



**CONSEJO DE CUENTAS**  
**DE CASTILLA Y LEÓN**

**ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SANTA  
MARTA DE TORMES (SALAMANCA)**

---

## ÍNDICE

<b>I. INTRODUCCIÓN .....</b>	<b>5</b>
I.1. INICIATIVA DE LA FISCALIZACIÓN .....	5
I.2. MARCO NORMATIVO.....	5
I.2.1. NORMATIVA EUROPEA .....	5
I.2.2. NORMATIVA ESTATAL.....	6
I.2.3. NORMATIVA AUTONÓMICA .....	7
<b>II. OBJETIVOS, ALCANCE Y LIMITACIONES .....</b>	<b>7</b>
II.1. OBJETIVOS .....	7
II.2. ALCANCE.....	7
II.3. LIMITACIONES .....	18
II.4. TRÁMITE DE ALEGACIONES .....	19
<b>III. CONCLUSIONES .....</b>	<b>19</b>
III.1. ENTORNO TECNOLÓGICO Y SISTEMAS DE INFORMACIÓN OBJETO DE LA FISCALIZACIÓN.....	19
III.2. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS.....	20
III.3. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO Y NO AUTORIZADO (CBCS 2) .....	20
III.4. PROCESO CONTINUO DE IDENTIFICACIÓN Y CORRECCIÓN DE VULNERABILIDADES (CBCS 3) .....	21
III.5. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS (CBCS 4) .....	21
III.6. CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE DE DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES (CBCS 5).....	22
III.7. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS (CBCS 6).....	22
III.8. COPIAS DE SEGURIDAD DE DATOS Y SISTEMAS (CBCS 7).....	23
III.9. CUMPLIMIENTO NORMATIVO .....	23
III.10. SITUACIÓN GLOBAL DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD .....	24
<b>IV. RECOMENDACIONES.....</b>	<b>26</b>
<b>ÍNDICE DE CUADROS .....</b>	<b>28</b>
<b>ÍNDICE DE GRÁFICOS.....</b>	<b>29</b>
<b>ANEXOS .....</b>	<b>30</b>

## **SIGLAS Y ABREVIATURAS**

<b>AAPP</b>	Administración Pública/Administraciones Públicas
<b>AEPD</b>	Agencia Española de Protección de Datos
<b>APT</b>	Amenazas avanzadas persistentes del inglés “Advanced Persistent Threats”
<b>BBDD</b>	Bases de datos
<b>CBCS</b>	Controles básicos de ciberseguridad
<b>CCN</b>	Centro Criptológico Nacional
<b>CCN-CERT</b>	Servicio de Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional
<b>CCN-STIC</b>	Guías del Centro Criptológico Nacional sobre la seguridad de las tecnologías de la información y las comunicaciones
<b>CIPSA</b>	Centro informático provincial de Salamanca
<b>CIS</b>	Centro para la seguridad de Internet del inglés “ <i>Center for Internet Security</i> ”
<b>CMM</b>	Modelo de madurez de procesos del inglés “ <i>Capability Maturity Model</i> ”
<b>DPD</b>	Delegado de protección de datos
<b>EELL</b>	Entidades locales
<b>FEMP</b>	Federación española de municipios y provincias
<b>GPF-OCEX</b>	Guía práctica de fiscalización de los órganos de control externo
<b>INE</b>	Instituto Nacional de Estadística
<b>IP</b>	Protocolo de internet, del inglés “ <i>Internet Protocol</i> ”
<b>IRIA</b>	Informe sobre los Recursos Informáticos de las Administraciones públicas
<b>ISSAI-ES</b>	Normas Internacionales de las Entidades Fiscalizadoras Superiores
<b>LAN</b>	Redes con extensión física limitada, procede del inglés “ <i>Local Area Network</i> ”

