CONSEJO DE CUENTAS
DE CASTILLA Y LEÓN

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

CERTIFICO: Que el Pleno del Consejo de Cuentas de Castilla y León, en sesión celebrada el día 2 de noviembre de 2021, cuya acta está pendiente de aprobación, adoptó el Acuerdo 102/2021, por el que se aprueba el Informe "ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DEL AYUNTAMIENTO DE SANTA MARTA DE TORMES (SALAMANCA)", correspondiente al Plan Anual de Fiscalizaciones para el ejercicio 2021 y el tratamiento de las alegaciones.

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

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

Vº Bº
EL PRESIDENTE

Fdo.: Mario Amilivia González

CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

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

PLAN ANUAL DE FISCALIZACIONES 2021

ÍNDICE

SIGLAS Y ABREVIATURAS

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

MAC	Es la dirección física y única para cada dispositivo de red, proviene del inglés "*Media Acces control*"
NAS	Almacenamiento conectado a la red, del inglés *"Network-attached storage"*
OCEX	Órganos de Control Externo Autonómicos
PAM	La gestión de las cuentas con privilegios del inglés "*Privileged Account Management"*
PCs	Computadoras personales. Procede del inglés *"Personal computers"*
Porc.	Porcentaje
RAT	Registro de actividades de tratamiento
SaaS	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 "*Software as a Service"*
SI	Sistema de información
SIEM	Sistema de gestión de información y eventos de seguridad del inglés "*Security Information and Event Management*"
SW	Software
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y de las Comunicaciones
UE	Unión Europea
VPN	Red privada virtual, del inglés *"Virtual Private Network"*
VLAN	Red de extensión física limitada, del inglés *"Virtual Local Area Network"*

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

- Controles.

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

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

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

Finalmente, conforme a lo señalado en el referido apartado 7 de la GPF-OCEX, se evaluará el índice de cumplimiento sobre el nivel requerido, que será, de acuerdo 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 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[1].

[2]

[1] Párrafo modificado en virtud de alegaciones.
[2] 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 4ª 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[3].

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.

[3] 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[4].

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

[4] 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[5].

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[6].

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[7].

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

[5] Párrafo modificado en virtud de alegaciones.
[6] Párrafo modificado en virtud de alegaciones.
[7] 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[8].

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[9].

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[10]"*.

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.

[8] Párrafo añadido en virtud de alegaciones.
[9] Párrafo modificado en virtud de alegaciones.
[10] 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[11].

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[12].

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*[13]*"*.

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[14].

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,

[11] Párrafo modificado en virtud de alegaciones.
[12] Párrafo modificado en virtud de alegaciones.
[13] Párrafo modificado en virtud de alegaciones.
[14] Párrafo modificado en virtud de alegaciones.

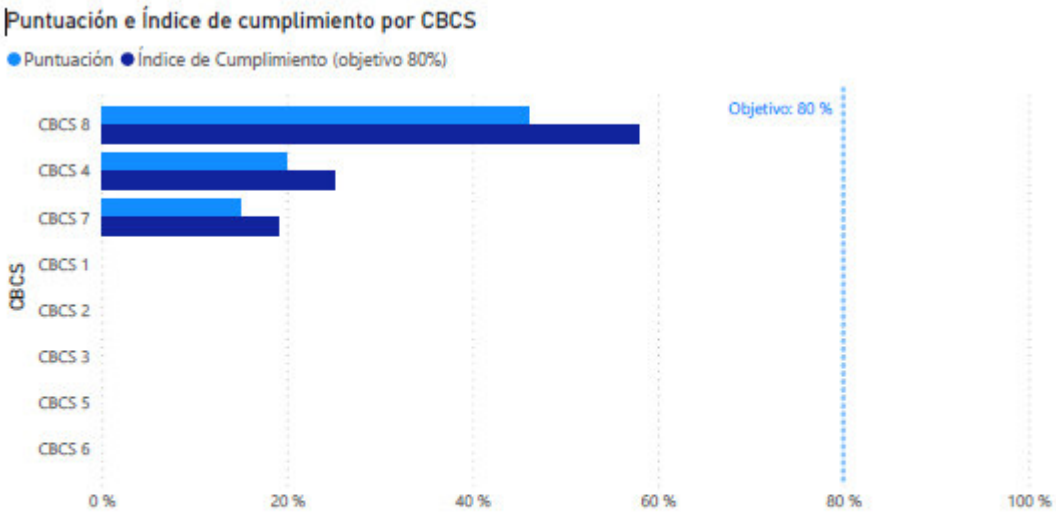
en menor medida, la LOPDGDD, se alcanza el objetivo en lo relativo al registro contable de facturas[15].

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[16].

[15] Párrafo modificado en virtud de alegaciones.
[16] Párrafo modificado en virtud de alegaciones.

Gráfico 1: Puntuación por CBCS[17]



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 %
Total			**13 %**

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%**.

[17] 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) [18]

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,

[18] 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

ÍNDICE DE GRÁFICOS

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.	
BCS 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 estas 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.	
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	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.	op.acc.4 op.acc.5
			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.	

Control		Objetivo de control	Subcontroles	Medidas de seguridad del ENS
		ordenadores, redes y aplicaciones.	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.	
			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	op.exp.2 op.exp.3
			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.	
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.	

