CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

SEGUIMIENTO DE RECOMENDACIONES Y ACTUALIZACIÓN DE LA SITUACIÓN DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE LA BAÑEZA (LEÓN)

PLAN ANUAL DE FISCALIZACIONES 2024

ÍNDICE

SIGLAS Y ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
Art.	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"*
DPD	Delegado de protección de datos
FEMP	Federación Española de Municipios y Provincias
GPF-OCEX	Guía práctica de fiscalización de los órganos de control externo
INE	Instituto Nacional de Estadística
ISSAI-ES	Normas Internacionales de las Entidades Fiscalizadoras Superiores
OCEX	Órganos de Control Externo Autonómicos
PPT	Pliego de Prescripciones Técnicas
PSI	Política de Seguridad de la Información
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*"
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.

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 2º 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 *Seguimiento de recomendaciones y actualización de la situación de la seguridad informática del Ayuntamiento de La Bañeza (León)*.

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 COMUNITARIA

- 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) 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 la actualización de la situación de los controles básicos de ciberseguridad en relación con la revisión realizada en el ejercicio 2021 y la comprobación de implantación de las medidas recomendadas en la fiscalización anterior.

Se han analizado las actuaciones, medidas y procedimientos adoptados desde la anterior auditoría para adoptar estas recomendaciones de manera que permitan garantizar la efectiva implantación de los controles básicos de ciberseguridad.

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

1. Proporcionar una reevaluación sobre el diseño y la eficacia operativa de los controles básicos de ciberseguridad, verificando hasta qué punto las mejoras realizadas han podido solventar aquellas deficiencias que pudieran 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 para continuar con la mejora.

II.2. ALCANCE

Este Informe tiene como ámbito subjetivo de manera específica, el Ayuntamiento de La Bañeza (León).

Este ayuntamiento, con una población de 10.023 habitantes (INE a fecha 1 de enero de 2024), En el anexo de personal que figura en la última cuenta general rendida, existen 74 puestos de trabajo. En cuanto a la estructura organizativa de la Entidad a nivel político y administrativo, dispone de los órganos necesarios previstos en la Ley (Pleno y Junta de Gobierno Local). El Pleno lo integran diecisiete concejales pertenecientes a cinco grupos políticos y un concejal no adscrito.

El tamaño de este tipo de municipios “que implica cierta complejidad de gestión” contrasta con las escasas dotaciones de recursos humanos y materiales dedicados a su área tecnológica.

Sin embargo, los ayuntamientos han 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, han sufrido una transformación digital que debe hacerse cumpliendo unos requisitos mínimos de seguridad en sus sistemas de información, al ser estos 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 la 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 objeto de fiscalización, se incluyen aquellos que fueron objeto de la anterior auditoría, salvo que la existencia de cambios relevantes en el entorno tecnológico aconseje otra delimitación.

El ámbito temporal de la fiscalización alcanza a la situación existente en el año 2024, y las actuaciones realizadas desde la anterior auditoría.

La fiscalización, de manera genérica, se refiere al estado de la seguridad de la información en el ayuntamiento, siendo esta una materia muy amplia, circunscribiéndose esta auditoría -operativa- a la verificación de las actuaciones, medidas y procedimientos adoptados para la implantación de los controles básicos de ciberseguridad y su grado de eficacia.

Una revisión completa de todos los aspectos relativos a la seguridad de la información de una entidad incluye un conjunto muy amplio de controles y aspectos a revisar, lo que requiere de un alto grado de dedicación, por parte del ente auditado y del organismo que audita.

Sin embargo, siguiendo el criterio de la GPF-OCEX 5313[1] 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 6 primeros controles críticos de ciberseguridad como básicos, y siguiendo este criterio de clasificación, la guía GPF-OCEX 5313 opta por establecer como Controles Básicos de Ciberseguridad (CBCS) estos 6 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.

[1] Guía práctica de fiscalización de los OCEX 5313 *"Revisión de los controles básicos de ciberseguridad"*.

