CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SEGOVIA

PLAN ANUAL DE FISCALIZACIONES 2024

ÍNDICE

SIGLAS Y ABREVIATURAS

Art.	Artículo.
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.
ENS	Esquema Nacional de Seguridad.
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.
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.

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

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 2024 del Consejo de Cuentas, aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León en su reunión del 12 de Febrero de 2024 (BOCyL n.º 44, de 1 de marzo de 2024), el "*Análisis de la seguridad informática del Ayuntamiento de Segovia*".

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 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.

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 EUROPEA

- El Reglamento (UE) 910/2024 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) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

II. OBJETIVOS, ALCANCE Y LIMITACIONES

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 2022, el importe de los créditos definitivos del presupuesto de gastos se elevó a 88.629.200,96 euros, siendo sus previsiones definitivas de ingresos, de 88.629.200,96 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 de cierta complejidad. Esta estructura permite la realización de pruebas y la comprobación *in situ* de los aspectos que sean precisos.

El Ayuntamiento de Segovia 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. Como consecuencia de ello, 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 más básicos los que se detallan en el alcance de esta fiscalización.

En cuanto a los sistemas de información del Ayuntamiento de Segovia, 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 2024, 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*", clasificado 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 analiza en un apartado los 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 se incluye una tabla resumen de cada uno de los expresados controles y sus correspondientes subcontroles.

Los resultados de la fiscalización, de acuerdo con lo previsto en el apartado 7 de la GPF-OCEX 5313, Evaluación de los hallazgos de auditoría, han sido ponderados siguiendo los criterios establecidos en el apartado 8, Evaluación de las deficiencias de control interno detectadas de la GPF-OCEX 5330:

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

Cuadro n.º 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, que a su vez están basadas en la guía de seguridad CCN-STIC 804 del CCN, usando una escala, según se resume en el siguiente cuadro. Las descripciones son las establecidas en el anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Los niveles globales para cada control son:

Cuadro n.º 2.- Valoración de los controles

Nivel	Madurez	Descripción
0- Inexistente.	0 %	No existe un proceso que soporte el servicio requerido.
1 - Inicial / ad hoc	10 %	Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes. Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.
2 - Repetible, pero intuitivo	50 %	En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad. Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos
3 - Proceso definido	80 %	Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

Nivel	Madurez	Descripción
4 – Gestionado y medible	90 %	Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.
5-Optimizado	100 %	La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

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

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
Básico	----------	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 auditoría), 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, en un principio, a partir 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 finalizaron en noviembre de 2024.

II.3. LIMITACIONES

Con carácter general no han existido limitaciones en el trabajo realizado, habiendo tenido el Ayuntamiento fiscalizado una actitud de colaboración.

El Consejo de Cuentas quiere destacar la disponibilidad y colaboración del personal encargado de las funciones de Tecnologías de la Información, 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 28 de febrero de 2025 al Ayuntamiento de Segovia, para que en un plazo de 15 días naturales formulara alegaciones.

El Ayuntamiento de Segovia ha presentado con fecha 13 de marzo de 2025, 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.

Las alegaciones formuladas se incorporan a este Informe y han sido objeto de análisis pormenorizado. A este respecto, se ha emitido informe motivado sobre dichas alegaciones, que ha servido de base para la aceptación o desestimación de las mismas. 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 Turismo; Innovación y Digitalización; Promoción Económica realiza todas las acciones necesarias para una dirección efectiva de la política de seguridad informática. No obstante, presenta carencias muy importantes en el ámbito de una adecuada relación de puestos de trabajo, e impulso de la cobertura de plazas. [1]

   Según la Relación de Puestos de Trabajo correspondiente al 2022, con sus respectivas modificaciones, el Ayuntamiento disponía de una dotación de 8 puestos, relacionados con las Tecnologías de la Información, estando 3 de estos puestos adscritos a otros servicios. Por otro lado, existen 2 puestos de trabajo adscritos a tareas de Tecnologías de la Información realizando funciones de administración electrónica. Por tanto, sumarían 7 puestos que son con los que cuenta realmente el servicio, estando 2 de ellos vacantes. La tipología de personal de estos puestos es la siguiente: 4 funcionarios de carrera, 1 funcionario interino.

