CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

D. ANDRÉS PÉREZ-MONEO AGAPITO, Secretario del Pleno, por Resolución del Presidente del Consejo de Cuentas de Castilla y León de 8 de enero de 2014,

CERTIFICO: Que el Pleno del Consejo de Cuentas de Castilla y León, en sesión celebrada el día 26 de septiembre de 2023, cuya acta está pendiente de aprobación, adoptó el Acuerdo 48/2023, por el que se aprueba el Informe "ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE VALLADOLID, EJERCICIO 2022", correspondiente al Plan Anual de Fiscalizaciones para el ejercicio 2022.

Asimismo, de conformidad con lo previsto en el artículo 28 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas, el Pleno acuerda la remisión del informe a las Cortes de Castilla y León, al Tribunal de Cuentas y a la Junta de Castilla y León. Del mismo modo, acuerda su remisión a la Fiscalía del Tribunal de Cuentas.

Y para que conste, a los efectos oportunos, expido la presente certificación, con el visto bueno del Excmo. Sr. Presidente del Consejo de Cuentas de Castilla y León, en Palencia, a la fecha de la firma electrónica.

Vº Bº
EL PRESIDENTE
(Art. 21.5 de la Ley 2/2002, de 9 de abril)

Mario Amilivia González

CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE VALLADOLID, EJERCICIO 2022

PLAN ANUAL DE FISCALIZACIONES 2022

ÍNDICE

I. INTRODUCCIÓN 5
I.1. INICIATIVA DE LA FISCALIZACIÓN 5
I.2. MARCO NORMATIVO 5
I.2.1. NORMATIVA EUROPEA 5
I.2.2. NORMATIVA ESTATAL 6
I.2.3. NORMATIVA AUTONÓMICA 7
II. OBJETIVOS, ALCANCE Y DEBER DE COLABORACIÓN 8
II.1. OBJETIVOS 8
II.2. ALCANCE 8
II.3. DEBER DE COLABORACIÓN 19
II.4. TRÁMITE DE ALEGACIONES 19
III. CONCLUSIONES 20
III.1. ENTORNO TECNOLÓGICO Y SISTEMAS DE INFORMACIÓN OBJETO DE LA FISCALIZACIÓN 20
III.2. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS (CBCS 1) 21
III.3. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO Y NO AUTORIZADO (CBCS 2) 22
III.4. PROCESO CONTINUO DE IDENTIFICACIÓN Y CORRECCIÓN DE VULNERABILIDADES (CBCS 3) 23
III.5. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS (CBCS 4) 24
III.6. CONFIGURACIONES SEGURAS DEL SOFTWARE Y *HARDWARE* DE DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES (CBCS 5) 25
III.7. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS (CBCS 6) 25
III.8. COPIAS DE SEGURIDAD DE DATOS Y SISTEMAS (CBCS 7) 26
III.9. CUMPLIMIENTO NORMATIVO (CBCS 8) 26
III.10. AVANCES EN LA APLICACIÓN DEL REAL DECRETO 311/2022 27
III.11. SITUACIÓN GLOBAL DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD) 28
IV. RECOMENDACIONES 29
ÍNDICE DE CUADROS 31
ÍNDICE DE GRÁFICOS 32

ANEXO 33

SIGLAS Y ABREVIATURAS

APT	Amenazas avanzadas persistentes, del inglés "*Advanced Persistent Threats"*
Art/s.	Artículo/artículos
BOCyL	Boletín Oficial de Castilla y León
CBCS	Controles básicos de ciberseguridad
CCN	Centro Criptológico Nacional
CCN-STIC	Guías del Centro Criptológico Nacional sobre la seguridad de las tecnologías de la información y las comunicaciones
CIS	Centro para la seguridad de Internet del Inglés "*Center for Internet Security"*
CMM	Modelo de madurez de procesos, del inglés "*Capability Maturity Model*"
DPD	Delegado de protección de datos
EIPD	Evaluación de impacto de protección de datos
ENS	Esquema Nacional de Seguridad
FEMP	Federación Española de Municipios y Provincias
GPF-OCEX	Guía práctica de fiscalización de los órganos de control externo
ISSAI-ES	Normas Internacionales de las Entidades Fiscalizadoras Superiores
OCEX	Órganos de Control Externo Autonómicos
RAT	Registro de actividades de tratamiento
RPT	Relación de puestos de trabajo
SIEM	Sistema de gestión de información y eventos de seguridad, del inglés "*Security Information and Event Management"*
SW/Sw	*Software*
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y de las Comunicaciones

Las siglas correspondientes a la normativa utilizada se encuentran incluidas en el apartado I.2. Marco Jurídico.

NOTA SOBRE ORIGEN DE DATOS

Los cuadros insertados a lo largo del presente Informe, salvo que se especifique otra cosa, se han elaborado a partir de la información facilitada por la entidad fiscalizada.

Los ratios y porcentajes que se recogen en los cuadros y gráficos incluidos en el Informe pueden presentar en algunos casos diferencias entre el total y la suma de los parciales, derivadas de la forma de presentación de los datos. Esto es debido a que los cálculos se han efectuado con todos los decimales, mientras que su presentación se hace en números enteros o con un decimal, lo que implica la realización de redondeos que en determinados casos dan lugar a diferencias.

I. INTRODUCCIÓN

I.1. INICIATIVA DE LA FISCALIZACIÓN

De conformidad con lo preceptuado en el artículo 90 del Estatuto de Autonomía de Castilla y León y en el artículo 1 de la Ley 2/2002, de 9 de abril, Reguladora del Consejo de Cuentas de Castilla y León, corresponde al Consejo la fiscalización externa de la gestión económica, financiera y contable del Sector Público de la Comunidad Autónoma y demás entes públicos de Castilla y León. Concretamente en el artículo 2 de la citada Ley se señala que están sometidas a la fiscalización del Consejo de Cuentas las Entidades Locales del ámbito territorial de la Comunidad Autónoma.

Por su parte, el apartado 2.º del artículo 3 de la misma Ley reconoce la iniciativa fiscalizadora del Consejo por medio de las fiscalizaciones especiales, en cuya virtud se incluye dentro del Plan Anual de Fiscalizaciones para el ejercicio 2022 del Consejo de Cuentas, aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León en su reunión del 13 de junio de 2022 (BOCyL n.º 123, de 28 de junio de 2022), el "*Análisis de la seguridad informática del Ayuntamiento de Valladolid, ejercicio 2022*".

I.2. MARCO NORMATIVO

La normativa en materia de la organización de los ayuntamientos de la Comunidad Autónoma de Castilla y León y de seguridad de sus sistemas de información, que resulta más relevante a los efectos del objeto de esta fiscalización, se encuentra recogida fundamentalmente en las siguientes disposiciones:

I.2.1. NORMATIVA EUROPEA

- El Reglamento (UE) 2014/910 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (RGPD).

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

I.2.2. NORMATIVA ESTATAL

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL).
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto-Ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la, ya derogada Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal (RGPD).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

I.2.3. NORMATIVA AUTONÓMICA

- Ley 1/1998, de 4 de junio, de Régimen Local de Castilla y León (LRLCyL).
- Ley 2/2002, de 9 de abril, reguladora del Consejo de Cuentas de Castilla y León.

II. OBJETIVOS, ALCANCE Y DEBER DE COLABORACIÓN

II.1. OBJETIVOS

Se trata de una auditoría operativa cuyo objetivo principal es verificar el funcionamiento de los controles básicos de ciberseguridad implantados por la entidad fiscalizada. Así, se analizarán las actuaciones, medidas y procedimientos adoptados para la efectiva implantación de los controles básicos de ciberseguridad y, además, el grado de efectividad alcanzado por estos controles.

De acuerdo con ello, se identifican los siguientes objetivos específicos:

1. Proporcionar una evaluación sobre el diseño y la eficacia operativa de los controles básicos de ciberseguridad, identificando posibles deficiencias de control interno que puedan afectar negativamente a la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los datos, la información y los activos de la entidad, así como posibles incumplimientos normativos relacionados con la ciberseguridad.