<b>MAC</b>	Es la dirección física y única para cada dispositivo de red, proviene del inglés “ <i>Media Acces control</i> ”
<b>NAS</b>	Almacenamiento conectado a la red, del inglés “ <i>Network-attached storage</i> ”
<b>OCEX</b>	Órganos de Control Externo Autonómicos
<b>PAM</b>	La gestión de las cuentas con privilegios del inglés “ <i>Privileged Account Management</i> ”
<b>PCs</b>	Computadoras personales. Procede del inglés “ <i>Personal computers</i> ”
<b>Porc.</b>	Porcentaje
<b>RAT</b>	Registro de actividades de tratamiento
<b>SaaS</b>	Solución de software integral que se adquiere de un proveedor de servicios en la nube mediante un modelo de pago por uso. Procede del inglés “ <i>Software as a Service</i> ”
<b>SI</b>	Sistema de información
<b>SIEM</b>	Sistema de gestión de información y eventos de seguridad del inglés “ <i>Security Information and Event Management</i> ”
<b>SW</b>	Software
<b>TI</b>	Tecnologías de la Información
<b>TIC</b>	Tecnologías de la Información y de las Comunicaciones
<b>UE</b>	Unión Europea
<b>VPN</b>	Red privada virtual, del inglés “ <i>Virtual Private Network</i> ”
<b>VLAN</b>	Red de extensión física limitada, del inglés “ <i>Virtual Local Area Network</i> ”

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

## NOTA SOBRE ORIGEN DE DATOS

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

## **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 2021 del Consejo de Cuentas, aprobado por la Comisión de Economía y Hacienda de las Cortes de Castilla y León en su reunión del 11 de febrero de 2021 (publicado en el Boletín Oficial de Castilla y León, el 22 de febrero de 2021), la relativa al Análisis de la seguridad informática del Ayuntamiento de Santa Marta de Tormes (Salamanca).

### **I.2. MARCO NORMATIVO**

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

#### **I.2.1. NORMATIVA EUROPEA**

- El Reglamento (UE) 2014/910 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (RGPD).
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

### I.2.2. NORMATIVA ESTATAL

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL).
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- 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 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 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local. (RD 424/2017).
- 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.
- 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.

### I.2.3. NORMATIVA AUTONÓMICA

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

## **II. OBJETIVOS, ALCANCE Y 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, así como 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**

El Plan Anual de Fiscalizaciones para el ejercicio 2021 del Consejo de Cuentas, incluyó la realización del Análisis de la seguridad informática del Ayuntamiento de Santa Marta de Tormes (Salamanca).

Este Informe tiene como ámbito subjetivo de manera específica, el Ayuntamiento de Santa Marta de Tormes.

La población del municipio de Santa Marta de Tormes, según los datos oficiales del INE a fecha 1 de enero de 2020, es de 14.730 habitantes y tiene una plantilla media

de 70 empleados según datos de la última Cuenta General rendida. En cuanto a la estructura organizativa de la Entidad a nivel político y administrativo, según consta en las actas de las sesiones extraordinarias celebradas el 15 de junio y el 16 de julio de 2019, dispone de los órganos necesarios previstos en la Ley (Pleno y Junta de Gobierno Local). El Pleno lo integran dieciséis concejales pertenecientes a tres grupos políticos. Respecto a los órganos complementarios, se encuentran constituidas cuatro Comisiones Informativas permanentes.

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. Según pone de manifiesto el informe “*Las Tecnologías de la Información y las Comunicaciones en la Administración Local. Informe IRIA 2018*” que elabora periódicamente la Secretaría General de Administración Digital (SGAD), el gasto TIC de las administraciones locales representa un porcentaje de su presupuesto del 1,6 % en el caso de ayuntamientos entre 10.000 y 30.000 habitantes, lo que representa una cantidad notablemente inferior al 2,2 % del presupuesto que de media dedican las entidades locales.

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.

El informe IRIA 2018 revela también que la mitad de los ayuntamientos del estrato entre 10.000 y 30.000 habitantes, no han adoptado requisitos formales para proteger los datos de los ciudadanos, siendo esta una situación que debe ser objeto de atención por cuanto afecta gravemente a sus derechos, en lo que se refiere a la protección de sus datos personales, por un lado, y a la capacidad del ayuntamiento de prestarles servicio si sus sistemas se ven comprometidos, por otro.

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 todos aquellos de 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 ha realizado

la revisión de 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 2021, sin perjuicio de las comprobaciones correspondientes a actuaciones realizadas en años anteriores que sean necesarias para cumplir los objetivos.

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.

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, y 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.

Finalmente se incluye un octavo control (CBCS 8), el 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.

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.