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

3) El Ayuntamiento carece de documentación detallada de sus sistemas y procesos de gestión, residiendo el conocimiento, prácticamente de manera exclusiva, en pocas personas, sin que exista un plan de actuación ante un cambio en el equipo de trabajo.

4) El Ayuntamiento ha realizado una identificación y categorización adecuada para el sistema de información que comprende la sede electrónica, pero falta una categorización completa y adecuada de los restantes sistemas de acuerdo con los criterios del Esquema Nacional de Seguridad. 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.

5) 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

[1] Párrafo modificado en virtud de alegaciones.
[2] Párrafo modificado en virtud de alegaciones.

de aplicaciones y de servidores, en un entorno con un dominio Windows, siendo esta una opción que precisa contar con personal suficiente y especializado para su mantenimiento y gestión. Se considera que el personal actual es insuficiente para las tareas que conllevan una adecuada gestión y mantenimiento.

6) Del examen de la estructura de la red corporativa se concluye que, dada su dimensión, tiene un sistema con una adecuada protección perimetral, redundancia en los accesos a internet, equipamiento y configuración de la Red de Área Local. 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.

7) La conexión inalámbrica con la que cuenta el Ayuntamiento, en líneas generales, es adecuada. Además, su diseño garantiza la independencia entre la red corporativa y la red Wifi de la entidad.

8) El Ayuntamiento dispone de una plataforma de teletrabajo teóricamente capaz de proporcionar un nivel suficiente de seguridad. Pero su implementación práctica actual contiene algún aspecto potencialmente inseguro.

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

9) La información del inventario de *hardware* si bien cubre razonablemente todos los elementos de los sistemas de información analizados y es bastante completa, en muchos de sus elementos no están adecuadamente actualizados o existen campos sin cumplimentar.

10) La información del inventario de hardware se encuentra dispersa ya que cuenta con dos métodos de gestión de la información de inventario, que pueden utilizarse a estos efectos en determinadas categorías de activos. No es posible establecer una relación inmediata entre ambos métodos de gestión porque no están adecuadamente actualizados ni tampoco se encuentran sincronizados. Esto implica una disminución de la fiabilidad. Todo ello resta utilidad a ese inventario. [3]

11) Existe el riesgo de perder el control sobre su utilización, ciclo de vida, vulnerabilidades, etc. Esa pérdida de control se traduce también en que no es posible programar con tiempo suficiente la sustitución de *hardware* obsoleto (fundamental en el caso de una administración sujeta a los plazos de la normativa en materia de contratación) ni, por consiguiente, realizar una planificación presupuestaria adecuada.

[3] Párrafo modificado en virtud de alegaciones.

12) Para la actualización del inventario, se realiza un proceso que no está documentado y automatizado y el realizarlo puntualmente depende únicamente de la actuación individual de los técnicos, 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 son muy básicas, a pesar de contar con equipamiento de red capaz de soportar funcionalidades avanzadas, pero que en buena parte no se están utilizando.

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 L1: "*En el nivel L1 de madurez, las organizaciones no disponen de un ambiente estable para la prestación del servicio requerido. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible".*

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

15) El Ayuntamiento de Segovia dispone de un inventario completo y actualizado de activos *software* con toda la información relevante sobre el activo (versiones, elementos donde se encuentra instalado), obtenido a través de una herramienta que vuelca al servidor su configuración completa. Por otro lado, para algunos activos esa captura es manual. Al igual que sucedía en el *hardware* esto implica una disminución de la fiabilidad.

16) El Ayuntamiento no efectúa una revisión del *software* instalado para la detección de anomalías pero dispone de un procedimiento de autorización de software o de acceso a aplicaciones/servicios a partir de las herramientas anteriormente citadas. En el procedimiento no se describe nada referente al mantenimiento y gestión del *software,* como tampoco la forma de proceder en cuanto a las actualizaciones de los equipos.