Finalmente se incluye un octavo control, el de legalidad básica, incluyendo la verificación del cumplimiento de una serie de normas elementales de seguridad de la información.

Las áreas de trabajo por lo tanto coincidirán con cada uno de los 8 CBCS, y se exponen a continuación, en conjunción con los objetivos de la auditoría anteriormente expuestos.

En este sentido, la revisión se centrará en aquellos aspectos que hayan sufrido alguna modificación desde la revisión realizada anteriormente, y se realizará una nueva valoración que permita cuantificar la mejora que se haya producido.

Para ello se reevaluará el resultado obtenido para cada uno de los CBCS detallados en las áreas de trabajo según el modelo de madurez de procesos CMM *(Capability Maturity Model)*, ampliamente utilizado para caracterizar la implementación de un proceso y que también es el propuesto por la GPF-OCEX 5313.

Los resultados detallados de la auditoría contendrán previsiblemente información de carácter confidencial y cuya difusión puede afectar negativamente a la seguridad de los sistemas de información de la entidad auditada, por lo que en ningún caso serán objeto de publicación. Únicamente se publicará el detalle de resultados en lo referente al seguimiento de las recomendaciones del informe anterior.

La GPF-OCEX 5313 se basa en el 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. Esta norma está derogada, y los sistemas que estaban sometidos a la misma deben estar ya adecuados al nuevo ENS contenido en el Real Decreto 311/2022, de 3 de mayo.

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, las más relevantes son 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, por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Así, de acuerdo con la Disposición transitoria única, los sistemas de información del ámbito de aplicación del Real Decreto 311/2022, preexistentes a su entrada en vigor, disponían de veinticuatro meses para alcanzar su plena adecuación al nuevo ENS. Teniendo en cuenta que la publicación del nuevo ENS se produjo el 4 de mayo de 2022, el periodo transitorio expiró el 5 de mayo de 2024.

Valorando la situación descrita, las valoraciones que contiene la GPF-OCEX 5313 tendrán en cuenta las posibles adaptaciones a la nueva normativa.

1) Inventario y control de dispositivos físicos

El objetivo de esta área es verificar si se gestionan activamente (inventariando, revisando y corrigiendo) todos los dispositivos *hardware* de la red, de forma que solo los dispositivos autorizados tengan acceso a la red.

Se ha comprobado si la entidad auditada:

- 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.

2) 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.

Se ha comprobado 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.

3) 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:

- Existe 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 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.

4) 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?

5) 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 riguroso, 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.

6) 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.

- 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.

7) 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 periódicamente 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.

8) Cumplimiento normativo

Las recomendaciones realizadas en el informe anterior precisaban para su implicación de un impulso por parte de la corporación, siendo el alcalde el máximo responsable.

Se ha revisado la aplicación efectiva de estas recomendaciones y en concreto si la corporación ha adoptado medidas para la aprobación de un plan estratégico en materia de tecnologías de la información que incluya planificación, dotación de recursos y plazos para la aprobación de las normativas en materia de seguridad obligatorias, la subsanación de las deficiencias de carácter técnico detectadas y la realización del proceso de certificación del ENS.

En lo que se refiere a la normativa se han revisado los siguientes aspectos:

- 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 en los casos en que se aplica.
  - 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 si:
  - 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 en el Sector Público):
  - Se ha verificado si se ha realizado la auditoría de sistemas anual del Registro Contable de Facturas.

9) 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 ha asignado, 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. 1. 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 ha evaluado cada uno de ellos utilizando el modelo de madurez de procesos para evaluar 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 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.
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 ha tenido 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 ha evaluado el índice de cumplimiento sobre el nivel requerido, que será, de acuerdo a 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 auditoría), se ha evaluado de acuerdo a 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 ha hecho 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 han evaluado 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 es la media de los resultados de los subcontroles que lo forman.

Es preciso considerar por tanto 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.

No existe documentación de la mayoría de los procedimientos analizados, por lo que la información que sirve de base a las verificaciones realizadas procede de los cuestionarios cumplimentados por las entidades fiscalizadas y de las entrevistas realizadas.