Los resultados detallados de la auditoría contienen información de carácter confidencial y cuya difusión puede afectar negativamente a la seguridad de los sistemas de información del Ayuntamiento de Santa Marta de Tormes por lo que en ningún caso será objeto de publicación. Habrá de proporcionarse únicamente a la Entidad fiscalizada que será quien finalmente determine el uso y publicidad que es pertinente de acuerdo a la valoración que realice de la confidencialidad de su contenido.

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 señaladas en las Directrices técnicas, coincidentes con los ocho controles previstos en la Guía práctica de fiscalización, GPF-OCEX 5313 (siete controles básicos y una revisión de cumplimiento de diversas normas relacionadas con la seguridad de la información). En el Anexo I se incluye una tabla resumen de cada uno de los expresados controles y sus correspondientes subcontroles.

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

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

Se ha procedido a realizar una revisión inicial del entorno de TI de la Entidad, incluyendo la estructura de su departamento de TI.

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

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

#### 2. Inventario y control de dispositivos físicos.

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

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:

- 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 estas son resueltas en el tiempo previsto en el procedimiento.
- La Entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.

### 5. Uso controlado de privilegios administrativos.

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

Para ello, se ha respondido a las siguientes cuestiones:

- ¿Los privilegios de administración se limitan adecuadamente y la Entidad dispone de un inventario de cuentas de administración que facilita su correcto control?
- ¿Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares, se cambian antes de la entrada en producción del sistema?
- ¿Las cuentas de administración solo se utilizan para las tareas que son estrictamente necesarias?
- ¿Las cuentas de administración están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas?
- ¿El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas?

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

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

Para ello, se ha comprobado si:

- La Entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y aplicaciones.
- La Entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección en un periodo de tiempo oportuno.

7. Registro de la actividad de los usuarios.

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

Para ello se ha obtenido información sobre las siguientes cuestiones:

- El registro de auditoría está activado en todos los sistemas y dispositivos de red y contiene el detalle suficiente para la detección, análisis, investigación y prevención de ataques.
- Los registros se conservan durante el tiempo indicado en la política de retención, de forma que se encuentran disponibles para su consulta y análisis

y además durante dicho periodo, se garantiza que no se producen accesos no autorizados.

- Los registros de todos los sistemas son revisados periódicamente para detectar anomalías y posibles compromisos de la seguridad del sistema y si se dispone de mecanismos para la centralización de estos registros de auditoría, de forma que se facilite la realización de las revisiones.
- Para sistemas de categoría ALTA, si la Entidad dispone de un SIEM (*Security Information and Event Management*) o una herramienta de analítica de registros de actividad para realizar correlación y análisis de estos datos.

#### 8. Copias de seguridad de datos y sistemas.

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

Para su consecución, se ha verificado si:

- La Entidad realiza copias de seguridad automáticas y periódicas de todos los datos y configuraciones del sistema.
- Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.
- Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.

#### 9. Cumplimiento normativo.

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

- Con respecto al cumplimiento del ENS, se ha verificado si:
  - Existe una política de seguridad y responsabilidades.
  - Se ha elaborado una declaración de aplicabilidad.
  - Se dispone del Informe de auditoría.
  - Se ha realizado el Informe del estado de la seguridad.

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

#### 10. Evaluación de los controles.

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

- Subcontroles.

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

**Cuadro 1: Valoración de los subcontroles**

Evaluación	Descripción
<b>Control efectivo</b>	<p>Cubre al 100% con el objetivo de control y:</p> <ul style="list-style-type: none"> <li>• El procedimiento está formalizado (documentado y aprobado) y actualizado.</li> <li>• El resultado de las pruebas realizadas para verificar su implementación y eficacia operativa ha sido satisfactorio.</li> </ul>
<b>Control bastante efectivo</b>	<p>En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100% y:</p> <ul style="list-style-type: none"> <li>• Se sigue un procedimiento formalizado, aunque puede presentar aspectos de mejora (detalle, nivel de actualización, nivel de aprobación, etc.).</li> <li>• Las pruebas realizadas para verificar la implementación son satisfactorias.</li> <li>• Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa, pero no son ni significativos ni generalizados.</li> </ul>
<b>Control poco efectivo</b>	<p>Cubre de forma muy limitada el objetivo de control y:</p> <ul style="list-style-type: none"> <li>• Se sigue un procedimiento, aunque este puede no estar formalizado.</li> <li>• El resultado de las pruebas de implementación y de eficacia no es satisfactorio.</li> </ul> <p>Cubre en líneas generales el objetivo de control, pero:</p> <ul style="list-style-type: none"> <li>• No se sigue un procedimiento claro.</li> <li>• Las pruebas realizadas para verificar la implementación o la eficacia operativa no son satisfactorias (se han detectado incumplimientos significativos, aunque no están generalizados).</li> </ul>
<b>Control no efectivo o no implantado</b>	<p>No cubre el objetivo de control.</p> <ul style="list-style-type: none"> <li>• 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).</li> </ul>

- 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 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.