17) La existencia de ese inventario para la mayoría de los equipos de la entidad, permite conocer la existencia de *software* fuera de soporte, pero no cuenta con documentación o procedimientos 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 Segovia ha implantado medidas para impedir la instalación de *software* no autorizado, no proporcionando privilegios de administrador a los usuarios, salvo en excepciones que deben ser abordadas lo antes posible porque supone una brecha de seguridad que debe ser controlada.

    Se realizan inspecciones periódicas del *software* instalado, contando para ello 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* pero de manera muy excepcional.

21) El proceso de gestión de inventario de *software* autorizado y no autorizado alcanza un índice de madurez L1, en el que "*las organizaciones no disponen de un ambiente estable para la prestación del servicio requerido. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible*". 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 Segovia sí cuenta con una política de alerta ante posibles incidencias de seguridad. 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. 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* esté fuera de soporte ni haya un procedimiento claro en los casos en que no sea posible la actualización automática.

    El riesgo de que una vulnerabilidad crítica sea pasada por alto y cree una ventana de oportunidad para un ataque es elevado.

23) La aplicación de los parches y actualizaciones en los elementos críticos sigue un procedimiento establecido, aunque no formalizado ni documentado, 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.

24) 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 nivel de madurez L1: "*En el nivel L1 de madurez, las organizaciones no disponen de un ambiente estable para la prestación del servicio requerido. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible".* Se confía en que las actualizaciones de los fabricantes solventarán todas las vulnerabilidades y que, además, se aplicarán sin demora, pero no se conoce el estado real al no utilizar herramientas de escaneo de vulnerabilidades.

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

25) Existe un procedimiento específico aprobado donde se definen las acciones a llevar a cabo para controlar el acceso a los sistemas. La entidad dispone de documentación para la creación de nuevos usuarios del sistema pero no existe nada particularizado para usuarios administradores. No se han definido políticas homogéneas para los sistemas de autenticación, ni para el uso dedicado de las cuentas de administración. Esta carencia propicia fallos de seguridad potencialmente relevantes.

26) No se mantienen en los dispositivos de la entidad cuentas genéricas. En los equipos de usuario se lleva a cabo esa supresión, pero no hay un procedimiento establecido que marque estas acciones, con lo que quedará sujeta al criterio profesional de los técnicos que realizan la instalación.

27) Se utilizan identificadores diferentes para poder acceder como usuario o administrador en función de las tareas que quiera realizar. Así se pueden elevar los permisos si tiene que realizar tareas concretas para luego volver al perfil de usuario.[4]

28) La práctica de contraseñas es adecuada en cuanto a generación de contraseñas robustas, así como en una serie de medidas para proteger dichas contraseñas; pero es necesario llevar a cabo medidas complementarias en ciertos elementos.

29) 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 establecida ninguna pauta respecto a su revisión con una determinada periodicidad y 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.

30) El Ayuntamiento dispone de un Sistema de gestión de información y eventos de seguridad, que le permite analizar y buscar correlaciones en los *logs* de la

[4] Párrafo modificado en virtud de alegaciones.

organización posibilitando una visualización de paneles de alertas e incidencias, aunque quedan por definir mediante un procedimiento aquellos aspectos que posibiliten una gestión más adecuada.

31) En el proceso para el control del uso de privilegios administrativos, el Ayuntamiento alcanza un índice de madurez L1, en el que "*las organizaciones no disponen de un ambiente estable para la prestación del servicio requerido. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible*".

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

32) El Ayuntamiento no realiza un proceso de configuración segura en los sistemas que administra directamente, ni consta la exigencia de su realización a las empresas de mantenimiento contratadas. A pesar de no seguir un procedimiento claro, las pruebas muestran que sí se siguen algunas pautas, aunque de manera insuficiente.

Los resultados de las pruebas realizadas indican que no existen disparidades en cuanto al seguimiento de normas para su bastionado resultando valores bastante bajos en los equipos analizados, provocando configuraciones inseguras.

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, las organizaciones no disponen de un ambiente estable para la prestación del servicio requerido. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible*".

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 Segovia 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 Sistema de gestión de información y eventos de seguridad 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 se encuentra desplegada la sonda individual SAT-INET, proporcionada por el Centro Criptológico Nacional 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 "*existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos*".

