SEGOVIA

Nota del Consejo de Cuentas:
Documento editado por protección de datos personales.

CONSEJO DE CUENTAS DE CASTILLA Y LEON
CALLE MAYOR, 54
34001- PALENCIA- PALENCIA

Documento	Comunicación Alcaldía	PG1.000.43_NOT
Expediente	1/2025/P18001 - P18.001 - Tecnología Tramitación General	
Asunto	Alegaciones al informe de auditoría del Consejo de Cuentas de Castilla y León sobre seguridad informática del Ayuntamiento	
Interesado		

FIRMAS

Autoridad / Cargo, identificación firmante y fecha firma
EL ALCALDE José Mazarías Pérez 13/03/2025
Documento firmado electrónicamente con código de identificación único XXXXXX6415556010XXX Autenticidad verificable en https://sede.segovia.es/validacion

Con fecha 28/02/2025 se ha recibido en este Ayuntamiento notificación efectuada por el Consejo de Cuentas de Castilla y León, a través del servicio de Dirección Electrónica Habilitada Única (DEHÚ), con el informe provisional para alegaciones al ANALISIS DE LA SEGURIDAD INFORMATICA DEL AYUNTAMIENTO DE SEGOVIA, otorgándose un plazo de 15 días naturales para formular ALEGACIONES, es por ello que tras el análisis y estudio de lo contenido en el referido informe, se procede dentro del plazo conferido a efectuar las alegaciones que a continuación se indican:

Nº	Texto del informe sobre el que se alega		Alegación realizada
	Apartado	Párrafo	
1	III. Conclusiones III.1. Entorno tecnológico …	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. (Apartado V.1.1)	No consideramos que existan importantes carencias en el nombramiento de los principales responsables de la gestión y seguridad informática, según indicamos en el anexo
2	III. Conclusiones	2) Diversos cometidos relacionados con las Tecnologías de la Información se acumulan en	Consideramos que no es correcta la expresión 'incumpliendo la necesaria

Plaza Mayor 1, 40001 Segovia. Tel. 921 419800. Fax: 921 419840
www.segovia.es

	III.1. Entorno tecnológico …	pocas personas, incumpliendo la necesaria segregación de funciones derivada del principio de seguridad como función diferenciada. (Apartado V.1.1)	segregación de funciones …', según indicamos en el anexo
3	III. Conclusiones III.2. Inventario y control de dispositivos …	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.	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
4	III. Conclusiones III.5. Uso controlado de privilegios …	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. (Apartado V.5.3)	Sí utilizamos identificadores diferentes para poder acceder como usuario o administrador, según se indica en el anexo
5	III. Conclusiones III.9. Cumplimiento normativo	48) 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. (Apartado V.9.4)	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

En las alegaciones realizadas, se hace referencia a un anexo donde se dan explicaciones complementarias. Este anexo se presenta en documento aparte.

Plaza Mayor 1, 40001 Segovia. Tel . 921 419800. Fax: 921 419840
www.segovia.es

Nota del Consejo de Cuentas:
Documento editado por protección de datos personales.

CONSEJO DE CUENTAS DE CASTILLA Y LEON
CALLE MAYOR, 54
34001- PALENCIA- PALENCIA

Documento	Comunicación Alcaldía PG1.000.43_NOT
Expediente	1/2025/P18001 - P18.001 - Tecnología Tramitación General
Asunto	Anexo al documento de alegaciones al informe de auditoría del Consejo de Cuentas de Castilla y León sobre seguridad informática del Ayuntamiento
Interesado	

FIRMAS

Autoridad / Cargo, identificación firmante y fecha firma

EL ALCALDE
José Mazarías Pérez
13/03/2025

Documento firmado electrónicamente con código de identificación único xxxxxx6407443731xxxx
Autenticidad verificable en https://sede.segovia.es/validacion

Anexo al documento de alegaciones al informe de auditoría del Consejo de Cuentas de Castilla y León sobre seguridad informática del Ayuntamiento de Segovia

ALEGACIÓN Nº 1

No consideramos que existan importantes carencias en el nombramiento de los principales responsables de la gestión y seguridad informática, dado que dicho nombramiento está formalizado en el documento de Política de Seguridad del Ayuntamiento, en su apartado '6.1. Roles o perfiles de seguridad':

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado de Protección de Datos (DPD): el así designado por el Ayuntamiento de Segovia.

Plaza Mayor 1, 40001 Segovia. Tel. 921 419800. Fax: 921 419840
www.segovia.es

- Responsable General de la Información y de los Servicios: el propio Comité de Seguridad de la Información.