Control		Objetivo de control	Subcontroles	Medidas de seguridad del ENS
CBCS 7	Copias de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	CBCS 7-1: Realización de copias de seguridad La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.	mp.info.9
			CBCS 7-2: Realización de pruebas de recuperación Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.	
			CBCS 7-3: Protección de las copias de seguridad Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.	
CBCS 8	Cumplimiento normativo	Cumplimiento de determinados preceptos legales relacionados con la seguridad de la información	CBCS 8-1: Cumplimiento del ENS Política de seguridad y responsabilidades. Declaración de aplicabilidad. Informe de Auditoría (nivel medio o alto). Informe del estado de la seguridad. Publicación de la declaración de conformidad y los distintivos de seguridad en la sede electrónica.	
			CBCS 8-2: Cumplimiento de la LOPD/RGPD Nombramiento del DPD. Registro de actividades de tratamiento. Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento (para los de riesgo alto). Informe de auditoría de cumplimiento (cuando el responsable del tratamiento haya decidido realizarla).	
			CBCS 8-3: Cumplimiento de la Ley 25/2013, de 27 de diciembre (Impulso de la factura electrónica y creación del registro contable de facturas). Informe de auditoría de sistemas anual del Registro Contable de Facturas.	

ASUNTO: TRAMITE DE ALEGACIONES AL INFORME PROVISIONAL RELATIVO A LA "FISCALIZACIÓN DE LA SITUACIÓN INFORMÁTICA DEL AYUNTAMIENTO DE SANTA MARTA DE TORMES (SALAMANCA)".
EXPTE: 1338/2020

DAVID MINGO PÉREZ, Alcalde-Presidente del Ayuntamiento de Santa Marta de Tormes (Salamanca), por medio del presente, comparezco y DIGO:

Que recibido escrito de esa institución con fecha de registro de entrada de 1 de septiembre de 2021 (nº 2021-E-RC-2313) por el que se recibe el informe provisional relativo al análisis de la seguridad informática de este Ayuntamiento, y dentro del plazo conferido al efecto, por medio del presente formula contra el mismo, las siguientes,

ALEGACIONES

PRIMERA.- Sobre el entorno tecnológico y sistemas de información objeto de fiscalización (Conclusión III.1).

(1). Hacen referencia a la inexistencia de dirección política en la materia, cuestión que no es cierta ya que el concejal de Nuevas Tecnologías está informado constantemente de las líneas de trabajo del área. Además, se llevan a cabo reuniones de trabajo en las que propone cambios y mejoras para el servicio.

(2, 3 y 4). Efectivamente la RPT del Ayuntamiento no contempla personal técnico adscrito al área de Nuevas Tecnologías por lo que es la empresa adjudicataria del contrato la responsable de la prestación del servicio, subrayando que no existe vinculación laboral entre el responsable de la empresa y el Ayuntamiento.

La persona designada de contacto, por tanto, no tiene ninguna vinculación laboral, ni funcionarial, ni como personal eventual tal y como se puede acreditar con la correspondiente Relación de Puestos de Trabajo (publicada en el BOP Nº 6 del 10-1-2020, modificada según anuncio publicado en el BOP Nº 22 del 3-2-2021), así como en la Plantilla (BOP Nº 13 del 18-1-2021).

La posible confusión puede deberse por aparecer dicha persona en algún correo electrónico en su calidad de "Jefe de Prensa del Ayuntamiento de Santa Marta de Tormes" (apartado II.3, pág. 22 del informe provisional), teniendo en cuenta que aquella es adjudicataria de un contrato de asesoría de comunicación, protocolo y relaciones con la prensa del Ayuntamiento.

Con respecto a la falta de cumplimiento del deber de colaboración para con este Consejo de Cuentas (tal y como se detalla en el apartado II.3 del citado informe provisional), este Ayuntamiento lamenta profundamente que la persona designada haya podido incurrir en ese incumplimiento, del cual no era conocedor hasta el extremo en que se refiere en el apartado II.3 del informe antes citado, pues, en ningún momento ha existido ánimo o intencionalidad alguna de no colaborar con esta institución.

En cualquier caso , este Ayuntamiento ofrece la colaboración necesaria, así como la práctica de las actuaciones y pruebas pertinentes que este Consejo de Cuentas considere oportunas, para que, de manera inmediata, se puedan aclarar todas aquellas cuestiones pendientes, siendo la única intención de esta Corporación la máxima colaboración con el Consejo de Cuentas, como, por otra parte, es habitual en otros procedimientos seguidos con esta institución.

A tal efecto, facilitamos como persona de contacto para futuras actuaciones que resulten necesarias practicar, además de la persona designada, a Dª Esther Corchero Martín, Jefa de Contabilidad y Presupuestos de este Ayuntamiento (con correo electrónico: ecorchero@santamartadetormes.org) rogando sea también objeto de las comunicaciones oportunas.

(5, 6 y 7). En la actualidad el Ayuntamiento está trabajando para sacar a licitación, de acuerdo con la nueva ley de contratos, el servicio de Mantenimiento Informático. En este contrato estarán plasmados y definidos todos los servicios y sistemas de gestión en los que sí estarán registrados toda la información, servicios, necesidades, así como el pliego de prescripciones técnicas y las pautas marcadas por el ENS. También se recogerán en este pliego cuestiones como el inventario de activos de hardware.

(8, 9 y 10). El día 1 de agosto han comenzado los trabajos para sustituir la red física del Ayuntamiento por un sistema totalmente virtualizado que estará funcionando plenamente a mediados de la semana del 13 de septiembre corrigiendo y eliminando la mayoría de los problemas de seguridad. Todos los trabajadores del Ayuntamiento accederán a través de una vpn y podrán compartir los archivos con un Nas.

SEGUNDA.- Sobre el inventario y control de dispositivos físicos (Conclusión III.2).

(11 y 13). Actualmente el Ayuntamiento no tiene un inventario actualizado de los activos de hardware. Esta situación será corregida en las próximas fechas ya que se han iniciado los trabajos para comenzar a inventariar todos los elementos de hardware que permitan un mayor control.

(12). Es cierto que no hay medidas específicas para conectar dispositivos físicos a no autorizados, aunque solamente están activas las "bocas" de la red a la que están conectados los equipos del consistorio. El resto de bocas están deshabilitadas y determinados equipos tiene bloqueados los puertos usb para que a los equipos no puedan conectarse dispositivos no autorizados.