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 Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica, apartado 16 para la 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 12 septiembre de 2025.

II.3. LIMITACIONES

El ayuntamiento fiscalizado ha mantenido una actitud de colaboración.

El Consejo de Cuentas quiere destacar la disponibilidad y colaboración del ayuntamiento a través del interlocutor designado para esta fiscalización, y del personal del ayuntamiento, 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 fue remitido al Ayuntamiento de La Bañeza el 3 de octubre de 2025, para que en un plazo de 15 días naturales formularan alegaciones. Concluido el plazo, el ente fiscalizado no ha realizado alegación alguna.

III. CONCLUSIONES

1) El ayuntamiento sigue careciendo de una estrategia de TI, y no ha establecido una gobernanza adecuada que le permita afrontar con garantías el proceso de dotar a sus sistemas de información de un nivel de seguridad suficiente.

   La estructura de TI es inexistente y durante el periodo trascurrido, no se ha tomado ninguna actuación para adecuar la organización del ayuntamiento a las necesidades que impone la transformación digital.

2) Con fecha 1 de septiembre de 2025 se ha realizado una contratación con carácter temporal para dotar al ayuntamiento con un recurso especializado. No obstante, siendo un paso necesario, es provisional y no supone todavía un cambio organizativo relevante.

3) Las actuaciones tecnológicas para cumplir con las recomendaciones realizadas se concretan en:

   - Cambios en el proceso de copias de seguridad. Se añade un almacenamiento en la nube que podría redundar en una mejora de su protección.

   - Actuaciones de renovación tecnológica para solucionar la obsolescencia de determinados elementos de los sistemas.

4) Se mantiene la situación por la que el Ayuntamiento de La Bañeza cuenta con apoyo específico en materia de administración electrónica, nóminas, padrón y gestión presupuestaria, a través la Diputación de León.

5) En el periodo transcurrido, no se ha adoptado un compromiso firme con la seguridad informática, especialmente relevante en lo que se refiere a la falta de aprobación de la política de seguridad como paso fundamental para iniciar el proceso de adaptación al ENS, a pesar de encontrarse muy avanzada en la anterior revisión. Dado el tiempo trascurrido y las novedades normativas, el borrador existente debe ser objeto de revisión en profundidad.

6) Con respecto a los procesos de inventario y control de *hardware* y *software*, (CBCS 1 y CBCS 2), se ha mantenido el proceso manual existente, pero se han dejado de aplicar de manera consistente algunas medidas, lo que ha afectado a la valoración del control cobre el *software* instalado, bajando el resultado en el control CBCS 2.

   Ambos controles siguen estando en el nivel de madurez L1 donde *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.*

7) En lo referente a la identificación y corrección de vulnerabilidades, uso controlado de privilegios administrativos, configuración segura y registro de actividad de los usuarios (CBCS 3, CBCS 4, CBCS 5 y CBCS 6), no hay ninguna actuación relevante

desde la anterior auditoría, y continúan teniendo la misma puntuación y nivel de madurez que ya tenían, que se corresponde con:

- L0 para los controles 3 y 6, *no existe un proceso que soporte el servicio requerido*.

- L1 para los controles 4 y 5, *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*.

8) Con respecto al CBCS 7, la situación es similar a la existente en la anterior auditoría, siendo el único cambio la introducción de una copia adicional en la nube, lo que podría redundar en una mejor protección de las copias. Sin embargo, al no disponer del contrato con las condiciones del servicio, no se ha valorado su efecto en la implantación del control.

   Al igual que en la auditoría anterior, sigue sin existir un procedimiento claro para la realización de las copias, pero se comprueba que efectivamente se realizan en los sistemas relevantes que instalados *on-premise*. No se hacen pruebas de recuperación completas y periódicas, ni se aplican medidas suficientes para la protección de las copias.