2. Complementariamente al objetivo principal, proporcionar al ente auditado información relevante sobre su grado de ciberseguridad y de su capacidad para continuar con la actividad en caso de producirse un ataque, así como una propuesta sobre posibles acciones de mejora.

II.2. ALCANCE

Según la información que aparece reflejada en el estado de liquidación del presupuesto correspondiente al ejercicio de 2021, el importe de los créditos definitivos del presupuesto de gastos se elevó a 360.646.235,43 euros, siendo sus previsiones definitivas de ingresos, de 360.646.235,43 euros.

De acuerdo con los datos económicos, el Ayuntamiento objeto de la presente fiscalización, cuenta con tamaño suficiente para disponer de una estructura de tecnologías de la información y de las comunicaciones (TIC) de cierta complejidad. Esta estructura permite la realización de pruebas y la comprobación *in situ* de los aspectos que sean precisos.

El Ayuntamiento de Valladolid ha tenido que adaptarse necesariamente al uso de las nuevas tecnologías, por la generalización de su uso como herramienta de trabajo, y también por la digitalización creciente impuesta por la normativa. En definitiva, ha sufrido una transformación digital que debe cumplir unos requisitos mínimos de seguridad en sus sistemas de información, al ser éstos el soporte de los procesos básicos de gestión que el Ayuntamiento lleva a cabo, incluyendo algunos tan relevantes como la gestión contable y presupuestaria, la recaudación de tributos o la gestión del padrón municipal.

Por otra parte, en el ejercicio de su función fiscalizadora, los órganos de control externo, y en el caso presente, el Consejo de Cuentas de Castilla y León, deben poder confiar en los datos contenidos en los sistemas de la entidad fiscalizada, como único soporte existente de la información económica y financiera. Y para afirmar que un sistema de información es fiable, es necesario (aunque no suficiente) que existan unos controles eficientes de ciberseguridad, siendo los que se detallan en el alcance de esta fiscalización, los más básicos.

En cuanto a los sistemas de información del Ayuntamiento de Valladolid, se incluyen todos aquellos de los que disponga la entidad para realizar sus procesos relevantes de gestión, incluyendo las aplicaciones informáticas que los soportan, las bases de datos subyacentes y los sistemas operativos instalados en los equipos que los constituyen. Además de estos elementos específicos de cada sistema de información, se realizará la revisión de los elementos comunes a todos ellos (controladores de dominio, equipos de usuario, *software* de virtualización, equipamiento de red, etc.).

El ámbito temporal de la fiscalización alcanza a la situación existente en el año 2023, sin perjuicio de las comprobaciones correspondientes a actuaciones realizadas en años anteriores que sean necesarias para cumplir los objetivos.

En el transcurso de la fiscalización, y en función de la información obtenida sobre los sistemas de información de la entidad auditada, podría ser preciso acotar este ámbito de actuación para adecuarlo a la disponibilidad de recursos y para la realización de la fiscalización.

La fiscalización se refiere al estado de la seguridad de la información en el Ayuntamiento. Esta es una materia muy amplia, por lo que se circunscribe esta auditoría a la verificación de las actuaciones, medidas y procedimientos adoptados para la implantación de los controles básicos de ciberseguridad y su grado de eficacia.

Siguiendo el criterio establecido en la GPF-OCEX 5313 Guía práctica de fiscalización de los OCEX, Revisión de los controles básicos de ciberseguridad, que a su vez se basa en el marco establecido por organismos internacionales de reconocido prestigio como el "*Center for Internet Security (CIS)*", se pueden seleccionar controles críticos de ciberseguridad, que son un conjunto priorizado de medidas de seguridad orientadas a mitigar los ataques más comunes y dañinos.

El CIS clasifica los seis primeros controles críticos de ciberseguridad como básicos. Siguiendo este criterio de clasificación, la guía GPF-OCEX 5313 opta por establecer como Controles Básicos de Ciberseguridad (CBCS) estos seis primeros controles, y añade un séptimo control "*Copias de seguridad de datos y sistemas*", clasificada como el control número 10 por el CIS y que se incluye por ser un elemento fundamental para mantener una capacidad razonable de continuar con la actividad en caso de producirse un ataque.

Se incluye un octavo control (CBCS 8), de cumplimiento de determinados aspectos clave de la normativa principal de seguridad de la información.

Se evaluará el resultado obtenido para cada uno de los CBCS según el modelo de madurez de procesos CMM (*Capability Maturity Model*), ampliamente utilizado para caracterizar la implementación de un proceso y también propuesto por la GPF-OCEX 5313.

Por último, se define un apartado de avances en la aplicación del Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, con objeto de verificar si la entidad ha comenzado a aplicar alguno de los cambios y novedades que conlleva la actualización del Esquema Nacional de Seguridad.

De manera adicional se tendrán en cuenta las recomendaciones contenidas en las guías publicadas por el Centro Criptológico Nacional (CCN), organismo perteneciente al Centro Nacional de Inteligencia que tiene entre sus funciones precisamente el difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. De entre las guías publicadas, son las más relevantes las pertenecientes a la serie CCN-STIC-800, que establecen las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS, correspondiendo los CBCS a un subconjunto de estas medidas. En este punto hay que recordar que algunas de estas guías pueden no concordar exactamente con el nuevo ENS que se ha actualizado, una vez iniciada la presente fiscalización, por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

A continuación se expone un resumen de las verificaciones realizadas en cada uno de los epígrafes que conforman los resultados de la presente auditoría en los que juntamente con la revisión inicial del entorno de TI de la entidad y la estructura de su departamento de TI, se indican las comprobaciones realizadas en cada una de las áreas de trabajo, coincidentes con los ocho controles previstos en la Guía práctica de fiscalización, GPF-OCEX 5313 (siete controles básicos y una revisión de cumplimiento de diversas normas relacionadas con la seguridad de la información). En el Anexo I se incluye una tabla resumen de cada uno de los expresados controles y sus correspondientes subcontroles.

Los resultados del trabajo, 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:

1) Entorno tecnológico y sistemas de información objeto de la fiscalización.

Se ha realizado una revisión inicial del entorno de TI de la entidad, incluyendo la estructura de su departamento de TI.

Es objetivo de este apartado determinar los sistemas de información que dispone el Ayuntamiento, cuáles soportan los procesos relevantes de gestión, sus componentes, y la modalidad en que se encuentran desplegados.

Se ha analizado si el Ayuntamiento dispone de una estructura de TI; cómo se organiza; qué puestos de trabajo existen y su estado de cobertura, identificando posibles riesgos para la entidad derivados del modelo de gobernanza y de gestión de TI adoptados.

2) Inventario y control de dispositivos físicos.

Se ha verificado si se gestionan activamente (inventariando, revisando y corrigiendo) todos los dispositivos *hardware* de la red, de forma que solo los dispositivos autorizados tengan acceso.

Se ha comprobado si el Ayuntamiento:

- Dispone de un inventario completo y actualizado de los elementos *hardware* de la red.
- Dispone de procedimientos efectivos para controlar la conexión de elementos *hardware* no autorizados.

3) Inventario y control de software autorizado y no autorizado.

El objetivo es verificar si se gestiona activamente todo el software en los sistemas, de forma que solo se pueda instalar y ejecutar *software* autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

Se ha verificado si la entidad auditada:

- Dispone de un inventario completo y actualizado del software instalado en cada elemento de la red.
- Dispone de un plan de mantenimiento y actualización del software instalado.
- Dispone de procedimientos efectivos para detectar y evitar la instalación de software no autorizado en elementos de la red.

4) Proceso continuo de identificación y corrección de vulnerabilidades.

El objetivo es conocer si la entidad auditada dispone de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.