TERCERA.- Sobre el inventario y control de software autorizado y no autorizado (Conclusión III.3).

(14 y 17) Como dice en este punto las conclusiones del informe provisional, el Ayuntamiento no dispone de inventario formalizado y estandarizado de software aunque sí existe una relación de las aplicaciones utilizadas por los usuarios dependiendo del puesto que desempeñan.

(15) También está previsto la contratación, de cara al próximo año, del servicio que permita el control y seguimiento de las pautas y estándares fijadas por el ENS.

(16) En cuanto a las licencias, están en poder del Ayuntamiento y pueden comprobarse las correspondiente a los sistemas antivirus de equipos y correo, así como de otras aplicaciones que se van incorporando como son Adobe DC, Photoshop o Autocad. En el futuro está previsto continuar con la compra e implantación de licencias.

CUARTA.- Sobre el proceso continuo de identificación y corrección de vulnerabilidades (Conclusión III.4).

(18) Como dicen el Ayuntamiento utiliza una herramienta externa, Gestiona, facilitada por Diputación de Salamanca para una de las partes más relevantes de sus sistemas de información. Esto se debe a que el Ayuntamiento de Santa Marta, como la gran mayoría de los Ayuntamientos de su tamaño y población no cuenta con los recursos necesarios ni suficiente para poder desarrollar este tipo de aplicaciones de gestión interna de expedientes o sede electrónica. Tampoco se cuenta con los recursos necesarios para tener mecanismo de vigilancia del correcto funcionamiento del servicio ni de la corrección de vulnerabilidades. Es otro de los motivos de la contratación de este servicio con una empresa especializada que ofrece todas las garantías y asesoramiento para la identificación de vulnerabilidades y su posterior corrección.

En cuanto al resto de sistemas, es cierto que ese proceso no está procedimentado y descrito pormenorizadamente pero existe. El Ayuntamiento revisa periódicamente los procedimientos para corregir esas posibles vulnerabilidades.

(19) El anterior punto se deduce que la identificación y corrección de vulnerabilidades no es un procedimiento que actualmente no se esté llevando a cabo en el Consistorio. En primer lugar se está haciendo por la empresa EsPúblico, propietaria y prestadora de la plataforma de gestión de expedientes y también por parte del Ayuntamiento, aunque no esté formalizado y procedimentado.

QUINTA.- Sobre el uso controlado de privilegios administrativos (Conclusión III.5)

(20, 21, 22 y 23) Actualmente en el Ayuntamiento las labores que desempeñan la mayoría de los trabajadores prácticamente se ciñen al uso de Gestiona. Esta aplicación tiene la seguridad suficiente y periódicamente se realiza un cambio obligatorio de las contraseñas de acceso.

Además, la herramienta Bitdefender asegura el uso de navegación según establecen círculos de privilegios en función de las necesidades de cada puestos. Hay permisos para navegar en cualquier url o permisos para acceder a un grupo de url´s determinado.

Los proveedores externos son habitualmente empresas reconocidas que ofrecen las garantías necesarias de profesionalidad y seguridad. En cualquier caso es otro de los puntos que se establecerá de cara a un futuro para incluir la firma de este tipo de convenios o contratos que aseguren el buen uso de estas cuentas.

SEXTA.- Sobre configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores (Conclusión III.6)

(24 y 25) La seguridad en todos los equipos aumentará y mejorará notablemente con el cambio y la virtualización que está realizando en estos momentos. Los dos servidores que están actualmente en funcionamiento y que albergan las bases de datos de Padrón, Contabilidad, Gestión Tributaria, Tasas.... pasarán a ser un servicio cloud y este problema se corregirá en gran medida.

SEPTIMA.- Sobre el registro de la actividad de los usuarios (Conclusión III.7).

(27) Por el tamaño y número de empleados del Ayuntamiento no se ha considerado necesario, hasta el momento, hacer una relación de los logs del Ayuntamiento, cuestión que será subsanada con la firma del próximo contrato de "Mantenimiento de Sistemas Informáticos". Esta opción será incluida dentro de los servicios exigidos.

OCTAVA.- Sobre copias de seguridad de datos y sistemas (Conclusión III.8)

(30, 31, 32 y 33) Se realizan copias de seguridad en el interior de las instalaciones municipales, en los servidores físicos y se esa copia de seguridad también sale hacia servidores, a un centro de datos que cuenta con todas las medidas de seguridad y protección. Además, periódicamente se revisan que las copias de validez son válidas y pueden ser restauradas en caso de ser necesario. El sistema a de copias de seguridad está pasando a servidores virtuales en estos momentos.

NOVENA.- Sobre el cumplimiento normativo (Conclusión III.9

(34) Efectivamente el Ayuntamiento no está siguiendo las recomendaciones de ENS aunque ya se están dando los pasos para que todas las pautas y normativa está establecida y presente en un nuevo contrato para el año 2022.

(35) El consistorio tiene adjudicado, tal como exige la ley, el servicio de protección de datos del que hay nombrado a delegado. Igualmente el Ayuntamiento cuenta con un Registro Contable de Facturas.

En conclusión:

1. El Ayuntamiento muestra toda su disposición para colaborar tanto en este como en cualquier otro procedimiento.

2. Que en la actualidad se está trabajando para sacar a licitación pública el contrato de Mantenimiento de Sistemas Informáticos.

3. El Ayuntamiento está realizando el cambio de la red física a una red virtual que conseguirá una mayor seguridad ya que los elementos dejarán de ser físicos y estarán en un entorno más seguro.

4. El Ayuntamiento nunca ha recibido recomendaciones expresas, ni formación, ni plazos de adaptación para cumplir con las diferentes normativas regionales, nacionales ni europeas.