   Con respecto a los sistemas en la nube proporcionados por la Diputación de León, al no disponer para su revisión de una versión actualizada de los convenios para su uso, se mantiene igualmente la situación anterior, en que se presupone que estas copias se realizan, pero no hay un instrumento que permita asegurarlo.

   El control continúa sin cambios en su valoración en el nivel L1, donde *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*.

9) Con respecto al CBCS 8, el resultado de la evaluación del control de manera global es similar a la anterior, ya que:

   - El ayuntamiento sigue incumpliendo de manera generalizada la normativa en materia de seguridad de la información. No se ha avanzado en la aprobación de la política de seguridad que se encontraba muy avanzada, y por tanto ha quedado desactualizada y debe revisarse íntegramente de nuevo antes de poder continuar con su aprobación.

   - En lo que respecta a la normativa en materia de protección de datos, se ha retrocedido con respecto a la situación anterior al prescindir de la contratación que permitía contar con un DPD y no revisarse el RAT en este periodo.

- No obstante, 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 realizando la auditoría de sistemas anual del Registro Contable de Facturas al menos en los dos ejercicios anteriores.

Debido al efecto compensatorio del tercer subcontrol, continúa un nivel de madurez L1, que implica la existencia de incumplimientos generalizados de la normativa y la carencia de actuaciones en marcha o con una planificación firme dirigidas a corregir la situación.

10) El Ayuntamiento de La Bañeza, como se puso de manifiesto en la anterior auditoría, se encontraba en una situación muy vulnerable frente a riesgos informáticos. la entidad continua prácticamente en la misma situación, que se corresponde a un índice de madurez L1, sin que se hayan realizados actuaciones para revertir la situación en el periodo transcurrido entre auditorías. Es preciso un impulso importante para conseguir un nivel de seguridad adecuado y garantizar el cumplimiento de la normativa de aplicación.

Gráfico 1. Situación de cada control (Evolución 2021-2024)