Para ello, se ha obtenido información de los siguientes hechos:

- Existencia de un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que se identifican con suficiente diligencia para gestionar adecuadamente el riesgo.

- Las vulnerabilidades identificadas son analizadas y priorizadas para su resolución atendiendo al riesgo que suponen para la seguridad del sistema.

- Se realiza un seguimiento de la corrección de las vulnerabilidades identificadas, de forma que se garantiza que estas son resueltas en el tiempo previsto en el procedimiento.

- La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.

5) Uso controlado de privilegios administrativos.

El objetivo es conocer si la entidad dispone de procesos y herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.

Para ello, se ha respondido a las siguientes cuestiones:

- ¿Los privilegios de administración se limitan adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita su correcto control?

- ¿Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares, se cambian antes de la entrada en producción del sistema?

- ¿Las cuentas de administración solo se utilizan para las tareas que son estrictamente necesarias?

- ¿Las cuentas de administración están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas?

- ¿El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas?

6) Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores.

El objetivo es verificar si la configuración de seguridad de dispositivos móviles, portátiles, equipos de sobremesa y servidores se gestiona activamente utilizando un proceso de gestión de cambios y configuraciones rigurosas, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.

Para ello, se ha comprobado si:

- La entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y aplicaciones.

- La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección en un periodo de tiempo oportuno.

7) Registro de la actividad de los usuarios.

El objetivo es conocer si la entidad recoge, gestiona y analiza registros de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.

Para ello se ha obtenido información sobre las siguientes cuestiones:

- El registro de auditoría está activado en todos los sistemas y dispositivos de red y contiene el detalle suficiente para la detección, análisis, investigación y prevención de ataques.

- Los registros se conservan durante el tiempo indicado en la política de retención, de forma que se encuentran disponibles para su consulta y análisis y además durante dicho periodo, se garantiza que no se producen accesos no autorizados.

- Los registros de todos los sistemas son revisados periódicamente para detectar anomalías y posibles compromisos de la seguridad del sistema y si se dispone de mecanismos para la centralización de estos registros de auditoría, de forma que se facilite la realización de las revisiones.

- Para sistemas de categoría ALTA, si la entidad dispone de un SIEM (Security Information and Event Management) o una herramienta de analítica de registros de actividad para realizar correlación y análisis de estos datos.

8) Copias de seguridad de datos y sistemas.

El objetivo es verificar que la entidad auditada utiliza procesos y herramientas para realizar la copia de seguridad de la información crítica, con una metodología probada que permita la recuperación de la información en tiempo oportuno.

Para su consecución, se ha verificado si:

- La entidad realiza copias de seguridad automáticas y periódicas de todos los datos y configuraciones del sistema.

- Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.

- Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.

9) Cumplimiento normativo.

Con respecto al cumplimiento normativo, la revisión se ha limitado a aspectos concretos y fundamentales de la normativa, ya que por su extensión y complejidad no entra en el alcance de esta fiscalización una comprobación exhaustiva.

- Con respecto al cumplimiento del ENS, se ha verificado si:
  - Existe una política de seguridad y responsabilidades.
  - Se ha elaborado una declaración de aplicabilidad.
  - Se dispone del Informe de auditoría.
  - Se ha realizado el Informe del estado de la seguridad.
  - Se ha publicado la declaración de conformidad y los distintivos de seguridad en la sede electrónica.
- Con respecto al cumplimiento de la LOPDGDD y del RGPD, se ha comprobado que:
  - Se ha nombrado el Delegado de protección de datos.
  - Se ha elaborado y publicado el registro de actividades de tratamiento.
  - Se ha realizado el análisis de riesgos y evaluación del impacto de las operaciones de tratamiento en los casos en que es de aplicación.
  - Se ha realizado una auditoría de cumplimiento o proceso alternativo para verificar la eficacia de las medidas de seguridad aplicadas.
- Sobre el cumplimiento de la Ley 25/2013, de 27 de diciembre (Impulso de la factura electrónica y creación del registro contable de facturas).
  - Se ha verificado la realización de la auditoría anual de sistemas del Registro Contable de Facturas.

10) Evaluación de los controles.

Se han seguido los criterios de evaluación establecidos en el apartado 8, Evaluación de las deficiencias de control interno detectadas de la GPF-OCEX 5330.

- Subcontroles.

Para cada subcontrol se asignará, en base a las evidencias obtenidas sobre su eficacia, una evaluación, que se corresponderá con uno de los siguientes valores:

Cuadro 1: Valoración de los subcontroles

Evaluación	Descripción
Control efectivo	Cubre al 100 % con el objetivo de control y: • El procedimiento está formalizado (documentado y aprobado) y actualizado. • El resultado de las pruebas realizadas para verificar su implementación y eficacia operativa ha sido satisfactorio.
Control bastante efectivo	En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100 % y: • Se sigue un procedimiento formalizado, aunque puede presentar aspectos de mejora (detalle, nivel de actualización, nivel de aprobación, etc.). • Las pruebas realizadas para verificar la implementación son satisfactorias. • Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa, pero no son ni significativos ni generalizados.
Control poco efectivo	Cubre de forma muy limitada el objetivo de control y: • Se sigue un procedimiento, aunque este puede no estar formalizado. • El resultado de las pruebas de implementación y de eficacia no es satisfactorio. Cubre en líneas generales el objetivo de control, pero: • No se sigue un procedimiento claro. • Las pruebas realizadas para verificar la implementación o la eficacia operativa no son satisfactorias (se han detectado incumplimientos significativos, aunque no están generalizados).
Control no efectivo o no implantado	No cubre el objetivo de control. • El diseño cubre el objetivo de control, pero el resultado de la revisión realizada pone de manifiesto que la implementación o la eficacia operativa del control no son satisfactorias (se han detectado incumplimientos significativos y generalizados).

- Controles.

  Los controles básicos de ciberseguridad son controles globales (compuestos por subcontroles) y se evaluará cada uno de ellos utilizando el modelo de madurez de procesos para valorar el grado de efectividad alcanzado por la entidad en cada uno de los controles, siguiendo el criterio del apartado 7 de la guía GPF-OCEX 5313.

  Los niveles globales para cada control son:

Cuadro 2: Valoración de los controles

Nivel	Madurez	Descripción
0- Inexistente.	0 %	Esta medida no está siendo aplicada en este momento.
1 - Inicial / ad hoc	10 %	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.
2 - Repetible, pero intuitivo	50 %	Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas, sin procedimientos escritos ni actividades formativas. La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
3 - Proceso definido	80 %	Los procesos están estandarizados, documentados y comunicados con acciones formativas. Se dispone de un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.

Nivel	Madurez	Descripción
4 – Gestionado y medible	90 %	La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere. Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.
5-Optimizado	100 %	Se siguen buenas prácticas en un ciclo de mejora continua. El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Para evaluar su nivel de madurez se tendrá en cuenta los resultados obtenidos en los subcontroles que lo forman (detallados en el Anexo I).

Finalmente, conforme a lo señalado en el referido apartado 7 de la GPF-OCEX, se evaluará el índice de cumplimiento sobre el nivel requerido, que será, de acuerdo con la categoría del sistema:

Categoría del Sistema	Nivel requerido
Básica	L2 (50 %)
Media	L3 (80 %)
Alta	L4 (90 %)

En el caso específico del control de cumplimiento de preceptos legales (CBCS–8) y que incluye actividades organizativas (aprobar una política de seguridad, realizar una auditoria), se evaluará de acuerdo con la siguiente escala para los subcontroles:

- No se ha iniciado la actividad.
- La actividad está solamente iniciada.
- La actividad está a medias.
- La actividad está muy avanzada.
- La actividad está prácticamente acabada.
- La actividad está completa.

La evaluación global del control se hará de manera idéntica al resto de controles, es decir, en función del nivel de madurez.