5. A pesar de los continuos ataques que se reciben en las ip´s diariamente el Ayuntamiento no ha tenido en los últimos 5 años ningún problema de vulneración de datos ni seguridad.

En virtud de lo expuesto,

SOLICITO.- Tenga por presentado el presente escrito, por admitidas las alegaciones contenidas en el mismo en relación al informe provisional sobre el análisis de seguridad informática de este Ayuntamiento, al objeto de que sean tenidas en cuenta para el informe definitivo

De igual manera, se solicita acordar las actuaciones y práctica de pruebas que considere oportunas esa institución, a fin de aclarar y comprobar todas las cuestiones que sean necesarias.

En Santa Marta de Tormes, firmado electrónicamente por el Alcalde en la fecha que figura en el margen del presente documento.

CONSEJO DE CUENTAS DE CASTILLA Y LEON
C/ Mayor, 54
34001 PALENCIA

CONSEJO DE CUENTAS

DE CASTILLA Y LEÓN

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

TRATAMIENTO DE ALEGACIONES

PLAN ANUAL DE FISCALIZACIONES 2021

ÍNDICE

ACLARACIONES

El contenido de las alegaciones figura en tipo de letra normal, reproduciéndose previamente el párrafo alegado en letra cursiva.

La contestación a las alegaciones presentadas se hace en tipo de letra negrita.

Las referencias de las páginas están hechas con relación al Informe provisional para alegaciones.

Se han numerado las alegaciones formuladas por el Ente fiscalizado a efectos de una mayor claridad en su exposición y tratamiento en la presente Propuesta.

I. ALEGACIÓN PRIMERA

Párrafos de referencia (páginas 24 y 25, conclusiones 1 a 10).

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

1) *Las competencias del área de nuevas tecnologías recaen en el 4ª 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. (Apartado V.1.1)*

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. (Apartado V.1.1)*

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. (Apartado V.1.1)*

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 ésta los desconoce, debiendo recurrir a la propia empresa para aportar la información solicitada. Se da la circunstancia de que el titular de esta empresa trabaja en el Ayuntamiento y ha incumplido el deber de colaboración para con el Consejo de Cuentas como se detalla en el apartado II.3 del presente Informe. (Apartado V.1.1)*

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. (Apartado V.1.1)*

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. (Apartado V.1.1)*

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. (Apartado V.1.2)*

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. (Apartado V.1.2)*

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, únicamente recursos compartidos en un grupo de trabajo. (Apartado V.1.3)*

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.(Apartado V.1.3)*

Alegación realizada

(1). Hacen referencia a la inexistencia de dirección política en la materia, cuestión que no es cierta ya que el concejal de Nuevas Tecnologías está informado constantemente de las líneas de trabajo del área. Además, se llevan a cabo reuniones de trabajo en las que propone cambios y mejoras para el servicio.

(2, 3 y 4). Efectivamente la RPT del Ayuntamiento no contempla personal técnico adscrito al área de Nuevas Tecnologías por lo que es la empresa adjudicataria del contrato la responsable de la prestación del servicio, subrayando que no existe vinculación laboral entre el responsable de la empresa y el Ayuntamiento.

La persona designada de contacto, por tanto, no tiene ninguna vinculación laboral, ni funcionarial, ni como personal eventual tal y como se puede acreditar con la correspondiente Relación de Puestos de Trabajo (publicada en el BOP N° 6 del 10-1-2020, modificada según anuncio publicado en el BOP N° 22 del 3-2-2021), así como en la Plantilla (BOP N° 13 del 18-1-2021).

La posible confusión puede deberse por aparecer dicha persona en algún correo electrónico en su calidad de "Jefe de Prensa del Ayuntamiento de Santa Marta de Tormes" (apartado II.3, pág. 22 del informe provisional), teniendo en cuenta que aquella

es adjudicataria de un contrato de asesoría de comunicación, protocolo y relaciones con la prensa del Ayuntamiento.

Con respecto a la falta de cumplimiento del deber de colaboración para con este Consejo de Cuentas (tal y como se detalla en el apartado II.3 del citado informe provisional), este Ayuntamiento lamenta profundamente que la persona designada haya podido incurrir en ese incumplimiento, del cual no era conocedor hasta el extremo en que se refiere en el apartado II.3 del informe antes citado, pues, en ningún momento ha existido ánimo o intencionalidad alguna de no colaborar con esta institución.

En cualquier caso, este Ayuntamiento ofrece la colaboración necesaria, así como la práctica de las actuaciones y pruebas pertinentes que este Consejo de Cuentas considere oportunas, para que, de manera inmediata, se puedan aclarar todas aquellas cuestiones pendientes, siendo la única intención de esta Corporación la máxima colaboración con el Consejo de Cuentas, como, por otra parte, es habitual en otros procedimientos seguidos con esta institución.

A tal efecto, facilitamos como persona de contacto para futuras actuaciones que resulten necesarias practicar, además de la persona designada, a Dª Esther Corchero Martín, Jefa de Contabilidad y Presupuestos de este Ayuntamiento (con correo electrónico: ecorchero@santamartadetormes.org) rogando sea también objeto de las comunicaciones oportunas.

(5, 6 y 7). En la actualidad el Ayuntamiento está trabajando para sacar a licitación, de acuerdo con la nueva ley de contratos, el servicio de Mantenimiento Informático. En este contrato estarán plasmados y definidos todos los servicios y sistemas de gestión en los que sí estarán registrados toda la información, servicios, necesidades, así como el pliego de prescripciones técnicas y las pautas marcadas por el ENS. También se recogerán en este pliego cuestiones como el inventario de activos de hardware.

(8, 9 y 10). El día 1 de agosto han comenzado los trabajos para sustituir la red física del Ayuntamiento por un sistema totalmente virtualizado que estará funcionando plenamente a mediados de la semana del 13 de septiembre corrigiendo y eliminando la mayoría de los problemas de seguridad. Todos los trabajadores del Ayuntamiento accederán a través de una vpn y podrán compartir los archivos con un Nas.