Los niveles globales para cada control son:

**Cuadro 2: Valoración de los controles**

Nivel	Madurez (Porc.)	Descripción
<b>0- Inexistente</b>	0 %	Esta medida no está siendo aplicada en este momento.
<b>1 - Inicial / ad hoc</b>	10 %	<p>El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado.</p> <p>La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.</p>
<b>2 - Repetible, pero intuitivo</b>	50 %	<p>Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas, sin procedimientos escritos ni actividades formativas.</p> <p>La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.</p>
<b>3 - Proceso definido</b>	80 %	<p>Los procesos están estandarizados, documentados y comunicados con acciones formativas.</p> <p>Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.</p> <p>Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.</p>
<b>4 - Gestionado y medible</b>	90 %	<p>La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere.</p> <p>Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.</p> <p>En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.</p>

<b>5-Optimizado</b>	100 %	Se siguen buenas prácticas en un ciclo de mejora continua.
		El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.
		En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

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

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

<b>Categoría del Sistema</b>	<b>Nivel requerido</b>
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 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, 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 de forma telemática. Cuando se ha considerado preciso, atendiendo a las especiales circunstancias derivadas de las restricciones a la movilidad impuestas por la situación de emergencia sanitaria provocada por la COVID-19, dicha información ha sido completada mediante 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 a lo dispuesto en las Guías prácticas de fiscalización de los OCEX 5313 Revisión de los controles básicos de ciberseguridad, y 5330 Evaluación de las deficiencias de control interno detectadas. Supletoriamente se han aplicado las ISSAI-ES (Nivel III) aprobadas por la Conferencia de Presidentes de las Instituciones Autonómicas de Control Externo el 16 de junio de 2014.

Los trabajos desarrollados para la elaboración del presente Informe han finalizado en el mes de septiembre de 2021.

### **II.3. LIMITACIONES**

El Ayuntamiento designó como persona de contacto para la remisión de la información que se solicitara, así como para la realización de las pruebas pertinentes, a D. Javier Martín Tapia. El Consejo de Cuentas intentó repetidamente obtener la información por todos los medios disponibles sin éxito, siendo finalmente en el periodo de alegaciones cuando el Alcalde del Ayuntamiento solicitó que se realizaran las pruebas que hasta el momento no se habían podido realizar, dando las instrucciones oportunas dentro de su organización<sup>1</sup>.

2

---

<sup>1</sup> Párrafo modificado en virtud de alegaciones.

<sup>2</sup> Párrafos suprimidos en virtud de las alegaciones.

## **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 31 de agosto de 2021 al Ayuntamiento de Santa Marta de Tormes, para que en un plazo de 15 días naturales formulara alegaciones.

Dentro del plazo establecido se han recibido alegaciones, realizándose pruebas de auditoría en aplicación del Art. 26.5 del Reglamento de Organización y funcionamiento del Consejo de Cuentas.

