# ASUNTO: FISCALIZACIÓN DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE VALLADOLID - ALEGACIONES SOBRE EL INFORME PROVISIONAL EMITIDO POR EL CONSEJO DE CUENTAS DE CASTILLA Y LEÓN

El presente informe recoge las alegaciones planteadas por el Ayuntamiento de Valladolid 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 Valladolid, ejercicio 2022", incluida dentro del Plan Anual de Fiscalizaciones para el ejercicio 2022, aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León del día 13 de junio de 2022 (BOCyL n.º 123, de 28 de junio de 2022).

Cabe destacar la conformidad general del Ayuntamiento con el informe provisional en sus distintos epígrafes, al considerar que realiza un análisis riguroso de la ciberseguridad de la organización, así como su agradecimiento al equipo auditor por la profesionalidad y minuciosidad del trabajo realizado. Las alegaciones aquí planteadas tratan de puntualizar ciertos aspectos que se considera que podrían matizarse, o subcontroles cuya valoración podría no corresponder con el nivel de madurez reflejado en el propio trabajo de campo llevado a cabo, con el propósito de que el informe refleje de la forma más fidedigna posible la realidad actual y sirva de base para el proceso de mejora continua que, indiscutiblemente, debe existir en un ámbito como la ciberseguridad.

Las alegaciones se agrupan por apartados y/o controles, para mayor claridad.

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

**Alegación 1**

- *Alegación relativa al punto 1 del apartado de conclusiones (página 22).*

En relación con la primera de las conclusiones del apartado y, en concreto, con la afirmación de que la concejalía de Planificación y Recursos, actual Concejalía de Hacienda, Personal y Modernización administrativa, *no realiza todas las acciones necesarias para una dirección efectiva de la política de seguridad informática, especialmente en el ámbito de impulso de la cobertura de plazas, del nombramiento de los principales responsables de la gestión y seguridad informática (pg. 22 del informe)*, cabe manifestar que, en esta materia, se está ejecutando la RPT aprobada por la Junta de Gobierno Local, órgano competente para la creación y modificación de la relación de puestos de trabajo, por la que actualmente se atribuye las competencias de responsable de seguridad a la delegada de Protección de Datos, tal y como recoge el propio informe en la descripción del puesto.

Por otra parte, no se aporta en el Informe provisional ninguna justificación expresa legal/normativa que exija dicha diferenciación funcional y orgánica, por lo que se puede

entender que estaríamos en su caso en el ámbito de lo recomendable, no en el ámbito de lo exigible jurídicamente.

Asimismo, cabe señalar que, en este contexto de la política de seguridad informática, durante el ejercicio 2022, la Concejalía de Planificación y Recursos adjudicó inversiones vinculadas con el proyecto de gasto "2020/2/9204/10 - Sistemas de Seguridad" por un total de 2.273.884,60 € IVA incluido, de los cuales 481.100,00 € fueron financiados por el Plan de Recuperación, Transformación y Resiliencia.

**Alegación 2**

- *Alegación relativa al punto 8 del apartado de conclusiones (página 23)*

La conclusión 8 del apartado de referencia enfatiza que "La conexión inalámbrica con la que cuenta el Ayuntamiento, en algunas localizaciones, adolece de las medidas de seguridad necesarias para poder gestionar adecuadamente los accesos y su correspondiente trazabilidad".

El Ayuntamiento considera que procedería matizar o bien complementar esta afirmación, dado que no refleja el estado de situación general de la conexión inalámbrica del Ayuntamiento, la cual se sustenta en el uso de un portal cautivo para todo el entorno inalámbrico público, y dado que toda su actividad, con independencia del SSID, queda registrada en una herramienta de de análisis.

El apartado 1 del Anexo I al presente informe profundiza en el detalle y relevancia de las cifras por las que se considera que debería revisarse la redacción de esta conclusión en el informe final, a fin de que refleje fielmente la realidad general del Ayuntamiento.

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

**Alegación 3**

- *Alegación relativa al punto 13 del apartado de conclusiones (página 23)*

- *Puntuación subcontrol CONTROL DE ACTIVOS FÍSICOS NO AUTORIZADOS (CBCS 1.2) – 68% (Control bastante efectivo).*

La conclusión 13 indica, literalmente, que las medidas implantadas para impedir la conexión de dispositivos físicos no autorizados "***no son muy avanzadas**, a pesar de contar con equipamiento de red capaz de soportarlas*".