Contestación a la alegación

Con respecto a lo indicado sobre la conclusión (1), el Informe afirma que la dirección política no es efectiva, no que sea inexistente. El Ayuntamiento no aporta en su alegación ninguna justificación de la efectividad de la dirección política que realiza, más allá de señalar que el Concejal está informado de las actuaciones que realiza la empresa de mantenimiento, y realiza propuestas de cambio o mejoras, tareas que no suponen una dirección política efectiva, como se deduce de los siguientes hechos:

- **No se ha definido una estructura de TI en el Ayuntamiento para asumir las responsabilidades que le corresponden (conclusión 3)**

- **No se han realizado licitaciones planificadas en materia de servicios informáticos, sino que se ha recurrido a contrataciones menores sucesivas, evidenciando la falta de planificación del servicio (conclusión 5)**

- **El conocimiento sobre el entorno tecnológico no se encuentra en el Ayuntamiento, como pone de manifiesto el hecho de que la interlocución con el equipo auditor haya tenido que ser asumida por la propia empresa de mantenimiento, y no por personal del Ayuntamiento, que en todo caso podría ser asistido en las cuestiones más técnicas por la empresa de mantenimiento informático, pero que debería tener un mínimo conocimiento sobre sus sistemas de información (conclusiones 3, 4 y 6)**

Acerca de las alegaciones realizadas sobre las conclusiones (2, 3 y 4), el Ayuntamiento confirma lo expuesto en el Informe acerca de la falta de una estructura de TI en el Ayuntamiento.

Con respecto a la vinculación laboral de la persona responsable de la interlocución del Ayuntamiento el Consejo de Cuentas constata que se presenta como "jefe de prensa" del ayuntamiento, con correo del ayuntamiento y el escudo del ayuntamiento en su firma. En caso de no ser efectivamente un trabajador, el Ayuntamiento deberá tomar las medidas necesarias para aclarar la situación y evitar el uso de su correo o de sus símbolos por personas ajenas al mismo.

Respecto a que es adjudicataria de un contrato de *"asesoría de comunicación, protocolo y relaciones con la prensa del Ayuntamiento",* en realidad según la Plataforma de Contratos del Sector Público, dicho contrato quedó desierto la primera vez que se licitó en marzo de 2021, y tras publicarse por segunda vez la licitación en agosto de 2021, está ahora en fase de evaluación, luego, de la documentación que obra en poder del Consejo, esa afirmación no sería precisa. Es cierto que en los menores publicados en el portal de transparencia (en la Plataforma de Contratos del Sector Público no se pudo encontrar) hay uno con el siguiente contenido: "*723 Asesoría de Comunicación, protocolo y relaciones con la prensa. 4 13332,99 02/03/2021 MARTIN TAPIA FRANCISCO JAVIER 002242730N SLNE*"

Con respecto a lo indicado sobre las conclusiones (5, 6 y 7), la alegación ratifica el contenido del Informe.

Finalmente, en las alegaciones sobre las conclusiones (8, 9 y 10), el Ayuntamiento informa de los cambios realizados con posterioridad a la emisión del Informe Provisional, y que según el Ayuntamiento suponen un cambio sustancial en la seguridad de la red y en el entorno tecnológico del Ayuntamiento.

Dado que el Ayuntamiento en esta primera alegación solicitó, además, la realización de las pruebas adicionales necesarias, se han llevado éstas a cabo y se ha evaluado su impacto, realizándose las siguientes modificaciones que se han incorporado al Informe en aplicación del Art. 26.5 del Reglamento del Consejo de Cuentas:

En la página 25, conclusión 12), donde dice "*No se han implantado medidas para impedir la conexión de dispositivos físicos no autorizados en la red cableada y las que existen en la red inalámbrica no se han podido verificar",* debe decir *"No se han implantado medidas efectivas para impedir la conexión de dispositivos físicos no autorizados".*

En la página 26, conclusión 15) donde dice "*El Ayuntamiento utiliza para sistemas de información muy relevantes, aplicaciones cuya contratación realiza la Diputación de Salamanca (a través de CIPSA) sin que se hayan previsto los medios de control que el ENS establece para el uso de proveedores externos."* Debe decir *"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".

En la página 26, conclusión 18) donde dice "*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.",* debe decir "*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".

En la misma conclusión donde dice *"Con respecto al resto de elementos que el Ayuntamiento mantiene directamente, no realiza ningún proceso de identificación y corrección de vulnerabilidades. El riesgo de que una vulnerabilidad crítica permanezca sin corregir en sus sistemas y cree una ventana de oportunidad para un ataque es elevado",* debe decir "*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".

En la página 27, se introduce una nueva conclusión, numerada como 21), *"Hay un cierto control de las cuentas con privilegios administrativos de los sistemas más relevantes, aunque con un amplio margen de mejora (Apartado V.5)".* Como

consecuencia, todas las conclusiones de la 21) en adelante se renumeran incrementándose una unidad.