- Responsable Particular de la Información y de los Servicios: los Jefes o máximos responsables de cada una de las Unidades Administrativas y Servicios Municipales del Ayuntamiento de Segovia en las materias que les conciernan.

- Responsable de Seguridad de la Información: el Jefe del Servicio de Informática.

- Responsable del Sistema: El técnico del Servicio de Informática.

El Delegado de Protección de Datos está nombrado mediante Decreto Alcaldía. Ver documento: '2020-06-12 - Decreto 2020-03819 - Nombramiento_delegada_PROTECCION_DE_DATOS.pdf'

ALEGACIÓN Nº 2

Consideramos que no es correcta la expresión 'incumpliendo la necesaria segregación de funciones …', ya que tenemos segregadas las funciones de responsable de seguridad y la de responsable de la explotación en distintas personas, y si bien la segunda tiene una dependencia jerárquica de la primera, nuestro tamaño de organización y la estructura del departamento de TI no permite disponer de estos dos roles con total independencia entre ellos.

Por otro lado, las funciones de responsable de la información y los servicios las tienen personas distintas de los responsables de seguridad y de explotación.

Por ello, creemos que no incumplimos ninguna prohibición específica en cuanto a segregación de funciones en este ámbito, y si bien sería recomendable una mayor independencia de roles, siguiendo el espíritu de la norma, con nuestro tamaño de organización y recursos humanos disponibles entendemos que es razonable nuestra distribución de funciones.

ALEGACIÓN Nº 3

La expresión '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' puede interpretarse de manera errónea.

Realmente sólo contamos con una herramienta de inventario, que es GLPI, que se actualiza mediante dos métodos, reconocimiento automático de equipos mediante OCS y carga

manual. Es decir, utilizamos dos soluciones distintas que se complementan en el proceso de actualización de inventario, pero el inventario como tal sólo se mantiene en GLPI.

Ello con independencia de la situación detectada por el auditor en cuanto a errores de carga y sincronización entre OCS y GLPI.

NOTA: aunque queda fuera del alcance de la auditoría practicada, sólo a efectos informativos, actualmente hemos dejado de utilizar OCS como agente de reconocimiento automático de equipos en la red, y ahora utilizamos el agente propio de GLPI. También hemos eliminado las duplicidades de equipos que se provocaron en su día por los problemas de sincronización con OCS.

ALEGACIÓN Nº 4

Sí que utilizamos identificadores diferentes para poder acceder como usuario o administrador, debe haber habido algún malentendido.

De hecho, esta es una exigencia que ya cumplimos para obtener la certificación ENS.

Por ejemplo, el usuario con el que se identifica el Jefe de Informática en su trabajo habitual es alberto.gomez, con el que no tiene ningún privilegio de administración. Si necesita efectuar algún acceso como administrador tiene que loguearse con un usuario distinto, en este caso alberto.gomez.adm

ALEGACIÓN Nº 5

La evaluación del control de Cumplimiento normativo se lleva a cabo teniendo en cuenta tres subcontroles:

- CBCS 8.1 – relativo al cumplimiento ENS
- CBBS 8.2 – relativo a protección de datos
- CBCS 8.3 – relativo a Registro Contable de Facturas

Sin embargo, sólo el control CBCS 8.3 presenta incumplimiento (0%), cuando los otros dos grados de cumplimiento son del 95% y 70%.

Aunque el control conjunto se evalúe con nivel L1, creemos que habría que diferenciar en las conclusiones el grado de cumplimiento de cada subcontrol, para poner de manifiesto dónde reside el problema de cumplimiento de este control.

Por otro lado, en el Ayuntamiento de Segovia los subcontroles 8.1 y 8.2 corresponde abordarlos a la unidad de Informática, mientras que el control 8.3 corresponde abordarlos a

Plaza Mayor 1, 40001 Segovia. Tel . 921 419800. Fax: 921 419840
www.segovia.es

la Unidad de Intervención, por lo que es importante la diferenciación para abordar su solución futura.

NOTA: en relación al subcontrol CBCS 8.3, a efectos informativos, el Interventor ha pedido que indiquemos en esta alegación que en 2024, con carácter previo a la realización de esta auditoría de seguridad informática, la unidad de Intervención inició un expediente de Contratación que contemplaba la ejecución de la auditoría del registro contable de facturas, contrato que no se ha llegado a formalizar por problema ajenos a la unidad de Intervención.