Dado que los niveles de madurez de los controles se corresponden con determinados porcentajes de cumplimiento, se evaluarán diferentes aspectos de cada uno de los subcontroles que los forman: documentación de los procesos, pruebas de efectividad, elementos cubiertos, etc., obteniendo una puntuación correspondiente al subcontrol, y un porcentaje de cumplimiento sobre el objetivo del 80 % (nivel L3).

La puntuación y porcentaje de cumplimiento de cada control será la media de los resultados de los subcontroles que lo forman.

Es preciso considerar que la puntuación se asigna a efectos de encuadrar el estado de un control dentro de un determinado nivel de madurez y, por lo tanto, es este nivel el que debe ser tenido en consideración en mayor medida como indicador del estado de ciberseguridad de la entidad, y no tanto como resultado numérico que únicamente se utiliza para obtener ese nivel de madurez.

Se ha contado con documentación más o menos completa de la mayoría de los procedimientos analizados, información que ha servido de base a las verificaciones realizadas a partir, en un principio, de los cuestionarios cumplimentados por la entidad fiscalizada y, en su parte final, de las entrevistas realizadas. Cuando se ha considerado preciso, atendiendo a las especiales circunstancias derivadas de la complejidad técnica en algunas partes del informe, dicha información ha sido completada mediante comprobaciones *in situ*, comunicación telefónica con los responsables de la entidad o a través de correo electrónico.

La adecuada comprensión de este Informe requiere que sea tenido en cuenta en su totalidad, ya que la mención o interpretación aislada de un párrafo, frase o expresión, podría carecer de sentido.

Los trabajos de fiscalización se han realizado de acuerdo con lo dispuesto en las Guías prácticas de fiscalización de los OCEX 5313 Revisión de los controles básicos de ciberseguridad, y 5330 Evaluación de las deficiencias de control interno detectadas. Supletoriamente se han aplicado las ISSAI-ES (Nivel III) aprobadas por la Conferencia de Presidentes de las Instituciones Autonómicas de Control Externo el 16 de junio de 2014.

Los trabajos desarrollados para la elaboración del presente Informe han finalizado en el mes de junio de 2023.

II.3. DEBER DE COLABORACIÓN

El Ayuntamiento fiscalizado ha mantenido una actitud de colaboración durante la realización del trabajo.

El Consejo de Cuentas quiere destacar la disponibilidad y colaboración del personal encargado de las funciones de TI, independientemente de las incidencias detectadas en el Informe. En ningún caso las conclusiones ponen en cuestión su capacidad o profesionalidad, considerándose que las conclusiones se dirigen a problemas de diseño o de inversión en medios humanos y materiales.

II.4. TRÁMITE DE ALEGACIONES

En cumplimiento de lo dispuesto en el artículo 25.4 del Reglamento de Organización y Funcionamiento del Consejo de Cuentas de Castilla y León, el Informe Provisional se remitió el 30 de junio de 2023 al Ayuntamiento de Valladolid, para que en un plazo de 15 días naturales formulara alegaciones.

El Ayuntamiento de Valladolid ha presentado con fecha 19 de julio de 2023, alegaciones al Informe de referencia, 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. Las modificaciones que se hayan efectuado en el Informe aparecen señaladas expresamente a pie de página.

En algunas de estas consideraciones el Ayuntamiento discrepa de determinadas calificaciones llevadas a cabo por el Consejo de Cuentas en cuanto al estado de formalización de sus procedimientos. Sin perjuicio de que el Consejo ha valorado la situación del Ayuntamiento al inicio de realización de los trabajos de campo y de acuerdo con la lógica de todas las evidencias aportadas, se deja constancia de la voluntad y trabajo del Ayuntamiento en la mejora y desarrollo de un ámbito tan específico y complejo como es el de la seguridad informática.

III. CONCLUSIONES

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

1) La concejalía de Planificación y Recursos 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.

2) Según la Relación de Puestos de trabajo aprobada en 2003, con sus respectivas modificaciones, el Ayuntamiento disponía de una dotación de 18 puestos, relacionados con las Tecnologías de la Información (TI), estando cubiertos 12 de estos puestos.

   La forma de cobertura de estos puestos es mediante 6 funcionarios de carrera y 6 funcionarios interinos.

3) Se verifica una concentración de funciones críticas en una única persona, concretamente en el Delegado de Protección de datos, debido a la relación de puestos de trabajo del Ayuntamiento. Esta situación dificulta su adecuado ejercicio.

4) El Ayuntamiento ha avanzado en los últimos meses en documentar detalladamente sus sistemas y procesos de gestión, pero aún gran parte del conocimiento reside casi de manera exclusiva en pocas personas, sin que exista un plan de actuación ante un cambio en el equipo de trabajo.

5) El Ayuntamiento no ha realizado una identificación y categorización según el ENS de los sistemas de información de que dispone. Esta es una 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.

6) Se ha optado en su mayor parte por un modelo *on-premise,* donde los servicios y la información se prestan y residen en equipos controlados por el Ayuntamiento e instalados físicamente en sus dependencias, con virtualización de aplicaciones y de servidores, en un entorno con un dominio Windows.

   Esta es una opción que precisa contar con personal suficiente y especializado para su mantenimiento y gestión. Se considera que el personal es suficiente, pero la forma actual de provisión de la mitad de las plazas no garantiza su estabilidad.

7) Del examen de la estructura de la red corporativa se concluye que tiene en general, dada su dimensión, un sistema con una adecuada protección perimetral, redundancia en los accesos a internet, equipamiento y configuración de la LAN. Sin embargo, se observa que el Ayuntamiento presenta algunas carencias en lo

que se refiere a la ubicación de cierto equipamiento ante contingencias que pudieran afectar a la red.

8) La conexión inalámbrica con la que cuenta el Ayuntamiento en líneas generales es adecuada. No obstante, en algunas localizaciones, adolece de las medidas de seguridad necesarias para poder gestionar adecuadamente los accesos y su correspondiente trazabilidad. Si bien se detecta que existe una independencia entre la red corporativa y esta red wifi de la entidad, es necesario evitar este tipo de situaciones. [1]

9) El Ayuntamiento dispone de las mismas soluciones de teletrabajo, tanto para los empleados del Departamento TIC como para el resto de los empleados de la entidad. Se considera que dichas soluciones son adecuadas.

III.2. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS (CBCS 1)

10) La información del inventario de *hardware* cubre razonablemente todos los elementos de los sistemas de información analizados y es bastante completa. No obstante, en algunos elementos no contienen detalles relevantes sobre su configuración y existen campos en los registros que no están actualizados.

11) La información del inventario de *hardware* se encuentra dispersa ya que, además de la base de datos principal de inventario, existen otras herramientas que pueden utilizarse a estos efectos en determinadas categorías de activos. No es posible establecer una relación inmediata entre los elementos de estas herramientas y el inventario principal.

    En concreto, el Ayuntamiento dispone de varias herramientas que le posibilitan tener un inventario completo de la planta de ordenadores personales y servidores con los que cuenta.

    El hecho de no tener una sincronización automática, sino que debe gestionarse y controlarse de forma manual, limita la capacidad de gestión y su efectividad. Todo ello resta utilidad a ese inventario.

12) Para la actualización del inventario se realiza un proceso que no está documentado y automatizado. Se ha comprobado que generalmente se sigue, pero depende únicamente de la actuación individual de los técnicos el realizarlo puntualmente, por lo que es fácil que haya elementos que no se actualicen o inventaríen adecuadamente.

13) Las medidas implantadas para impedir la conexión de dispositivos físicos no autorizados no son muy avanzadas, a pesar de contar con equipamiento de red

[1] Párrafo modificado en virtud de alegaciones

capaz de soportarlas. No obstante, las medidas en su conjunto dificultan el acceso no controlado a la red.

14) De las pruebas realizadas en esta área se puede concluir que el proceso de gestión de inventario y control de dispositivos físicos alcanza, un índice de madurez L2, en el que "*…la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y riesgo*".