En la página 27, conclusión 22) (renumerada como 23), donde dice ***"No consta que se hayan establecido contractualmente o por convenio mecanismos que permitan asegurar el buen uso y gestión de las cuentas de administración controladas por proveedores externos"*****, debe decir** ***"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".***

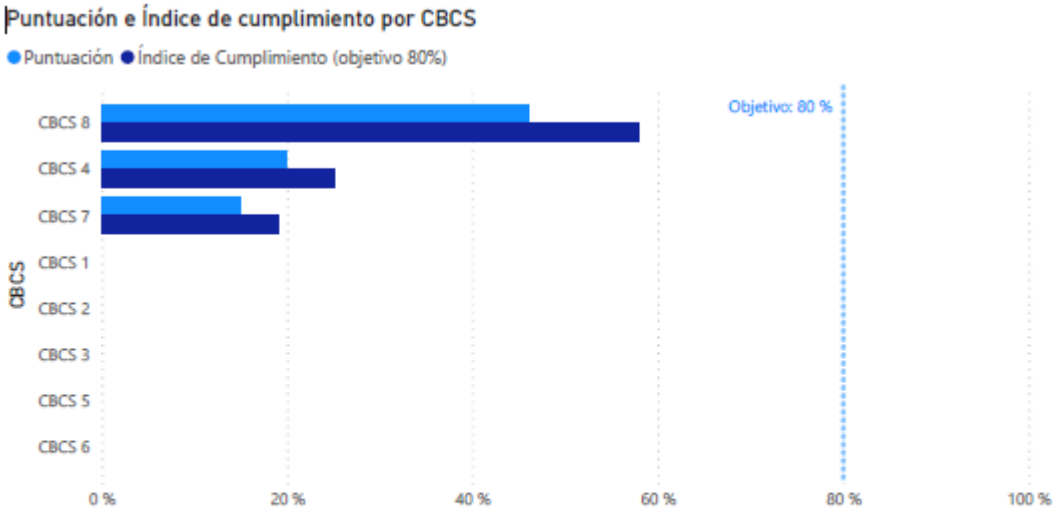
En la página 27, conclusión 23) (renumerada como 24), donde dice ***"No se ha podido verificar la existencia de un proceso de control del uso de privilegios administrativos, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos""*****, debe decir "*****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"."***

En la página 28, conclusión 30) (renumerada como 31), donde dice ***"No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento si describe una sistemática para su realización. Sin embargo, no se ha podido verificar que se estén realizando"*****, debe decir** ***"No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento sí describe una sistemática para su realización y se realizan en parte de los sistemas relevantes, disponiendo de herramientas para ello".***

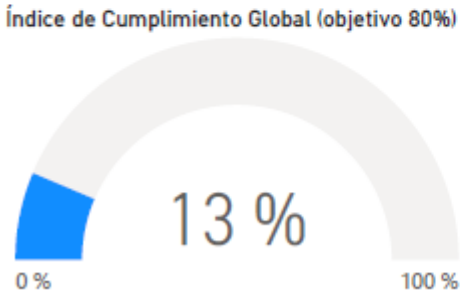
En la página 28, conclusión 32) (renumerada como 33) donde dice ***"No se ha podido verificar que se aplican medidas suficientes para la protección de las copias de seguridad"*****, debe decir** ***"Se aplican medidas insuficientes para la protección de las copias de seguridad, siendo de especial relevancia la carencia de mecanismos de control en la contratación de las copias de seguridad en infraestructuras de terceros".***

En la página 28, conclusión 33) (renumerada como 34), donde dice ***"No se ha podido verificar la existencia del proceso para la realización de copias de seguridad, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos""*****, debe decir** ***"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"."***

En la página 29, apartado "III.10", donde dice ***"El Ayuntamiento de Santa Marta de Tormes no ha implantado ninguno de los subcontroles revisados, o bien, dada la falta de disposición para la realización de pruebas, o para aportar la documentación requerida, no ha podido demostrar su efectividad."*** **debe decir** ***"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.", y se introduce a continuación el siguiente gráfico, numerado como "1":***



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 %
Total			**13 %**



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%**.

Como consecuencia, se renumeran los gráficos del 1 en adelante, incrementándose en una unidad.

En cuanto a la falta de colaboración que el Consejo reflejó en el Informe Provisional, una vez que ha sido subsanada por parte del Alcalde, el Consejo solo puede destacar la necesidad de una adecuada valoración del trabajo de las Instituciones de la Comunidad, especialmente cuando el beneficiario del Informe es el Ayuntamiento, en tanto recibe una visión objetiva de su situación en este ámbito junto con propuestas claras para mejorarla.

Como consecuencia de la alegación presentada se modifica el apartado II.3 LIMITACIONES que pasa a tener la siguiente redacción:

"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."

Se modifica la conclusión 4 que pasa a tener la siguiente redacción:

"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 ésta los desconoce, debiendo recurrir a la propia empresa para aportar la información solicitada."

Se elimina la recomendación 1.

Como consecuencia, se renumeran las siguientes recomendaciones decrementándose en una unidad.

II. ALEGACIÓN SEGUNDA

Párrafos de referencia conclusiones apartado III.2.

III.2. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

11) No existe un inventario que permita un control adecuado de los activos hardware. (Apartado V.2.1)

12) No se han implantado medidas para impedir la conexión de dispositivos físicos no autorizados en la red cableada y las que existen en la red inalámbrica no se han podido verificar. (Apartado V.2.2)

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". (Apartado V.2.3)

Alegación realizada

(11 y 13). Actualmente el Ayuntamiento no tiene un inventario actualizado de los activos de hardware. Esta situación será corregida en las próximas fechas ya que se han iniciado los trabajos para comenzar a inventariar todos los elementos de hardware que permitan un mayor control.

(12). Es cierto que no hay medidas específicas para conectar dispositivos físicos a no autorizados, aunque solamente están activas las "bocas" de la red a la que están conectados los equipos del consistorio. El resto de bocas están deshabilitadas y determinados equipos tiene bloqueados los puertos usb para que a los equipos no puedan conectarse dispositivos no autorizados.

Contestación a la alegación

Sobre lo señalado acerca de las conclusiones (11 y 13), la alegación ratifica el contenido del Informe.

Para dar respuesta a la alegación al contenido de la conclusión (12), tal y como se ha detallado con anterioridad, se realizaron las pruebas adicionales pertinentes para comprobar si en efecto se encontraban deshabilitadas, concluyéndose tras solicitar aclaración al Ayuntamiento durante la sesión de pruebas, que la medida aplicada consiste en no parchear los puertos de red que no se están utilizando.