No se considera correcta dicha evaluación ni utilizar dicho calificativo, y, de hecho, no se corresponde con la explicación adicional sobre el despliegue de una solución NAC (Network Access Control), que restringe el acceso a los dispositivos autorizados en base a reglas

predefinidas. Cabe señalar que, durante la semana en la que se realizó la auditoría de campo, se verificó la efectividad del NAC a raíz de la ejecución de unas pruebas de penetración técnicas incluidas en una auditoría interna.

En base a dicha corrección, el Ayuntamiento solicita modificar la redacción de la conclusión 13 para que refleje la realidad analizada y entiende que, en caso de no haberse valorado debidamente la cuestión relativa al NAC, cabría revisar el nivel de madurez/puntuación asociado al subcontrol CBCS 1.2.

**Apartado INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO Y NO AUTORIZADO (CBCS 2)**

**Alegación 4**

- *Alegación relativa al punto 19 del apartado de conclusiones (página 24)*

En relación con las conclusiones relativas al control CBCS 2.2 "Software soportado por el fabricante" se indica:

> *19) No existe un plan formalizado de mantenimiento de activos software ni de compra o adquisición de licencias, sino que anualmente se realizan adquisiciones y renovaciones según el criterio técnico del personal y sujeto a limitaciones presupuestarias, asumiéndose riesgos asociados a la falta de soporte de software con impacto potencial importante para el funcionamiento de la organización.*

El Ayuntamiento considera que debería matizarse esta redacción, ya que cuenta con contratos de renovación periódica de licencias estables en el tiempo, tal y como se expone en el apartado 2 del Anexo I, y, salvo casos aislados, la existencia de sistema operativos fuera de soporte no se debe a la falta de planificación o a indisponibilidad presupuestaria, como sugiere la conclusión referida, sino al hecho de que dichos servidores alojan aplicaciones críticas para la operativa diaria del Ayuntamiento que resultan incompatibles con sistemas operativos más modernos y su renovación se encuentra en proceso, o bien aún no ha podido iniciarse por parte de los servicios municipales involucrados. En estos casos, adicionalmente, el Servicio VMaaS viene determinando la aplicación de medidas paliativas que minimizan los riesgos derivados de esta situación.

A fin de argumentar este extremo, el apartado 2 del Anexo I al presente informe desglosa los datos aportados en el resultado de la fiscalización con mayor detalle.

**APARTADO PROCESO CONTINUO DE IDENTIFICACIÓN Y CORRECCIÓN DE VULNERABILIDADES (CBCS 3) -**

**Alegación 5**

- *Alegación relativa al punto 24 del apartado de conclusiones (página 25)*

- *Puntuación subcontrol RESOLUCIÓN DE VULNERABILIDADES (CBCS-3.3) – 30% (Control poco efectivo)*

El Ayuntamiento no se muestra conforme con la puntuación otorgada en el subcontrol CBCS 3.3, ya que el procedimiento seguido actualmente, aunque no formalizado en un documento de normativa interna del Ayuntamiento, viene encauzado por una operativa del servicio VMaaS que ya tiene actividades preplanificadas para los escaneos, el reporte, el seguimiento de cada vulnerabilidad, y la supervisión por parte de los responsables. Como es lógico, el criterio de los responsables de los equipos técnicos se tiene en cuenta para la planificación de las acciones de tratamiento (importante por el contexto del sistema y las limitaciones que puedan darse), pero todas ellas se inician en plazos razonables tras el reporte y atienden a una priorización coherente con la criticidad.

Dado que se está gestionando el tratamiento de todas las vulnerabilidades con criticidad no aceptable, mitigándose en corto plazo muchas de ellas y reduciéndose el nivel de riesgo cuantificado por el servicio VMaaS y, en general, se sigue un proceso con pautas regulares, se entiende que la puntuación del subcontrol CBCS 3.3 debería ser equivalente a la de un nivel L2 Repetible y/o "Control bastante efectivo".

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

**Alegación 6**

- *Alegación relativa al punto 28 del apartado de conclusiones (página 26)*

- *Puntuación subcontrol USO DEDICADO DE CUENTAS DE ADMINISTRACIÓN (CBCS 4.3) – 36% (*Control poco efectivo)

Tanto el punto 28 de las conclusiones como el resultado de la fiscalización, expone que se cumple correctamente el subcontrol CBCS 4.3 en tanto en cuanto"Se verifica que se utilizan identificadores diferentes para poder acceder como usuario o administrador en función de las tareas que quiera realizar y se elevan permisos, por tanto, si tiene que realizar tareas concretas para luego volver al perfil de usuario".