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

15) El Ayuntamiento de Valladolid dispone de un inventario completo y actualizado de activos *software* con toda la información relevante sobre el activo (versiones, fechas de fin de soporte, elementos donde se encuentra instalado), obtenido a través de una herramienta que vuelca al servidor su configuración completa.

16) El Ayuntamiento no cuenta con un procedimiento documentado que describa cómo se debe efectuar el proceso de alta, mantenimiento y gestión del *software*, como tampoco la manera de efectuar las actualizaciones del parque municipal, definiendo equipos y marcos temporales.

17) La existencia de ese inventario completo y actualizado permite conocer la existencia de *software* fuera de soporte, pero no cuenta con procedimientos aprobados que permitan gestionar esa eventualidad, sin perjuicio de la realización de revisiones periódicas que no se documentan.

18) Se ha constatado la existencia de *software* fuera de soporte en una parte sustancial de los sistemas de información, incluyendo posibles elementos críticos.

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.

20) El Ayuntamiento de Valladolid ha implantado medidas para impedir que la instalación de *software* no autorizado, no proporcionando privilegios de administrador a los usuarios. Además, existe una sistemática para instalar el *software* de manera organizada mediante plantillas, si bien el proceso no está adecuadamente documentado en un procedimiento.

Se realizan inspecciones periódicas del *software* instalado y cuenta con herramientas especializadas, pero están ligadas a la voluntad del personal técnico

y no se realiza ningún informe resultante de estas inspecciones. Se hace uso de la herramienta microCLAUDIA para evitar la instalación de *ransomware*.

21) El proceso de gestión de inventario de *software* autorizado y no autorizado alcanza un índice de madurez L1, en el que "*la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia."*

Un ejemplo de las consecuencias de esta falta de gestión es que el Ayuntamiento tiene *software* que no se ha renovado a tiempo y ya no tiene soporte del fabricante.

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

22) El Ayuntamiento de Valladolid cuenta con una política de alerta ante posibles incidencias de seguridad, empleando distintas herramientas. A tal efecto la entidad revisa las informaciones y comunicaciones procedentes de diferentes fuentes de carácter técnico, aunque no realiza habitualmente ningún proceso de priorización y seguimiento de su corrección.

Por otro lado, se llevan a cabo acciones de detección de vulnerabilidades y actualizaciones para su resolución, pero no hay un procedimiento formalmente aprobado que defina la frecuencia, la periodicidad o la asignación de roles.

23) Se confía en la aplicación automática de los parches de los fabricantes para su resolución, sin que se hagan consideraciones adicionales en los casos en que el software está fuera de soporte ni hay un procedimiento claro en los casos en que no es posible la actualización automática. Estos casos generan un riesgo elevado de que una vulnerabilidad crítica sea pasada por alto y cree una ventana de oportunidad para un ataque.

24) La aplicación de los parches y actualizaciones en los elementos críticos sigue un procedimiento establecido, aunque no formalizado, lo cual deja al criterio profesional de los técnicos el priorizar la resolución de determinadas vulnerabilidades en función del riesgo que aprecien para sus sistemas.

25) En cuanto al cumplimiento de la presente área en la que se ha analizado el proceso continuo de identificación y corrección de vulnerabilidades, el Ayuntamiento alcanza un índice de madurez L2, en el que *"…la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y riesgo*".

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

26) No existe un procedimiento específico aprobado para la realización de tareas como la gestión de usuarios administradores, ni para el cambio de las contraseñas por defecto. Tampoco se han definido políticas homogéneas para los sistemas de autenticación.

A pesar de lo anterior, sí que se dispone de un documento interno de alta de usuario, donde se establece de manera genérica que todos los usuarios serán nominativos, cómo se lleva a cabo el alta, con cuestiones generales sobre cómo implementar o cambiar las credenciales una vez creado el usuario.

27) Se sigue manteniendo en parte de su equipamiento cuentas genéricas. En los equipos de usuario se lleva a cabo esa supresión, pero en parte del equipamiento permanecen, lo cual supone una importante brecha de seguridad.

28) 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.

29) La práctica de contraseñas es en general adecuada, a través de la generación de contraseñas robustas, guardándose en un repositorio seguro las de aquellos sistemas que no hacen uso del directorio activo. La política del directorio activo es correcta en la gestión de las contraseñas. (

30) En el caso de directorio activo, además de almacenar los registros de eventos, se genera un informe resumen diario "*inteligible*" con la utilización de los usuarios de administración y los cambios. No hay ningún procedimiento que marque esta frecuencia ni quién lo debe realizar.

Se ha comprobado tanto la robustez de los accesos, como la marca de estos accesos en los logs de la entidad.

Aunque existe un proceso establecido, no hay un procedimiento formalizado que defina una periodicidad de revisión de registros de actividad en busca de patrones de actividad con el fin de detectar posibles acciones sospechosas o ilícitas, ni tampoco determinar qué registros deben guardarse, ni el periodo de retención ni se definen responsabilidades, por lo que queda a criterio del técnico el determinarlo y su correcta realización.

31) 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. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia*".

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

32) El Ayuntamiento realiza un proceso de configuración segura, siguiendo plantillas propias y las instrucciones del fabricante en función del tipo de dispositivo y funcionalidad, de los elementos que constituyen sus sistemas, pero sin seguir un procedimiento claro que detalle las tareas a realizar, quién debe hacerlo y la manera de dejar constancia de su ejecución.

Los resultados de las pruebas realizadas indican que no existen disparidades en cuanto al seguimiento de normas para su bastionado resultando en configuraciones seguras, pero con valores que deberían intentar aumentarse.

33) El Ayuntamiento ha implantado una serie de medidas que, si bien no son completamente efectivas, sí dificultan que los usuarios puedan cambiar la configuración de los sistemas, aunque no existen mecanismos que permitan detectar cambios no autorizados o erróneos de la configuración y su corrección en un periodo de tiempo oportuno.

34) Los resultados en cuanto a la configuración segura del *software* y *hardware* se corresponden con un nivel de madurez L1: "*En el nivel L1 de madurez, el proceso existe, pero no se gestiona. Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad*".

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

35) En el Ayuntamiento no cuentan con ningún procedimiento que indique qué actividades serán objeto de registro, el periodo de retención, o la protección que se aplicará a los registros.

36) El Ayuntamiento de Valladolid lleva a cabo la revisión de los registros de actividad en busca de patrones anormales; bien mediante algún proceso de alerta automática, a través del SIEM o de otras herramientas de las que disponen o bien mediante procesos de alerta manual. Pero no se dispone de una política o normativa documentada que establezca qué se debe registrar, quién realiza la actividad, cuándo la realiza y sobre qué información. Por otro lado, es necesario continuar los esfuerzos en la centralización de todos los logs existentes.

37) En la red del Ayuntamiento no se encuentra desplegada ninguna sonda individual SAT-INET, proporcionada por el CCN, donde se lleva a cabo la detección en tiempo real de las amenazas existentes en el tráfico que fluye entre la red interna del Ayuntamiento e Internet.

38) Se concluye que en el área de registro de la actividad de los usuarios se alcanza un índice de madurez L2, en el que "*existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias, pero es impredecible el resultado si se dan circunstancias nuevas*".

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

39) Existe un proceso bien definido y parcialmente formalizado para la realización de copias de seguridad. El Ayuntamiento dispone de las herramientas adecuadas y el proceso se ejecuta correctamente. Sin embargo, carece de un procedimiento formalmente aprobado que defina las responsabilidades y la forma de documentar el proceso.

40) En lo que respecta al procedimiento de recuperación de copias completas y periódicas en un entorno de pruebas sí que cuentan con un procedimiento, si bien no aprobado formalmente, en el que se detallan las pruebas que hay que realizar de restauración para comprobar que se están realizando correctamente las copias de seguridad. No se han detectado problemas en las recuperaciones realizadas en el último año.

41) Se aplican medidas en general efectivas para la protección de las copias de seguridad.