Se modifica en consecuencia el memorándum detallado enviado al Ayuntamiento y una vez evaluadas nuevamente las medidas que se aplican en su conjunto, se estima que esta medida, es insuficiente, y no se aplican otras adicionales que puedan complementarla, por lo que no se modifican las conclusiones sobre la aplicación del control.

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

III. ALEGACIÓN TERCERA

Párrafos de referencia Conclusiones apartado III.3.

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 autorizado, por lo que no existe control sobre qué software se utiliza, ni del estado de sus licencias ni del soporte del software. (Apartado V.3.1)*

15) *El Ayuntamiento utiliza para sistemas de información muy relevantes, aplicaciones cuya contratación realiza la Diputación de Salamanca (a través de CIPSA) sin que se hayan previsto los medios de control que el ENS establece para el uso de proveedores externos. (Apartado V.3.2)*

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. (Apartado V.3.2.3)

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". (Apartado V.3.4)*

Alegación realizada

(14 y 17) Como dice en este punto las conclusiones del informe provisional, el Ayuntamiento no dispone de inventario formalizado y estandarizado de software aunque sí existe una relación de las aplicaciones utilizadas por los usuarios dependiendo del puesto que desempeñan.

(15) También está previsto la contratación, de cara al próximo año, del servicio que permita el control y seguimiento de las pautas y estándares fijadas por el ENS.

(16) En cuanto a las licencias, están en poder del Ayuntamiento y pueden comprobarse las correspondiente a los sistemas antivirus de equipos y correo, así como de otras aplicaciones que se van incorporando como son Adobe DC, Photoshop o Autocad. En el futuro está previsto continuar con la compra e implantación de licencias.

Contestación a la alegación

Sobre lo indicado acerca de las conclusiones (14 y 15), la alegación ratifica el contenido del Informe, dado que el Ayuntamiento confirma la inexistencia de inventario, y sobre la relación de aplicaciones por usuario, solicitada esta al Ayuntamiento, únicamente se proporciona un listado de tres aplicaciones, con indicación del número de puestos en que se encuentran instaladas, y por tanto no implica ningún cambio sobre las conclusiones del Informe.

No obstante, para una mayor precisión y como consecuencia de la documentación aportada por el Ayuntamiento en la fase de alegaciones, se realiza el cambio en la redacción de la conclusión 15) que ya se ha detallado en la respuesta a la alegación primera.

Sobre lo indicado acerca de la conclusión 16) no se ha aportado documentación que sustente la afirmación del Ayuntamiento, por lo que la alegación presentada no modifica el contenido del Informe.

IV. ALEGACIÓN CUARTA

Párrafos de referencia Conclusiones apartado III.4

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. (Apartado V.4.1)*

19) *Con respecto al resto de elementos que el Ayuntamiento mantiene directamente, no realiza ningún proceso de identificación y corrección de vulnerabilidades. El riesgo de que una vulnerabilidad crítica permanezca sin corregir en sus sistemas y cree una ventana de oportunidad para un ataque es elevado. (Apartado V.4.1)*

20) *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". (Apartado V.4.2)*

Alegación realizada

(18) Como dicen el Ayuntamiento utiliza una herramienta externa, Gestiona, facilitada por Diputación de Salamanca para una de las partes más relevantes de sus sistemas de información. Esto se debe a que el Ayuntamiento de Santa Marta, como la gran mayoría de los Ayuntamientos de su tamaño y población no cuenta con los recursos necesarios ni suficiente para poder desarrollar este tipo de aplicaciones de gestión interna de expedientes o sede electrónica. Tampoco se cuenta con los recursos necesarios para tener mecanismo de vigilancia del correcto funcionamiento del servicio ni de la corrección de vulnerabilidades. Es otro de los motivos de la contratación de este servicio con una empresa especializada que ofrece todas las garantías y asesoramiento para la identificación de vulnerabilidades y su posterior corrección.

En cuanto al resto de sistemas, es cierto que ese proceso no está procedimentado y descrito pormenorizadamente, pero existe. El Ayuntamiento revisa periódicamente los procedimientos para corregir esas posibles vulnerabilidades.

(19) El anterior punto se deduce que la identificación y corrección de vulnerabilidades no es un procedimiento que actualmente no se esté llevando a cabo en el Consistorio. En primer lugar se está haciendo por la empresa EsPúblico, propietaria y prestadora de la plataforma de gestión de expedientes y también por parte del Ayuntamiento, aunque no esté formalizado y procedimentado.

Contestación a la alegación

La falta de recursos que impiden realizar un correcto seguimiento del servicio prestado por proveedores externos ya sea mediante el convenio con la

Diputación, o por contrataciones realizadas, no exime al Ayuntamiento de sus obligaciones, y refuerza el sentido de la recomendación que señala la necesidad de dotar con recursos suficientes a su departamento de TI.

Con respecto a la afirmación de que la contratación de una empresa especializada ofrece todas las garantías, sólo puede aceptarse como cierta en caso de que se apliquen los requisitos mínimos que exige en ENS acerca del uso de recursos externos, lo que no se da para la contratación de las empresas *"MT Comunicación"* y "*Wurth*", ni para el uso de los recursos que proporciona la Diputación.

En las pruebas realizadas en la fase de alegaciones, el Ayuntamiento detalla cómo realiza la gestión de vulnerabilidades, deduciéndose que no existe una sistemática, dependiendo en todo caso de actuaciones individuales de los técnicos de la empresa mantenedora y con las limitaciones que implica la falta de control sobre el software instalado, que no permite conocer en detalle las aplicaciones, versiones, niveles de parcheo, etc. y por tanto realizar un proceso de gestión de vulnerabilidades adecuado.

Se procede a aclarar en el memorándum detallando las actuaciones que realiza el Ayuntamiento y se modifica la conclusión 18) en el sentido ya detallado en la contestación a la alegación primera.