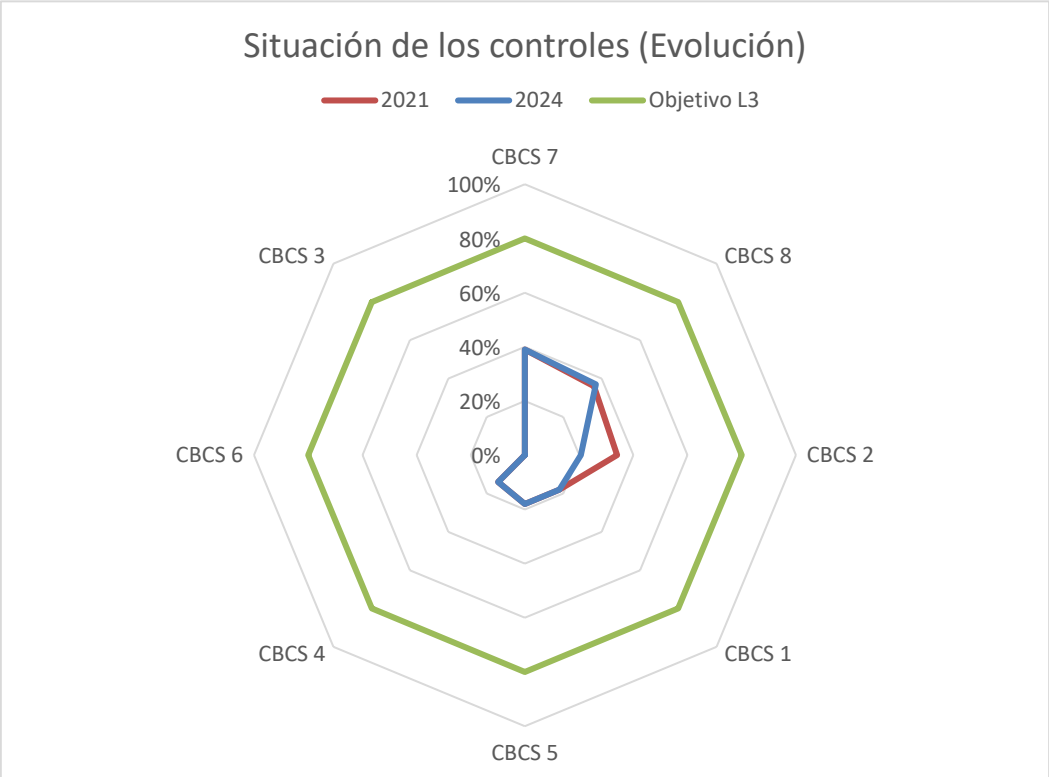
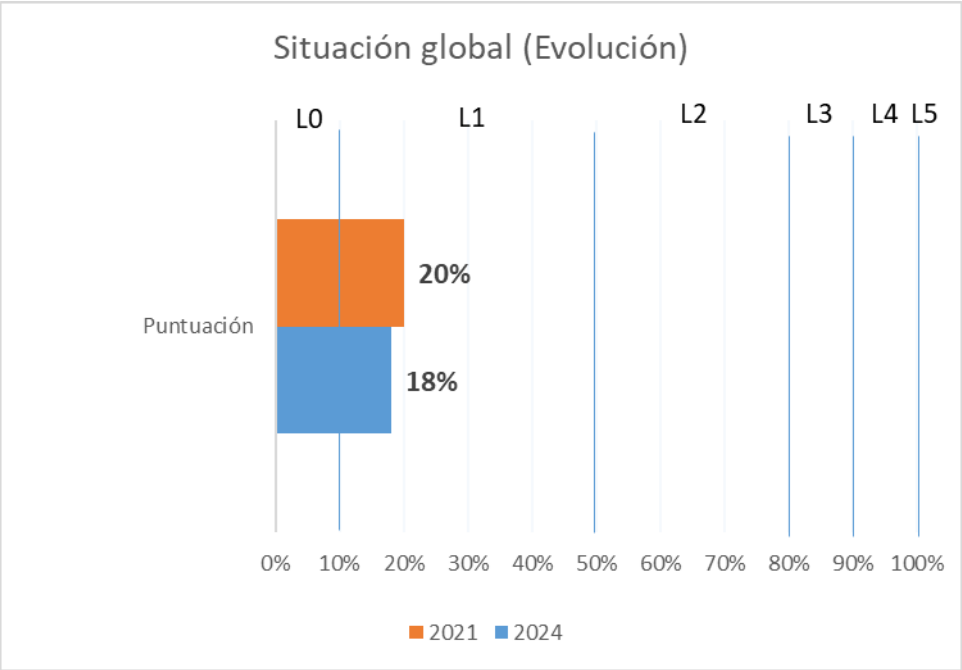


Gráfico 2. Madurez global de los controles (Evolución 2021-2024)



IV. RECOMENDACIONES

1) El alcalde debería impulsar, de manera decidida y continuada, las actuaciones para acometer, inmediatamente, la adecuación del ayuntamiento al ENS y la LOPDGG, para que el ayuntamiento alcance un nivel de ciberseguridad adecuado.

2) De manera específica, el alcalde debería:

   - Asignar los roles y responsabilidades, implantando una gobernanza de ciberseguridad que garantice que el proceso de adaptación se llevará a cabo en un plazo determinado y tendrá la continuidad imprescindible para garantizar que se alcanza el objetivo y que se mantiene a largo plazo.

   - Aprobar la normativa en materia de seguridad de la información y protección de datos personales necesaria.

3) El alcalde debería asegurar la dotación de recursos materiales y humanos imprescindibles para alcanzar un nivel de seguridad acorde al uso intensivo y la relevancia que suponen los sistemas de información como soporte de los procesos fundamentales en la gestión municipal.

   En concreto, debería asegurar que la relación de puestos de trabajo y el organigrama del ayuntamiento, al menos, contemple las funciones de tecnologías de la información de acuerdo con la importancia que estas tienen para el ayuntamiento.