## **III. CONCLUSIONES**

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

- 1) Las competencias del área de nuevas tecnologías recaen en el 4<sup>a</sup> Teniente de Alcalde, que se responsabiliza de entre otras áreas, “*nuevas tecnologías*”. De los trabajos realizados reflejados en las conclusiones siguientes no se deduce que esa concejalía ejecute una dirección política efectiva de la seguridad informática.
- 2) Según la relación de puestos de trabajo aprobada en sesión ordinaria celebrada por el Pleno el día 23 de diciembre de 2019, el Ayuntamiento de Santa Marta de Tormes no dispone de personal dedicado a las tecnologías de la información.
- 3) No se ha definido una estructura de TI en el Ayuntamiento para asumir las responsabilidades que le corresponden con respecto a la seguridad de los servicios que ofrece y la información que maneja, con independencia de si la gestión se asume con recursos propios o externalizados en empresas privadas o en otras administraciones.
- 4) A efectos de esta fiscalización, la interlocución con el equipo auditor ha sido asumida por personal de la empresa “*MT Comunicación*” que realiza las tareas de gestión de TI en el Ayuntamiento de Santa Marta de Tormes, reconociendo así el Ayuntamiento que no ejerce un control sobre la prestación, toda vez que los detalles sobre esta los desconoce, debiendo recurrir a la propia empresa para aportar la información solicitada<sup>3</sup>.
- 5) No ha sido posible obtener los detalles de los servicios que presta la empresa al no existir una contratación unificada de éstos, sino que se trata de una serie de contratos menores que se realizan periódicamente y también para cubrir las necesidades puntuales que van apareciendo, de los que, por su carácter de contrato menor, no se dispone de un pliego de prescripciones técnicas para su revisión, ni ha aportado el ayuntamiento detalle de los servicios que incluyen.

---

<sup>3</sup> Párrafo modificado en virtud de alegaciones.

- 6) El Ayuntamiento carece de documentación detallada de sus sistemas y procesos de gestión, estando la única información existente en manos de terceros, y al carecer de personal de TI tampoco tiene la experiencia y el conocimiento que puede aportar el capital humano.
- 7) El Ayuntamiento no ha realizado una identificación y categorización según el ENS de los sistemas de información de que dispone, 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.
- 8) Se ha optado por un modelo mixto, utilizando para procesos muy relevantes los servicios ofrecidos por la Diputación de Salamanca (administración electrónica, padrón y contabilidad), estando los servicios y la información que se presta, en algunos casos en la nube (modalidad *SaaS*) y en otros en local. La utilización de modelos en la nube simplifica la implantación de medidas de seguridad, pero requiere un control sobre la prestación del servicio, al no eximir en modo alguno al Ayuntamiento de la responsabilidad última. Los modelos en local requieren de la aplicación de medidas de seguridad más complejas para lo que es necesario disponer de recursos, humanos y materiales, suficientes.
- 9) Del examen de la estructura de la red del Ayuntamiento se concluye que en buena medida no existe una red corporativa como tal, sino un conjunto de equipos que comparte un acceso a internet y un grupo de trabajo, ya que no hay un servidor de ficheros o un dominio, sino únicamente recursos compartidos en un grupo de trabajo.
- 10) El Ayuntamiento facilita el teletrabajo a su personal mediante acceso por VPN y también gracias al sistema de administración electrónica en la nube (*SaaS*), que permite acceder de igual forma con independencia de la ubicación física.

### **III.2. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS**

- 11) No existe un inventario que permita un control adecuado de los activos *hardware*.
- 12) No se han implantado medidas efectivas para impedir la conexión de dispositivos físicos no autorizados<sup>4</sup>.
- 13) No existe el proceso de gestión de inventario y control de *hardware*, lo que corresponde al nivel L0 de madurez, que identifica “*un proceso inexistente o no aplicado en estos momentos*”.

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

- 14) El Ayuntamiento de Santa Marta de Tormes no dispone de un inventario de activos software, ni ha adoptado medidas efectivas para impedir el uso de software no

---

<sup>4</sup> Párrafo modificado en virtud de alegaciones.

autorizado, por lo que no existe control sobre qué software se utiliza, ni del estado de sus licencias ni del soporte del software.

- 15) El Ayuntamiento utiliza para sistemas de información muy relevantes, aplicaciones cuya contratación realiza bien Diputación de Salamanca (a través de CIPSA), bien el propio Ayuntamiento directamente, sin que se hayan previsto los medios de control que el ENS establece para el uso de proveedores externos<sup>5</sup>.
- 16) No existe un plan de mantenimiento de software ni de compra o adquisición de licencias, delegando por completo en la empresa de mantenimiento cualquier control, sin que el Ayuntamiento disponga al menos de un inventario de licencias, asumiéndose riesgos importantes asociados a la falta de soporte y uso inadecuado de licencias de software, con impacto potencial importante para el funcionamiento de la organización.
- 17) No existe el proceso de gestión de inventario de software autorizado, lo que corresponde al nivel L0 de madurez, que identifica “*un proceso inexistente o no aplicado en estos momentos*”.