Efectivamente, los equipos técnicos del Ayuntamiento disponen de cuentas unipersonales específicas para el desarrollo de funciones de administrador de los sistemas, así como de cuentas personales para el desarrollo del resto de sus actividades diarias. Esto fue verificado durante la visita, tal y como se redacta en el informe, razón por la que no considera ajustada la valoración del subcontrol y se entiende que esta debería ser el equivalente a un nivel L3 "Proceso definido" y/o "control bastante efectivo".

**Alegación 7**

- *Alegación relativa al punto 29 del apartado de conclusiones (página 26)*

- *Puntuación subcontrol MECANISMOS DE AUTENTICACIÓN (CBCS 4.4) – 36% (Control poco efectivo)*

Aunque aún no se han aplicado diferentes configuraciones de política de contraseñas para usuarios normales y usuarios con privilegios de administrador, la parametrización de la política aplicada con carácter general está alineada con los requisitos del ENS, tal y como se detalla en el apartado 3 del Anexo I.

Por tanto, aunque el conjunto de mecanismos de autenticación tiene margen de mejora, se identifica una pauta regular por mantener un nivel de seguridad mínimo y se busca homogeneizar todos los sistemas. En consecuencia, el Ayuntamiento considera que sería más razonable otorgar al subcontrol 4.4 una puntuación equivalente al nivel de madurez L2 Repetible y/o "Control bastante efectivo".

**Apartado CUMPLIMIENTO NORMATIVO (CBCS 8)**

**Alegación 8**

- *Alegación trasladada por la Delegada de Protección de Datos del Ayuntamiento de Valladolid en informe firmado con fecha 18/07/2023, al recaer en una cuestión de su ámbito competencial.*
- *Alegación relativa al punto 44) del apartado de "Conclusiones" (página 29)*

- *Puntuación subcontrol CUMPLIMIENTO DE LA LOPD-GDD (CBCS 8.2)– 33%*

De acuerdo con la escala de evaluación de los subcontroles del control CBCS-8 recogida en la página 19 del informe provisional para alegaciones que nos ocupa, la evaluación que en el punto 44) de la página 29 se efectúa sobre *"El proceso de adaptación a la normativa en materia de protección de datos"* ha de ser, al menos: **"La actividad está a medias"** y no, únicamente iniciado y ello con fundamentado en la evidencia de que existe un *Proyecto de implantación de la normativa de protección de datos para este Ayuntamiento* suscrito el 26 de octubre de 2022 el cual, previo análisis de la situación del grado de cumplimiento de tal normativa en este Ayuntamiento, recoge ocho (8) líneas de actuación-medidas a adoptar con un período temporal previsto que abarca desde noviembre 2022 a marzo 2024, que se está ejecutando.

Entre las ocho (8) líneas de actuación -medidas se incluyen no solo las referidas en el apartado (Registro de Actividades de Tratamiento y Análisis de riesgos y evaluación de impacto), sino también otras, siendo su detalle el siguiente:

| Nº | Línea de actuación | Objetivos | Planificación propuesta | Estado de cumplimiento |
|---|---|---|---|---|
| **1** | **Requisitos para la validez del consentimiento** | Normalizar el modelo para que el otorgamiento del consentimiento, cuando sea la base legitimadora del tratamiento, cumpla los requisitos del RGPD. | Noviembre/2022 | **Cumplido** |
| **2** | **Deber de información previsto en el art. 13 y 14 del RGPD.** | Normalizar el modelo para cumplir el deber de información previsto en el art. 13 y 14 RGPD. | Enero a febrero 2023 | **Cumplido** |
| **3** | **Encargados de tratamiento.** | Dar orientaciones y/o normalizar el modelo del acto jurídico por el que se establecen las condiciones entre el responsable (ayuntamiento) y el encargado de tratamiento (adjudicatario), actualmente recogido en el documento contractual municipal del Cuadro de Características Particulares del Pliego tipo del Contrato de Servicios. | No se especificó plazo | **Cumplido** |
| **4** | **Registro de Actividades de Tratamiento** | Elaborar y aprobar el Registro de Actividades de Tratamiento del | Enero/2023 a Marzo/2024 | En proceso |

| Nº | Línea de actuación | Objetivos | Planificación propuesta | Estado de cumplimiento |
|---|---|---|---|---|
| | | ayuntamiento con el contenido exigido en el art. 30 del RGPD. | | |
| **5** | **Análisis de riesgos y Evaluaciones de Impacto** | Diseñar la metodología para realizar el análisis de riesgos o Evaluación de Impacto de protección de datos con carácter previo al tratamiento de los datos. | Marzo a junio 2023. | En proceso; afectado por la nueva herramienta GESTIONA RGPD de la Agencia Española de Protección de Datos publicada el pasado 14 de junio de 2023. |
| **6** | **Brechas de seguridad** | Diseñar el proceso para documentar y comunicar las brechas de seguridad a la AEPD así como la notificación a los afectados, cuando proceda. | Julio a agosto 2023 | En plazo |
| **7** | **Derechos en protección de datos** | Normalizar el procedimiento para que el ejercicio de los derechos en materia de protección de datos sea real y efectivo, y se resuelva en los plazos legales. | Septiembre a octubre 2023. | |
| **8** | **Concienciación/cultura administrativa** | Redacción de un Manual de Bienvenida al personal municipal con contenido en protección de datos. | Diciembre 2022 | **Cumplido** |