42) 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 L2, en el que "*existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias, pero es impredecible el resultado si se dan circunstancias nuevas".*

III.9. CUMPLIMIENTO NORMATIVO (CBCS 8)

43) El Ayuntamiento de Valladolid no cumple con las especificaciones contenidas en los artículos 11, 27.4, 34 y 41 del ENS, que han sido objeto de revisión en esta fiscalización. No obstante, nos traslada con evidencias documentales que está trabajando en la actualidad de forma prioritaria en la subsanación de este incumplimiento. Así se encuentra desarrollando una política de seguridad formal y la declaración de aplicabilidad.

En cuanto a lo que respecta al artículo 35 del ENS cumple, salvo aspectos puntuales, con las especificaciones contenidas, que han sido objeto de revisión en esta fiscalización.

44) El proceso de adaptación a la normativa en materia de protección de datos está únicamente iniciado. En ese sentido se enmarca el nombramiento del delegado de protección de datos con fecha el 11 de julio de 2022, pero no se ha dispuesto de un modo formal de un Registro de actividades de tratamiento (RAT), y, por tanto, tampoco se ha podido evaluar si existen tratamientos considerados de alto riesgo,

ni en ese caso, hacer con carácter previo, una evaluación del impacto del tratamiento (EIPD). Asimismo, tampoco se han terminado otras acciones fuertemente interrelacionadas con esa normativa para la adaptación del Ayuntamiento al ENS. Esta situación no es conveniente dado que ambas normativas no son independientes.

45) El Ayuntamiento de Valladolid ha realizado la auditoría de sistemas anual del Registro Contable de Facturas correspondiente al ejercicio 2022.

46) De acuerdo con las conclusiones de esta área, el resultado de la evaluación del control es un nivel de madurez L2, en el que *"existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias, pero es impredecible el resultado si se dan circunstancias nuevas"*.

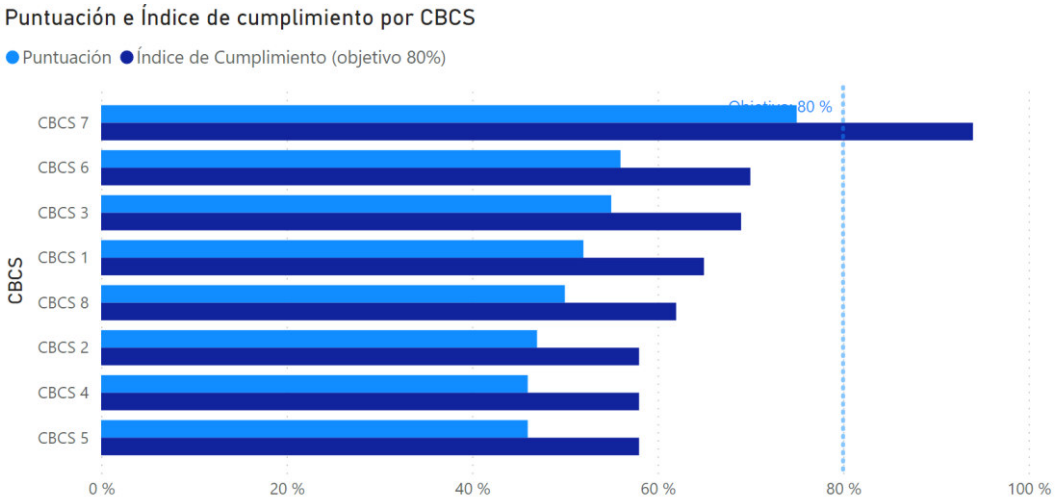
III.10. AVANCES EN LA APLICACIÓN DEL REAL DECRETO 311/2022

47) El Ayuntamiento está trabajando en la adaptación al nuevo ENS siguiendo el plan de adecuación elaborado por la Oficina Técnica de Seguridad. Dicho plan se está desarrollando, partiendo de un plan de adecuación alineado con el perfil de cumplimiento para ayuntamientos (de gran tamaño), adaptándolo a las modificaciones introducidas en el RD 311/2022.

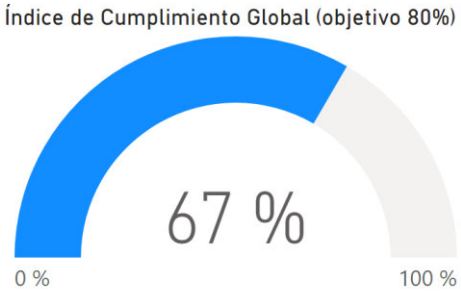
III.11. SITUACIÓN GLOBAL DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD)

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 los controles.

Gráfico 1: Puntuación e Índice de cumplimiento por CBCS



CBCS	Descripción	Puntuación	Índice de Cumplimiento (objetivo 80%)
CBCS 1	Inventario y control de dispositivos físicos	52 %	65 %
CBCS 2	Inventario y control de software autorizado y no autorizado	47 %	58 %
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	55 %	69 %
CBCS 4	Uso controlado de privilegios administrativos	46 %	58 %
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	46 %	58 %
CBCS 6	Registro de la actividad de los usuarios	56 %	70 %
CBCS 7	Copias de seguridad de datos y sistemas	75 %	94 %
CBCS 8	Cumplimiento normativo	50 %	62 %
Total			**67 %**



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

El índice de cumplimiento (sobre un objetivo de madurez L2 que corresponde a una puntuación del 80%) es del **67%**.

IV. RECOMENDACIONES

Con carácter general:

1) El Alcalde debería impulsar las actuaciones necesarias para solventar los incumplimientos normativos y las deficiencias de carácter técnico que se han constatado durante la revisión de los controles.

   Para esta tarea, organismos como el CCN, la FEMP o la AEPD publican guías detalladas que ofrecen modelos completos para la adaptación de los ayuntamientos de características similares al de Valladolid que pueden ser tomadas como referencia para facilitar el proceso.

2) El Alcalde debería asumir y promover un compromiso firme por parte del Pleno del Ayuntamiento con el cumplimiento de la normativa, elaborando una estrategia a largo plazo, que establezca una gobernanza de Tecnologías de la Información adecuada, comenzando por:

   - Solventar la situación en cuanto a plazas relevantes como son las de responsable de seguridad, con el fin de solventar aquellos aspectos técnicos que precisan mejoras y establecer estrategias adecuadas con una diferenciación de responsabilidades que ahora recaen en la misma persona.

   - Específicamente, se debería culminar el proceso mediante la realización de auditorías o autoevaluaciones de cumplimiento del ENS, valorándose su realización conjunta con las relativas a protección de datos personales.

Específicamente para cada una de las áreas, por su relevancia, se recomienda llevar a cabo las siguientes acciones:

Sobre el entorno tecnológico del Ayuntamiento:

3) El Alcalde debería impulsar las acciones necesarias para dotar adecuadamente los puestos contemplados en la RPT para garantizar una estructura que cumpla los principios de seguridad como función diferenciada y que tenga capacidad de asumir las tareas requeridas para la gestión de sus sistemas de información según el modelo general *on-premise* adoptado.

4) El responsable de seguridad que se determine en la política de seguridad debería garantizar que existe una documentación suficiente del entorno de TI del Ayuntamiento para asegurar que el conocimiento sobre los sistemas de información está disponible con independencia de las personas que formen el departamento de TI. Debe resolverse la situación en cuanto a los roles principales que son necesarios en una organización para una adecuada política de seguridad.

Sobre el inventario y control de activos (*hardware* y *software*) y el uso controlado de privilegios administrativos:

5) El Alcalde debería impulsar la realización de una planificación a largo plazo de las necesidades de renovación tecnológica para evitar la obsolescencia del *hardware* y utilización de *software* sin soporte del fabricante, asegurando una dotación presupuestaria adecuada.