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

- 18) El Ayuntamiento hace uso del software ofrecido por la Diputación en una parte relevante de sus sistemas de información, sin que por parte del Ayuntamiento se hayan previsto mecanismos que aseguren que se realiza el proceso de identificación y corrección de vulnerabilidades en tiempo y forma. Tampoco se introducen cláusulas en este sentido en las contrataciones que el Ayuntamiento realiza directamente<sup>6</sup>.

Con respecto al resto de elementos que el Ayuntamiento mantiene directamente, no realiza un proceso de identificación y corrección de vulnerabilidades sistemático, dependiendo únicamente de actuaciones puntuales de los técnicos. El riesgo de que una vulnerabilidad crítica permanezca sin corregir en sus sistemas y cree una ventana de oportunidad para un ataque es elevado<sup>7</sup>.

- 19) No existe el proceso de identificación y corrección de vulnerabilidades, lo que corresponde al nivel L0 de madurez, que identifica “*un proceso inexistente o no aplicado en estos momentos*”.

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

- 20) No existe un procedimiento para la realización de tareas como la gestión de usuarios administradores, el cambio de las contraseñas por defecto, ni se han

---

<sup>5</sup> Párrafo modificado en virtud de alegaciones.

<sup>6</sup> Párrafo modificado en virtud de alegaciones.

<sup>7</sup> Párrafo modificado en virtud de alegaciones.

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.

- 21) Hay un cierto control de las cuentas con privilegios administrativos de los sistemas más relevantes, aunque con un amplio margen de mejora<sup>8</sup>.
- 22) Los usuarios son administradores de sus equipos sin que se justifique la necesidad de tener esa condición.
- 23) No se han establecido contractualmente o por convenio mecanismos que permitan asegurar el buen uso y gestión de las cuentas de administración controladas por proveedores externos<sup>9</sup>.
- 24) En el proceso para el control del uso de privilegios administrativos el Ayuntamiento alcanza un índice de madurez L1, en el que *“el proceso existe, pero no se gestiona<sup>10</sup>”*.

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

- 25) El Ayuntamiento no realiza un proceso de configuración segura en los sistemas que administra directamente, lo que incluye todos los equipos de usuario y los servidores donde se instalan las aplicaciones del fabricante Wurth (Wintask SICAL y Padrón).
- 26) No se ha podido verificar la existencia de mecanismos que impidan cambios no autorizados o erróneos de la configuración, ni permitan su detección y su corrección en un periodo de tiempo oportuno.
- 27) No existe el proceso de configuración segura, lo que corresponde al nivel L0 de madurez, que identifica *“un proceso inexistente o no aplicado en estos momentos”*.

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

- 28) El Ayuntamiento no realiza ninguna acción específica para recoger, recopilar, proteger o analizar los registros de actividad de los usuarios, contando únicamente con los *logs* que por defecto o por parte de los proveedores externos, se encuentren activados en los sistemas.
- 29) No aporta un procedimiento formalizado que indique qué actividades serán objeto de registro, el periodo de retención, o la protección que se aplicará a los registros.

---

<sup>8</sup> Párrafo añadido en virtud de alegaciones.

<sup>9</sup> Párrafo modificado en virtud de alegaciones.

<sup>10</sup> Párrafo modificado en virtud de alegaciones.

La carencia de procedimiento impide asegurar tal y como establece el ENS, que el registro de actividad, donde se realice, se haga “*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*”.

- 30) No existe el proceso para el registro de la actividad de los usuarios, lo que corresponde al nivel L0 de madurez, que identifica “*un proceso inexistente o no aplicado en estos momentos*”.

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

- 31) No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento si describe una sistemática para su realización y se realizan en parte de los sistemas relevantes, disponiendo de herramientas para ello<sup>11</sup>.
- 32) No se realizan pruebas de recuperación completas y periódicas por lo que no es posible asegurar que las copias serán válidas en caso de necesitar una recuperación.
- 33) Se aplican medidas insuficientes para la protección de las copias de seguridad, siendo de especial relevancia la carencia de mecanismos de control en la contratación de las copias de seguridad en infraestructuras de terceros<sup>12</sup>.
- 34) 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 L1, en el que en el que “*el proceso existe, pero no se gestiona*”<sup>13</sup>.