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

39) Existe un proceso definido y formalizado para la realización de copias de seguridad, aunque parte de su alcance y especificaciones más detalladas necesitan ser mejor definidos. El Ayuntamiento dispone de las herramientas adecuadas y el proceso se ejecuta correctamente.

40) En lo que respecta a la realización de pruebas de recuperación programadas, si están previstas en el procedimiento definido, pero no existe ningún registro que marque su realización. Sí se hacen recuperaciones a demanda. Se define la sistemática de recuperación, incluyendo cómo se debe solicitar y la manera en que se entrega al solicitante la copia, pudiéndose verificar que se sigue correctamente.

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 "e*xisten procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos".*

III.9. CUMPLIMIENTO NORMATIVO (CBCS 8)

43) El Ayuntamiento de Segovia dispone de una política de seguridad formalmente aprobada con fecha 9 de noviembre de 2023. En dicha política se precisan de manera adecuada los objetivos y se marca de manera adecuada el marco legal y regulatorio en el que se desarrollarán las actividades, conforme a lo reflejado en el Art.12 del Esquema Nacional de Seguridad.

44) El Ayuntamiento no dispone de una declaración de aplicabilidad, salvo en lo aplicable a la sede electrónica, donde se determinan la relación de las medidas del Esquema Nacional de Seguridad que son de aplicación al sistema, conforme a lo determinado en el Art. 28 del mencionado Esquema aunque se encuentra trabajando en su realización.

45) El Ayuntamiento de Segovia cumple con las especificaciones contenidas en los artículos 31 y 38 del Esquema Nacional de Seguridad, objeto de la presente fiscalización, para el sistema de información que comprende la sede electrónica. En cuanto a lo que respecta al artículo 32 del Esquema Nacional de Seguridad ha cumplido con las especificaciones contenidas, que han sido objeto de revisión en esta fiscalización, aunque tiene margen de mejora que se potenciaría con la extensión del cumplimiento de los citados artículos al resto de sistemas de información.

46) El proceso de adaptación a la normativa en materia de protección de datos está bastante avanzado. En ese sentido se enmarca el nombramiento del delegado de protección de datos con fecha el 12 de junio de 2020. Por otro lado, se dispone de un Registro de actividades de tratamiento, pero en cuanto al análisis de riesgos de los tratamientos considerados de alto riesgo, no tenemos ninguna aportación por parte del Ayuntamiento, salvo el referente a la huella dactilar, que está suspendido actualmente, y, por tanto, tampoco se ha podido evaluar si existen estos tratamientos, ni en ese caso, hacer con carácter previo, una evaluación del impacto de protección de datos. Esta situación no es conveniente y si bien se están realizando actuaciones en el buen sentido se espera que tengan continuidad en cuanto a los tratamientos considerados de alto riesgo.

47) No se ha cumplido lo establecido en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas, al no realizar la auditoría de sistemas anual del Registro Contable de Facturas.