Además, como acción no planificada, se ha emitido Recomendación 3/2023 por la Delegada de Protección de Datos sobre identificación de los interesados en las publicaciones de los actos administrativos y notificaciones por medio de anuncios, fechada el 13 de junio de 2023.

En consecuencia, el grado de cumplimiento de este proyecto permite estimar en el apartado 44) que *el proceso de adaptación a la normativa en materia de protección de datos*, al menos, está en la escala de evaluación **"La actividad está a medias"** al llevarse a cabo acciones en la buena dirección, de lo que deriva que el resultado otorgado al subcontrol CBCS 8.2 tenga que ser superior: tanto el de la puntuación (ahora de un 33%) como el del índice de cumplimiento (ahora en un 41%).

En otro orden de cuestiones, se aclara el sentido de la argumentación recogida de suerte que no es que las fichas de los tratamientos no hayan sido validados adecuadamente por la DPD, lo cual parece dar a entender que el resultado de la validación no es favorable, sino que se encuentran en fase de revisión.

Como evidencias, se adjunta:

1. Para la línea de actuación nº 1: Recomendación 1/2023, de la Delegada de Protección de Datos, sobre la base legitimadora del consentimiento en el tratamiento de datos personales, fechada el 20 de enero de 2023
2. Para la línea de actuación nº 2: Recomendación 2/2023, de la Delegada de Protección de Datos, sobre las mejores prácticas para cumplir el deber de informar en materia de protección de datos personales, fechada el 24 de febrero de 2023.
3. Para la línea de actuación nº 3: Modelo de encargado de tratamiento, versión definitiva.
4. Para la línea de actuación nº 8: Guía Básica sobre protección de datos personales para el personal del Ayuntamiento de Valladolid V.1.0, fechada el 26 de enero de 2023
5. Recomendación 3/2023 de la Delegada de Protección de Datos sobre identificación de los interesados en las publicaciones de los actos administrativos y notificaciones por medio de anuncios, fechada el 13 de junio de 2023.

**Apartado "RECOMENDACIONES"**

**<u>Alegación 9</u>**

- *Alegación relativa al punto 6 del apartado de recomendaciones (página 32).*

En relación con la recomendación 6, sobre el proceso continuo de identificación y corrección de vulnerabilidades, del siguiente tenor literal:

> *"6) El responsable de seguridad que se defina en la política de seguridad debería valorar juntamente con el responsable del sistema,* ***el empleo de herramientas automatizadas para la detección de vulnerabilidades y la realización (o contratación dada lo***

***especializados de los perfiles necesarios) de pruebas de penetración (pentesting)*** *y que simulan ataques reales (Red team).”*

Se considera que esta conclusión no procedería en el escenario actual, o bien debería matizarse en su redacción, dado que, tal y como se constató en el trabajo de campo, el Ayuntamiento de Valladolid ya cuenta con herramientas automatizadas para la detección de vulnerabilidades a través del servicio VMaaS, al que se hacen múltiples referencias dentro del propio informe.

Asimismo, el Ayuntamiento viene realizando, de forma periódica y programada, pruebas de penetración (*pentesting*), tal y como se verificó en el trabajo de campo.

En Valladolid, a la fecha de la firma electrónica.

| | |
|---|---|
| **LA DIRECTORA DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES** | **EL CONCEJAL DELEGADO DEL ÁREA DE HACIENDA, PERSONAL Y MODERNIZACIÓN ADMINISTRATIVA** |
| **Marina Vega Maza** | **Francisco de Paula Blanco Alonso** |

Ayuntamiento de Valladolid

# Resumen de Firmas



Título:Alegaciones informe provisional Consejo de Cuentas

## Firmante 1

Firmado digitalmente por VEGA MAZA MARINA DNI
Fecha miércoles, 19 julio 2023 10:37:13 GMT
Razón He aprobado el documento

## Firmante 2

Firmado digitalmente por BLANCO ALONSO FRANCISCO DE PAULA DNI
Fecha miércoles, 19 julio 2023 11:05:46 GMT
Razón He aprobado el documento