### **III.9. CUMPLIMIENTO NORMATIVO**

- 35) El Ayuntamiento de Santa Marta de Tormes no aporta documentación que permita verificar que cumple con ninguno de los aspectos del ENS y de la normativa en materia de protección de datos personales revisados, con excepción del nombramiento del DPD.
- 36) El Ayuntamiento cumple con 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 realizar la preceptiva auditoría anual de sistemas del Registro Contable de Facturas<sup>14</sup>.
- 37) El resultado de la evaluación del control es un nivel de madurez L2, que implica que, aunque existen incumplimientos significativos en aspectos relativos al ENS y,

---

<sup>11</sup> Párrafo modificado en virtud de alegaciones.

<sup>12</sup> Párrafo modificado en virtud de alegaciones.

<sup>13</sup> Párrafo modificado en virtud de alegaciones.

<sup>14</sup> Párrafo modificado en virtud de alegaciones.

en menor medida, la LOPDGDD, se alcanza el objetivo en lo relativo al registro contable de facturas<sup>15</sup>.

### **III.10. SITUACIÓN GLOBAL DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD**

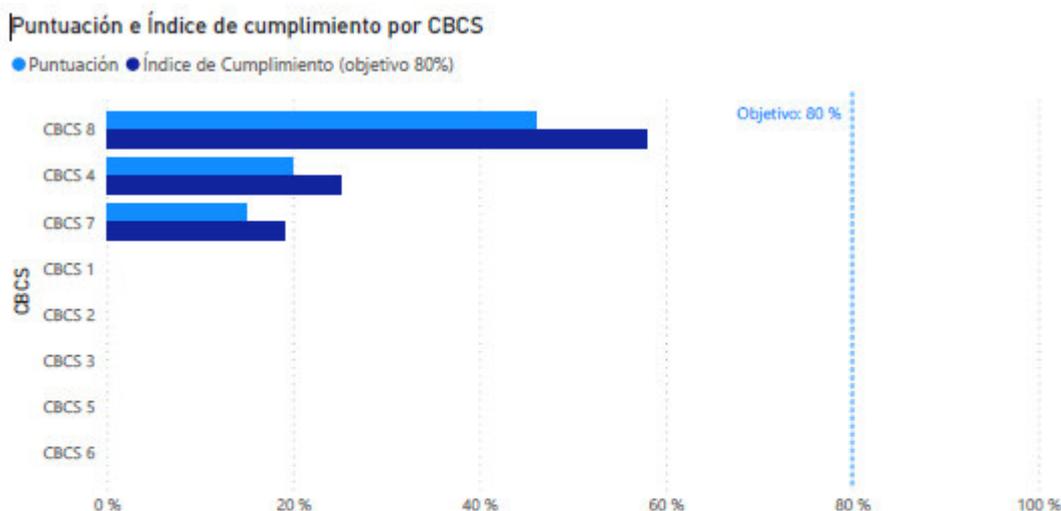
La situación global de los controles básicos de ciberseguridad se puede resumir en el siguiente gráfico donde se indica la puntuación alcanzada y el objetivo de cumplimiento para cada uno de ellos<sup>16</sup>.

---

<sup>15</sup> Párrafo modificado en virtud de alegaciones.

<sup>16</sup> Párrafo modificado en virtud de alegaciones.

Gráfico 1: Puntuación por CBCS<sup>17</sup>



CBCS	Descripción	Puntuación	Índice de Cumplimiento (objetivo 80%)
CBCS 8	Cumplimiento normativo	46 %	58 %
CBCS 4	Uso controlado de privilegios administrativos	20 %	25 %
CBCS 7	Copias de seguridad de datos y sistemas	15 %	19 %
CBCS 1	Inventario y control de dispositivos físicos	0 %	0 %
CBCS 2	Inventario y control de software autorizado y no autorizado	0 %	0 %
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	0 %	0 %
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	0 %	0 %
CBCS 6	Registro de la actividad de los usuarios	0 %	0 %
<b>Total</b>			<b>13 %</b>

Índice de Cumplimiento Global (objetivo 80%)



El nivel de madurez alcanzado globalmente por la entidad corresponde al nivel **L1**

El índice de cumplimiento (sobre un objetivo de madurez L3 que corresponde a una puntuación del 80%) es del **13%**.