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

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

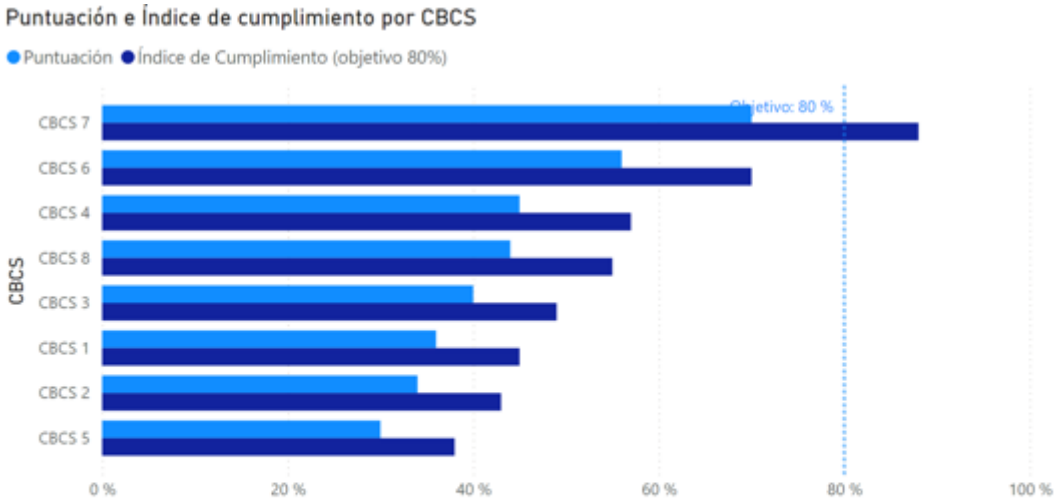
49) El Ayuntamiento está trabajando en la adaptación al nuevo Esquema Nacional de Seguridad siguiendo el plan de adecuación elaborado. Dicho plan se está desarrollando, partiendo de la certificación de la conformidad con el Esquema Nacional de Seguridad obtenida en 2023, así como otros aspectos tales como la gestión y monitorización por parte de un Centro de Operaciones en Seguridad o la utilización de un Sistema de gestión de información y eventos de seguridad. Es necesario continuar avanzando en la adaptación de los

sistemas de información y en la implementación de las medidas definidas en el nuevo Esquema Nacional de Seguridad.

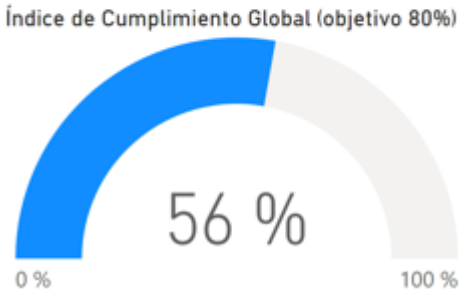
III.11. SITUACIÓN GLOBAL DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD

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 n.º 1.- Puntuación e Índice de cumplimiento por CBCS[5]



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



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

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

[5] Gráfico modificado en virtud de alegaciones

IV. RECOMENDACIONES

Con carácter general:

1) El Alcalde por razón de la materia 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 Centro Criptológico Nacional, la Federación Española de Municipios y Provincias o la Agencia Española de Protección de Datos publican guías detalladas que ofrecen modelos completos para la adaptación de los ayuntamientos de características similares al de Segovia 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 alguna de las plazas relevantes que conforman en entorno de Tecnologías de la Información de la entidad, con el fin de solventar aquellos aspectos técnicos que precisan mejoras y establecer estrategias adecuadas con una diferenciación de responsabilidades.

   - Dotar de los recursos necesarios al Servicio de Sistemas y Tecnologías de la Información, poniendo especial énfasis en regularizar situaciones de puestos especialmente relevantes para la organización.

   - Específicamente, se debería culminar el proceso mediante la realización de auditorías o autoevaluaciones de cumplimiento del Esquema Nacional de Seguridad, 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 relación de puesto de trabajo 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/cloud* adoptado.

4) El responsable de seguridad que se ha definido en la política de seguridad debe garantizar que existe una documentación suficiente del entorno de Tecnologías de la Información del Ayuntamiento para asegurar que el conocimiento sobre los sistemas

de información está disponible con independencia de las personas que formen el Servicio de Tecnologías de la Información.

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 debe participar juntamente con el responsable del sistema, en las decisiones que conllevan el empleo de herramientas automatizadas para la detección de vulnerabilidades.

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 Esquema Nacional de Seguridad.

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 declaración de aplicabilidad, de acuerdo con lo especificado en el artículo 28 del Esquema Nacional de Seguridad.

9) El Alcalde debería requerir al delegado de protección de datos que supervise el cumplimiento del Reglamento General de Protección de Datos, 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 24 del Esquema Nacional de Seguridad, 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.

11) La Intervención Municipal debería realizar la auditoría anual de sistemas del registro contable de facturas. Para facilitar su cumplimiento, la Intervención General de la Administración del Estado, publicó una guía marco que contiene una serie de orientaciones a efectos de su realización.

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

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.	

Control		Objetivo de control	Subcontroles	Medidas de seguridad del ENS
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.	