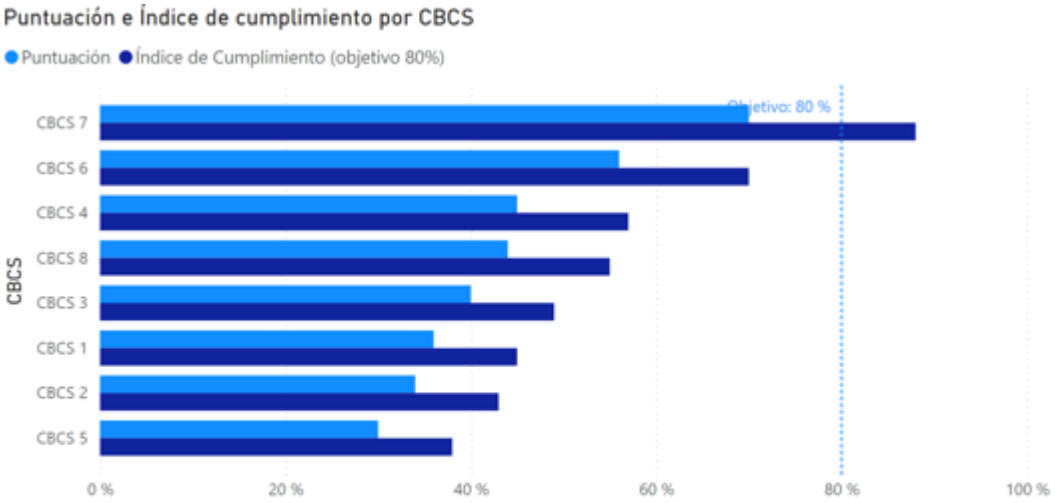
Donde dice:

27) "No se utilizan identificadores diferentes para poder acceder como usuario o administrador en función de las tareas que se quieran realizar. Por tanto, no se produce la elevación de permisos si se tienen que realizar tareas concretas para luego volver al perfil de usuario, lo cual supone un riesgo de seguridad importante."

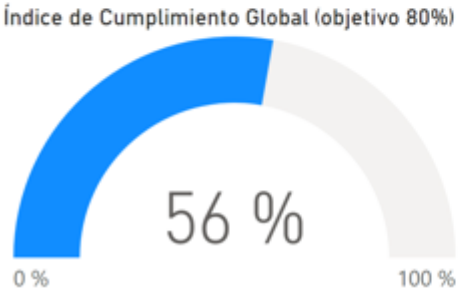
Debe decir:

27) "Se utilizan identificadores diferentes para poder acceder como usuario o administrador en función de las tareas que quiera realizar. Así se pueden elevar los permisos si tiene que realizar tareas concretas para luego volver al perfil de usuario.

Asimismo, dicha corrección influye en la valoración de uno de los subcontroles, lo cual influye en la valoración total del control CBCS 4 y, por ende, en el apartado de "*Situación Global de los Controles Básicos de Ciberseguridad*". Se han llevado a cabo las modificaciones oportunas en las valoraciones anteriormente mencionadas, quedando el gráfico 1 "Puntuación e Índice de cumplimiento por CBCS" del siguiente modo:



CBCS	Descripción	Puntuación	Índice de Cumplimiento (objetivo 80%)
CBCS 1	Inventario y control de dispositivos físicos	36 %	45 %
CBCS 2	Inventario y control de software autorizado y no autorizado	34 %	43 %
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	40 %	49 %
CBCS 4	Uso controlado de privilegios administrativos	45 %	57 %
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	30 %	38 %
CBCS 6	Registro de la actividad de los usuarios	56 %	70 %
CBCS 7	Copias de seguridad de datos y sistemas	70 %	88 %
CBCS 8	Cumplimiento normativo	44 %	55 %
Total			**56 %**



El nivel de madurez alcanzado globalmente por la entidad corresponde al nivel **L2.**

El índice de cumplimiento (sobre un objetivo de madurez L3 que corresponde a una puntuación del 80%) es del **56%**.

VI. ALEGACIÓN QUINTA

Párrafo alegado

Apartado *"CUMPLIMIENTO NORMATIVO" (CBCS 8)*

- *Alegación relativa al punto 48 del apartado de conclusiones (página 28).*

"De acuerdo con las conclusiones de esta área, el resultado de la evaluación del control es un nivel de madurez L1, que implica la existencia de incumplimientos de la normativa."

Alegación realizada

La evaluación del control se lleva a cabo teniendo en cuenta tres subcontroles, de los que sólo uno de ellos presenta incumplimiento. Aunque el control conjunto se evalúe con nivel L1, creemos que habría que diferenciar en las conclusiones el grado de cumplimiento de cada subcontrol. Ver anexo.

Contestación a la alegación

La evaluación del control mencionado referente al cumplimiento de la legalidad, publicado en la GPF-OCEX 5313 "Revisión de los controles básicos de ciberseguridad", incluye la verificación del cumplimiento de diversas normas relacionadas con la seguridad de la información:

- **Cumplimiento del ENS**
- **Cumplimiento de la LOPD/RGPD**
- **Cumplimiento de la Ley 25/2013, de 27 de diciembre (Impulso de la factura electrónica y creación del registro contable de facturas)**

Los resultados de la fiscalización, de acuerdo con lo previsto en el apartado 7 de la GPF-OCEX 5313, "Evaluación de los hallazgos de auditoría", han sido ponderados siguiendo los criterios establecidos en el apartado 8, "Evaluación de las deficiencias de control interno detectadas" de la GPF-OCEX 5330, tal y como se referencia en el informe.

Por tanto, la evaluación del CBCS debe efectuarse del mismo modo que el resto de los CBCS, estableciendo la evaluación en su conjunto.

Asimismo, en el anexo se indica una actuación por parte del Interventor que pretende justificar la actuación del ente fiscalizado, pero que en todo caso ratifica el contenido del Informe.

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