4) El alcalde, dada la relevancia que las aplicaciones proporcionadas por la Diputación de León y las contrataciones externas tienen para la gestión municipal, debería asegurar que los convenios y contratos en los que se basa su utilización están actualizados y contienen las previsiones que exige el ENS para estos casos.

V. RESULTADOS DE LA FISCALIZACIÓN

V.1. SEGUIMIENTO DE RECOMENDACIONES

A continuación, se detalla en qué medida el ayuntamiento ha aplicado las recomendaciones del Consejo de Cuentas realizadas en el informe "ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE LA BAÑEZA (LEÓN)" cuyos trabajos de campo finalizaron en abril de 2021.

V.1.1. RECOMENDACIÓN 1

La primera recomendación que se realizó y que se pasa a analizar es la siguiente: *El concejal competente por razón de la materia debe 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 La Bañeza que pueden ser tomadas como referencia para facilitar el proceso.

En la actualidad no existe una delegación de competencias en materia de TI, por lo que se asumen directamente por la alcaldía.

No constan actuaciones para solventar la situación de vulnerabilidad del ayuntamiento y promover la mejora de la seguridad informática.

1. No existe una estructura de TI en el organigrama del ayuntamiento, no se contemplan en la RPT plazas dedicadas a estas tareas ni tampoco existía, en el momento de iniciar la fiscalización, personal que las asuma.

   La situación en la anterior auditoría ya era precaria, con una sola persona que se ocupaba de esas funciones y que ya no está en el ayuntamiento. La solución adoptada en este periodo, mediante la contratación de una empresa externa para contar con el apoyo puntual de un técnico, deja al ayuntamiento en una situación más desfavorable que antes, dado que supone perder el único recurso interno que mantenía un control y el conocimiento de los Sistemas de Información que utiliza el ayuntamiento.

   Con fecha 1 de septiembre de 2025 se ha contratado a una persona, con carácter temporal, para realizar las tareas que venía desarrollando la empresa contratada. Aunque se trata de un paso necesario, sigue siendo provisional y no implica un cambio en cuanto a la relevancia e integración de la TI en la estructura del ayuntamiento que se precisa.

2. No hay evidencia de que se hayan asumido las responsabilidades en materia de seguridad de la información que determina el ENS por parte de los responsables municipales.

3. No se ha aprobado la política de seguridad de la información que se encuentra publicada en el portal de transparencia desde la anterior auditoría.

4. En cuanto a las actuaciones técnicas realizadas, el ayuntamiento únicamente ha referido actuaciones puntuales de renovación tecnológica y una mejora en la protección de las copias de seguridad, al contratar un servicio de copias en la nube.

5. Se mantiene la situación por la que el Ayuntamiento de La Bañeza cuenta con apoyo específico en materia de administración electrónica, nóminas, padrón y gestión presupuestaria, a través la Diputación de León.

6. Otros aspectos, especialmente en lo que se refiere a incumplimientos normativos, que ya fueron objeto de recomendación en 2021, y que resultan relevantes:

    - En materia de protección de datos, no hay constancia del nombramiento del DPD, ni de que se haya continuado con la contratación de la empresa que realizaba estas funciones con anterioridad, empeorando la situación con respecto a la existente en la anterior auditoría, incumpliendo aspectos básicos de la normativa.

    - Sin embargo, en lo referente al ENS, el proceso iniciado en la anterior auditoría con la elaboración y publicación del borrador de PSI se ha paralizado. Como consecuencia, el borrador no está ya adaptado a la normativa vigente y deberá ser objeto de una revisión en profundidad.

La recomendación no se ha aplicado, el ayuntamiento ha mostrado falta de atención continuada hacia la seguridad informática, evidenciada por la ausencia de una estrategia para la protección de sus sistemas, lo que refleja una carencia de compromiso institucional con la integridad tecnológica y la protección del ayuntamiento y por tanto del servicio prestado a los ciudadanos. En un contexto donde las amenazas cibernéticas son cada vez más frecuentes, resulta imperativo que el ayuntamiento adopte medidas concretas para garantizar la seguridad de sus sistemas de información.