<sup>17</sup> Gráfico añadido en virtud de alegaciones.

#### **IV. RECOMENDACIONES**

Se considera urgente que el Ayuntamiento impulse las siguientes actuaciones para revertir la situación en la que se encuentra:

- 1) <sup>18</sup>
- 2) El Interventor del Ayuntamiento debe comprobar el contenido y alcance de las contrataciones realizadas en materia de sistemas de información a los efectos de comprobar el cumplimiento de su contenido y alcance en el marco del ENS y de la Ley de Contratos del Sector Público en aplicación del RD 424/2017.
- 3) 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 Santa Marta de Tormes que pueden ser tomadas como referencia para facilitar el proceso.
- 4) 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.
- 5) 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 podrá proceder al desarrollo de la estructura y procedimientos necesarios.
- 6) 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,

---

<sup>18</sup> Párrafo suprimido en virtud de alegaciones.

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.

## **ÍNDICE DE CUADROS**

<b>Cuadro 1: Valoración de los subcontroles.....</b>	<b>15</b>
<b>Cuadro 2: Valoración de los controles.....</b>	<b>16</b>

## **ÍNDICE DE GRÁFICOS**

<b>Gráfico 1: Puntuación por CBCS .....</b>	<b>25</b>
---	-----------

## **ANEXOS**

<b>Anexo I. Detalle de controles y subcontroles.....</b>	<b>31</b>
--	-----------

**Anexo I. Detalle de controles y subcontroles**

Control	Objetivo de control	Subcontroles	Medidas de seguridad del ENS
<b>CBCS 1</b>	Gestionar activamente todos los dispositivos <i>hardware</i> en la red, de forma que solo los dispositivos autorizados tengan acceso a la red.	<p>CBCS 1-1: Inventario de activos físicos autorizados La entidad dispone de un inventario de activos físicos autorizados completo, actualizado y detallado.</p> <p>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.</p>	op.exp.1
<b>CBCS 2</b>	Gestionar activamente todo el software en los sistemas, de forma que solo se pueda instalar y ejecutar software autorizado.	<p>CBCS 2-1: Inventario de SW autorizado La entidad dispone de un inventario de SW completo, actualizado y detallado.</p> <p>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.</p> <p>CBCS 2-3: Control de SW no autorizado La entidad dispone de mecanismos que impiden la instalación y ejecución de SW no autorizado.</p>	op.exp.1 op.exp.2
<b>BCS 3</b>	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	<p>CBCS 3-1 Identificación. Existe un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que estas son identificadas en tiempo oportuno.</p> <p>CBCS 3-2 Priorización Las vulnerabilidades identificadas son analizadas y priorizadas para su resolución atendiendo al riesgo que suponen para la seguridad del sistema.</p> <p>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.</p> <p>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.</p>	mp.sw.2 op.exp.4
<b>CBCS 4</b>	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en	<p>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.</p> <p>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.</p>	op.acc.4 op.acc.5

Control	Objetivo de control	Subcontroles	Medidas de seguridad del ENS
	ordenadores, redes y aplicaciones.	<p>CBCS 4-3 Uso dedicado de cuentas de administración Las cuentas de administración solo se utilizan para las tareas que son estrictamente necesarias.</p> <p>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.</p> <p>CBCS 4-5 Auditoría y control El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.</p>	
<b>CBCS 5</b>	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.	<p>CBCS 5-1 Configuración segura La entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y SW</p> <p>CBCS 5-2: Gestión de la configuración La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o errores de configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.</p>	op.exp.2 op.exp.3
<b>CBCS 6</b>	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.  Registro de la actividad de los usuarios	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	op.exp.8 op.exp.10

Control	Objetivo de control	Subcontroles	Medidas de seguridad del ENS
<b>CBCS 7</b> 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.	<p><b>CBCS 7-1:</b> Realización de copias de seguridad La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.</p> <p><b>CBCS 7-2:</b> 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.</p> <p><b>CBCS 7-3:</b> 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.</p> <p><b>CBCS 8-1:</b> 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.</p>	mp.info.9
<b>CBCS 8</b> Cumplimiento normativo	Cumplimiento de determinados preceptos legales relacionados con la seguridad de la información	<p><b>CBCS 8-2:</b> 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).</p> <p><b>CBCS 8-3:</b> 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.</p>	