Sobre el proceso continuo de identificación y corrección de vulnerabilidades:

6) El responsable de seguridad que se defina en la política de seguridad debería participar juntamente con el responsable del sistema, en las decisiones que conllevan el empleo de herramientas automatizadas para la detección de vulnerabilidades.[2]

7) El Alcalde debería impulsar la inclusión en la contratación de los servicios informáticos de las cláusulas que permitan realizar un control de cómo se llevan a cabo los servicios y el uso y control de los privilegios de administración de acuerdo a lo especificado en el ENS.

Sobre el cumplimiento normativo:

8) El Pleno del Ayuntamiento debe seguir liderando las actuaciones ya iniciadas en lo que se refiere a dotar a la entidad de una adecuada política de seguridad y una declaración de aplicabilidad, de acuerdo con lo especificado en los artículos 11 y 27.4 del ENS.

9) El Alcalde debería requerir al delegado de protección de datos que supervise el cumplimiento del RGPD, solicitándole su asesoramiento cuando lo considere oportuno.

10) El Pleno del Ayuntamiento debería aprobar una normativa que garantice que el registro de actividad de los usuarios se realiza de acuerdo con lo establecido en el artículo 23 del ENS, en concreto con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral. Para ello podría utilizarse como referencia la guía CCN-STIC 831 Registro de la actividad de los usuarios.

[2] Párrafo modificado en virtud de alegaciones

ÍNDICE DE CUADROS

Cuadro 1: Valoración de los subcontroles..... 15

Cuadro 2: Valoración de los controles..... 16

ÍNDICE DE GRÁFICOS

Gráfico 1: Puntuación e Índice de cumplimiento por CBCS 28

ANEXO

Detalle de controles y subcontroles

Control		Objetivo de control	Subcontroles	Medidas de seguridad del ENS
CBCS 1	Inventario y control de dispositivos físicos.	Gestionar activamente todos los dispositivos *hardware* en la red, de forma que solo los dispositivos autorizados tengan acceso a la red.	CBCS 1-1: Inventario de activos físicos autorizados. La entidad dispone de un inventario de activos físicos autorizados completo, actualizado y detallado.	op.exp.1
			CBCS 1-2: Control de activos físicos no autorizados. La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el acceso de dispositivos físicos no autorizados.	
CBCS 2	Inventario y control de *software* autorizado y no autorizado.	Gestionar activamente todo el *software* en los sistemas, de forma que solo se pueda instalar y ejecutar *software* autorizado.	CBCS 2-1: Inventario de SW autorizado. La entidad dispone de un inventario de SW completo, actualizado y detallado.	op.exp.1 op.exp.2
			CBCS 2-2: SW soportado por el fabricante. El SW utilizado por la entidad tiene soporte del fabricante. En caso contrario, se marca en el inventario como fuera de soporte.	
			CBCS 2-3: Control de SW no autorizado. La entidad dispone de mecanismos que impiden la instalación y ejecución de SW no autorizado.	
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades.	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	CBCS 3-1 Identificación. Existe un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que éstas son identificadas en tiempo oportuno.	mp.sw.2 op.exp.4
			CBCS 3-2 Priorización. Las vulnerabilidades identificadas son analizadas y priorizadas para su resolución atendiendo al riesgo que suponen para la seguridad del sistema.	
			CBCS 3-3 Resolución de vulnerabilidades. Se realiza un seguimiento de la corrección de las vulnerabilidades identificadas, de forma que se garantiza que estas son resueltas en el tiempo previsto en el procedimiento.	
			CBCS 3-4 Parcheo. La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.	

Control		Objetivo de control	Subcontroles	Medidas de seguridad del ENS
CBCS 4	Uso controlado de privilegios administrativos.	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	CBCS 4-1 Inventario y control de cuentas de administración. Los privilegios de administración están limitados adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita su correcto control.	
			CBCS 4-2 Cambio de contraseñas por defecto. Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares, se cambian antes de la entrada en producción del sistema.	op.acc.4
			CBCS 4-3 Uso dedicado de cuentas de administración. Las cuentas de administración solo se utilizan para las tareas que son estrictamente necesarias.	
			CBCS 4-4 Mecanismos de autenticación. Las cuentas de administración están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.	op.acc.5
			CBCS 4-5 Auditoría y control. El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.	
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores.	Implementar la configuración de seguridad de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.	CBCS 5-1 Configuración segura La entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y SW.	
			CBCS 5-2: Gestión de la configuración La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.	op.exp.2 op.exp.3

Control		Objetivo de control	Subcontroles	Medidas de seguridad del ENS
CBCS 6	Registro de la actividad de los usuarios.	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	CBCS 6-1: Activación de logs de auditoría. El log de auditoría está activado en todos los sistemas y dispositivos de red y contiene el detalle suficiente para la detección, análisis, investigación y prevención de ciberataques.	op.exp.8 op.exp.10
			CBCS 6-2: Almacenamiento de logs: Retención y protección. Los logs se conservan durante el tiempo indicado en la política de retención, de forma que se encuentran disponibles para su consulta y análisis. Durante dicho periodo, el control de acceso garantiza que no se producen accesos no autorizados.	
			CBCS 6-3: Centralización y revisión de logs. Los logs de todos los sistemas son revisados periódicamente para detectar anomalías y posibles compromisos de la seguridad del sistema. Se dispone de mecanismos para la centralización de los logs de auditoría, de forma que se facilite la realización de las revisiones anteriores.	
			CBCS 6-4: Monitorización y correlación. La entidad dispone de un SIEM (Security Information and Event Management) o una herramienta de analítica de logs para realizar correlación y análisis de logs. Solo para sistemas de categoría ALTA.	
CBCS 7	Copias de seguridad de datos y sistemas.	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	CBCS 7-1: Realización de copias de seguridad. La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.	mp.info.9
			CBCS 7-2: Realización de pruebas de recuperación. Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.	
			CBCS 7-3: Protección de las copias de seguridad. Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.	

CBCS 8	Cumplimiento normativo.	Cumplimiento de determinados preceptos legales relacionados con la seguridad de la información.	CBCS 8-1: Cumplimiento del ENS. Política de seguridad y responsabilidades Declaración de aplicabilidad. Informe de Auditoría (nivel medio o alto). Informe del estado de la seguridad. Publicación de la declaración de conformidad y los distintivos de seguridad en la sede electrónica.	
			CBCS 8-2: Cumplimiento de la LOPD/RGPD Nombramiento del DPD Registro de actividades de tratamiento. Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento (para los de riesgo alto). Informe de auditoría de cumplimiento (cuando el responsable del tratamiento haya decidido realizarla).	
			CBCS 8-3: Cumplimiento de la Ley 25/2013, de 27 de diciembre (Impulso de la factura electrónica y creación del registro contable de facturas). Informe de auditoría de sistemas anual del Registro Contable de Facturas.	

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

CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE VALLADOLID, EJERCICIO 2022

TRATAMIENTO DE ALEGACIONES

PLAN ANUAL DE FISCALIZACIONES 2022

ÍNDICE

ALEGACIONES PRESENTADAS AL INFORME PROVISIONAL DEL "ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE VALLADOLID, EJERCICIO 2022"

I. EXPOSICIÓN PRELIMINAR 3
II. ALEGACIÓN PRIMERA 4
III. ALEGACIÓN SEGUNDA 5
IV. ALEGACIÓN TERCERA 6
V. ALEGACIÓN CUARTA 7
VI. ALEGACIÓN QUINTA 8
VII. ALEGACIÓN SEXTA 9
VIII. ALEGACIÓN SÉPTIMA 9
IX. ALEGACIÓN OCTAVA 10
X. ALEGACIÓN NOVENA 14

ACLARACIONES

El Ayuntamiento de Valladolid ha presentado con fecha 19 de julio de 2022, alegaciones al Informe de referencia, 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

Expone:

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.

Contestación

No se trata propiamente de una alegación, sino que se trata de una exposición preliminar realizada por parte del Ayuntamiento de Valladolid 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 "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

Alegación realizada

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.