V.1.2. RECOMENDACIONES 2, 3 Y 4

Las siguientes recomendaciones incluyen lo siguiente:

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:

- *Aprobar una política de seguridad que defina claramente las responsabilidades sobre la seguridad de los servicios que ofrece y la información que maneja, permitiendo dar continuidad al esfuerzo de adaptación necesario para el cumplimiento normativo.*

- *Dotar de recursos al departamento de TI para solventar aquellos aspectos técnicos que precisan mejoras.*

- *Específicamente, se deberá 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*.

3) Un aspecto básico y que permitirá comenzar a estructurar y documentar el proceso de seguridad informática debería ser el nombramiento por parte del Alcalde del responsable de la información, del responsable del servicio y del responsable de la seguridad. Con estos nombramientos y el apoyo y concienciación política al más alto nivel se podría proceder al desarrollo de la estructura y procedimientos necesarios.

4) El responsable de seguridad que se determine en la política de seguridad, en coordinación con el responsable del sistema para cada proceso de gestión de TI, debería elaborar y elevar a su aprobación formal el procedimiento que lo describe en el que se detalle el alcance, tareas a realizar, responsabilidades, registros o documentación que se genere, así como cualquier otro aspecto relevante del proceso en concreto.

Estas recomendaciones se realizaron en un contexto en el que el ayuntamiento había comenzado a dar pasos para establecer una gobernanza de TI, con un borrador de PSI muy avanzado, solo pendiente de aprobación final. Sin embargo, en el tiempo transcurrido, se ha retrocedido con respecto a la situación anterior y, por tanto, ninguna de estas recomendaciones ha podido ser llevaba a cabo al ser preciso previamente que se apruebe la PSI.

V.1.3. RECOMENDACIONES 5 Y 6

Las recomendaciones de la 5 en adelante, iban dirigidas a corregir aspectos técnicos concretos que se observaron durante la revisión de los controles en la anterior auditoría.

El contenido de las recomendaciones 5 y 6 es el siguiente:

Sobre el entorno tecnológico del ayuntamiento:

5) El Concejal competente por razón de la materia debería impulsar las acciones necesarias para que se apruebe una RPT que contemple 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 adoptado.

6) 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.

No consta ninguna modificación de la RPT para contemplar la función de TI en el ayuntamiento, ni un compromiso para su adecuación, más allá de la mera intención

manifestada por el ayuntamiento de abordar la situación en la próxima revisión que se realice, ni se ha nombrado un responsable de seguridad.

V.1.4. RECOMENDACIONES 7 Y 8

Sobre el proceso continuo de identificación y corrección de vulnerabilidades:

7) El responsable de seguridad que se defina en la política de seguridad debería valorar conjuntamente con el responsable del sistema, el empleo de herramientas automatizadas para la detección de vulnerabilidades y la realización (o contratación dado lo especializados de los perfiles necesarios) de pruebas de penetración (pentesting) y que simulan ataques reales (Red team).

8) El Concejal competente debería impulsar la inclusión en los contratos o convenios para la prestación de servicios informáticos, de las cláusulas que permitan realizar un control de cómo prestan, así como del uso de los privilegios de administración, de acuerdo a lo especificado en el ENS.

No consta ningún avance en este sentido.

V.1.5. RECOMENDACIÓN 9

Sobre el cumplimiento de la normativa en materia de protección de datos:

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

Anteriormente, el ayuntamiento contrataba a una empresa externa la función de DPD. Sin embargo, en la actualidad el ayuntamiento no ha aportado contratos en vigor formalizados con este objeto, ni el nombramiento del DPD.

Al no existir DPD, no se ha aplicado la recomendación, y el ayuntamiento empeora su situación con respecto a la auditoría anterior.

V.1.6. RECOMENDACIÓN 10

10) 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.

Se ha verificado que, durante al menos los dos últimos ejercicios, se ha realizado el informe requerido por la normativa, por tanto, la recomendación ha sido completamente aplicada.

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

Anexo I. 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 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.	