Contestación a la alegación

Tal y como se marca de manera explícita en el Informe, seis de los doce puestos consignados en la Unidad Organizativa "*Departamento de las Tecnologías de la Información y las Comunicaciones*" son de personal funcionario interino. Por tanto, la tasa de temporalidad en el departamento es del 50 %, siendo cuatro de dichos puestos muy especializados "*Técnico Superior de Sistemas y Tecnologías de la Información*".

A esto hay que añadir que las tareas propias del responsable de seguridad, a nivel de la RPT, recaen en la delegada de protección de datos, según se establece en la Resolución de 27 de enero de 2022, del concejal Delegado de Planificación y Recursos del Ayuntamiento de Valladolid, relativa al concurso específico para la provisión del puesto de delegado de protección de datos. Si bien dichas cuestiones,

tal y como se indica en la alegación, entran en el ámbito de lo recomendable y no en lo exigible jurídicamente, esto está afectando, tal y como también se indica en el informe, en la constitución del Comité de Seguridad.

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

III. ALEGACIÓN SEGUNDA

Alegación realizada

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 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.

Contestación a la alegación

Tal y como se denota de manera explícita en la conclusión, se trata de algunas localizaciones concretas, conocidas por el Ayuntamiento. Asimismo, se cita de manera clara que existe una independencia entre la red corporativa y esta red wifi de la entidad, pero afirmando que es necesario evitar este tipo de situaciones.

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

Donde dice:

8) 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. Si bien se detecta que existe una independencia entre la red corporativa y esta red wifi de la entidad, es necesario evitar este tipo de situaciones.

Debe decir:

8) La conexión inalámbrica con la que cuenta el Ayuntamiento en líneas generales es adecuada. No obstante, en algunas localizaciones, adolece de las medidas de seguridad necesarias para poder gestionar adecuadamente los accesos y su correspondiente trazabilidad. Si bien se detecta que existe una independencia entre la red corporativa y esta red wifi de la entidad, es necesario evitar este tipo de situaciones.

IV. ALEGACIÓN TERCERA

Alegación realizada

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.

Contestación a la alegación

En cuanto a la conexión de dispositivos físicos no autorizados, las apreciaciones realizadas se fundamentan en las medidas aplicadas a la electrónica de red con la que cuenta el Ayuntamiento y a las acciones que se dan en esta electrónica de red para evitar esos accesos.

En el nivel de madurez asociado al subcontrol CBCS 1.2. sí que se tuvo en cuenta la solución NAC referenciada y verificada en los trabajos de campo efectuados, tal y como se indica en el texto de la alegación.

Para obtener una calificación superior en dicho control, sería necesario contar con un procedimiento formalizado y aprobado en dicha materia, en el que se definiese de manera explícita cómo se lleva a cabo el control de acceso a la red, quién es el responsable y cómo se actúa en caso de acceso indebido.

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

V. ALEGACIÓN CUARTA

Alegación realizada

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 con mayor detalle.

Contestación a la alegación

El hecho de que se trate de aplicaciones críticas hace todavía más necesaria su actualización y que cuenten con *software* que se encuentre dentro de soporte para hacer frente, de un modo más robusto, a posibles vulnerabilidades que surjan o que provoquen incidentes de seguridad. Si dicho *software* no es aplicable en máquinas

actuales, se debería establecer una migración de dichos aplicativos a otros que sí que lo fueran con el fin de mitigar esta situación.

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

VI. ALEGACIÓN QUINTA

Alegación realizada

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”.

Contestación a la alegación

Si bien la operativa está marcada adecuadamente por el servicio VMaaS esto en ningún caso puede suplir a un procedimiento formalizado para el tratamiento de vulnerabilidades incluyendo su identificación, priorización, resolución y parcheo en el que se especifican cómo se identifican (si se usan herramientas automáticas o no), cómo se priorizan y según qué criterios, cómo se hace el seguimiento y se aplica un proceso de gestión del cambio. La falta de un procedimiento adecuadamente formalizado deja al buen hacer de los técnicos su adecuado seguimiento.

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

VII. ALEGACIÓN SEXTA

Alegación realizada

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".

Contestación a la alegación

La no utilización de cuentas genéricas resulta evidente que es una buena práctica de seguridad, que debe ser seguida por cualquier organización. En caso de que existan sistemas en los que, por imposibilidad técnica, no se puedan personalizar las cuentas de acceso, deben implantarse controles compensatorios para suplir la falta de trazabilidad.

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

VIII. ALEGACIÓN SÉPTIMA

Alegación realizada

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".

Contestación a la alegación

Tal y como se indica en la alegación y en el apartado 3 del anexo I se siguen medidas que, con carácter general y así se indica en la conclusión 29, la práctica de contraseñas es, en general, adecuada. No obstante, no existen otras medidas compensatorias para elementos críticos en la organización que eleven el nivel de seguridad.

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

IX. ALEGACIÓN OCTAVA

Alegación realizada

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 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 (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 en la última parte de la página 85 del informe provisional que nos ocupa, 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 n.º 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 n.º 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 n.º 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.

<u>Contestación a la alegación</u>

Si bien el *Proyecto de implantación de la normativa de protección de datos para este Ayuntamiento* suscrito el 26 de octubre de 2022, enunciado en la alegación, recoge ocho (8) líneas de actuación-medidas a adoptar con un período temporal previsto que abarca desde noviembre 2022 a marzo 2024 (las cuáles son acciones importantes a desarrollar), el objeto de la presente fiscalización se fundamenta en

dos de dichas líneas especialmente importantes: Registro de actividades de tratamiento y Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento (para los tratamientos de riesgo alto).

Se destaca el esfuerzo que está llevando a cabo la Institución, pero, tal y como refleja la propia DPD, dichos registros de actividades de tratamiento se encuentran en revisión y, por tanto, no ha obrado en manos del equipo auditor ningún documento adecuadamente validado o revisado que pueda ser considerado documento definitivo. De ahí que en la evaluación se haya constado que la "*La actividad está solamente iniciada*" en lugar de "*No se ha iniciado la actividad*", reconociendo esos trabajos llevados a cabo.

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

X. ALEGACIÓN NOVENA

Alegación realizada

Alegación 9

- *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*** *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.

Contestación a la alegación

Las Normas de Auditoría del Sector Publico establecen que las recomendaciones contenidas en un informe de fiscalización se formulan por el órgano de fiscalización sobre la base de las pruebas efectuadas y la información obtenida en el transcurso de la fiscalización, y pretenden proponer mejoras en los procedimientos de gestión llevados a cabo por el ente fiscalizado.

Con carácter general, las recomendaciones derivan de las conclusiones expuestas en el informe, y estas, a su vez, de los resultados del trabajo. La

contestación de la entidad fiscalizada a las recomendaciones que efectúa el Consejo de Cuentas tiene un cauce distinto, a través del informe de seguimiento de recomendaciones previsto en el artículo 30 de su Reglamento de organización y funcionamiento.

No obstante, lo señalado, a partir de la referencia que el Ayuntamiento de Valladolid hace en su escrito de alegaciones al contenido de la recomendación 6), puede observarse lo siguiente: La recomendación recogía que el responsable de seguridad debe participar en las decisiones que comportan el empleo de dichas herramientas. Se reconoce el esfuerzo llevado a cabo, tanto en lo concerniente al servicio VMaaS como a las pruebas de penetración (pentesting) realizadas, y así se ha referenciado en el informe.

A los efectos de mejorar el contenido del Informe se realiza la siguiente precisión.

Donde dice:

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 simulan ataques reales (Red team).”***

Debe decir:

6) ***El responsable de seguridad que se defina en la política de seguridad debería participar juntamente con el responsable del sistema, en las decisiones que conllevan el empleo de herramientas automatizadas para la detección de vulnerabilidades y la realización (o contratación dada lo simulan ataques reales (Red team).”***