V. ALEGACIÓN QUINTA

Párrafos de referencia Conclusiones apartado III.5.

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

21) *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 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. (Apartado V.5)*

22) *Los usuarios son administradores de sus equipos sin que se justifique la necesidad de tener esa condición. (Apartado V.5.1.1)*

23) *No consta que se hayan establecido contractualmente o por convenio mecanismos que permitan asegurar el buen uso y gestión de las cuentas de administración controladas por proveedores externos. (Apartado V.5.1.2)*

24) *No se ha podido verificar la existencia de un proceso de control del uso de privilegios administrativos, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.5.6)*

Alegación realizada

(20, 21, 22 y 23) Actualmente en el Ayuntamiento las labores que desempeñan la mayoría de los trabajadores prácticamente se ciñen al uso de Gestiona. Esta aplicación tiene la seguridad suficiente y periódicamente se realiza un cambio obligatorio de las contraseñas de acceso.

Además, la herramienta Bitdefender asegura el uso de navegación según establecen círculos de privilegios en función de las necesidades de cada puesto. Hay permisos para navegar en cualquier url o permisos para acceder a un grupo de url's determinado.

Los proveedores externos son habitualmente empresas reconocidas que ofrecen las garantías necesarias de profesionalidad y seguridad. En cualquier caso es otro de los puntos que se establecerá de cara a un futuro para incluir la firma de este tipo de convenios o contratos que aseguren el buen uso de estas cuentas.

Contestación a la alegación

Lo indicado sobre las conclusiones (20, 21, 22 y 23) sobre el uso prácticamente exclusivo de la aplicación Gestiona, siendo este un sistema de información en la nube, en la modalidad "*software como servicio o SaaS, Software as a Servicie*" implica que precisamente el proceso de gestión de privilegios administrativos adquiere aún mayor relevancia, dado que el uso inadecuado de usuarios administradores es uno de los riesgos que la *"Guía Práctica de Fiscalización de los Órganos de Control Externo (GPF-OCEX) 1403, Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube"* identifica como derivado o acentuado por el uso de soluciones en la nube. Dicha guía indica que *"habrá administradores ajenos a la entidad cuya existencia no será "visible" (en la mayoría de los casos) ni para los auditores ni para la propia entidad auditada. A veces las entidades con servicios cloud contratados confían, sin verificar, en la buena gestión de los usuarios realizada por el CSP incurriendo en riesgos importantes".*

En el caso de Santa Marta de Tormes, se produce esta circunstancia, al carecer de los mecanismos de control mínimos exigidos por el ENS.

Tras la realización de las pruebas correspondientes, se verificó que la herramienta BitDefender no realiza ninguna función relativa a la gestión de usuarios administradores.

Finalmente, como ya se ha indicado, la contratación de servicios a proveedores de prestigio reconocido en el sector, y con certificaciones de cumplimiento del ENS al nivel requerido, es condición necesaria pero no suficiente como se ha puesto de relieve en el Informe.

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

VI. ALEGACIÓN SEXTA

Párrafos de referencia Conclusiones apartado III.6.

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). (Apartado V.6.1)*

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. (Apartado V.6.2)*

Alegación realizada

(24 y 25) La seguridad en todos los equipos aumentará y mejorará notablemente con el cambio y la virtualización que está realizando en estos momentos. Los dos servidores que están actualmente en funcionamiento y que albergan las bases de datos de Padrón, Contabilidad, Gestión Tributaria, Tasas.... pasarán a ser un servicio cloud y este problema se corregirá en gran medida.

Contestación a la alegación

La alegación refuerza el contenido del Informe toda vez que el Ayuntamiento reconoce la necesidad de realizar cambios para poder implantar este proceso de configuración segura.

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

VII. ALEGACIÓN SÉPTIMA

Párrafos de referencia Conclusiones apartado III.7.

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

27) *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. (Apartado V.7.1)*

Alegación realizada

(27) Por el tamaño y número de empleados del Ayuntamiento no se ha considerado necesario, hasta el momento, hacer una relación de los logs del Ayuntamiento, cuestión que será subsanada con la firma del próximo contrato de

"Mantenimiento de Sistemas Informáticos". Esta opción será incluida dentro de los servicios exigidos.

Contestación a la alegación

La alegación refuerza el contenido del Informe toda vez que el Ayuntamiento reconoce la necesidad de subsanar esta carencia.

VIII. ALEGACIÓN OCTAVA

Párrafos de referencia Conclusiones apartado III.8.

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

30) *No existe un procedimiento formalizado para la realización de copias de seguridad, aunque el Ayuntamiento si describe una sistemática para su realización. Sin embargo, no se ha podido verificar que se estén realizando. (Apartado V.8.1)*

31) *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. (Apartado V.8.2)*

32) *No se ha podido verificar que se aplican medidas suficientes para la protección de las copias de seguridad. (apartado V.8.3)*

33) *No se ha podido verificar la existencia del proceso para la realización de copias de seguridad, lo que corresponde al nivel L0 de madurez, que identifica "un proceso inexistente o no aplicado en estos momentos". (Apartado V.8.4)*

Alegación realizada

(30, 31, 32 y 33) Se realizan copias de seguridad en el interior de las instalaciones municipales, en los servidores físicos y se esa copia de seguridad también sale hacia servidores, a un centro de datos que cuenta con todas las medidas de seguridad y protección. Además, periódicamente se revisan que las copias de validez son válidas y pueden ser restauradas en caso de ser necesario. El sistema a de copias de seguridad está pasando a servidores virtuales en estos momentos.

Contestación a la alegación

En las pruebas complementarias que se realizan en la fase de alegaciones, se verifican aquellos aspectos que no se pudieron comprobar en su momento, y siempre teniendo en cuenta que ha habido un cambio tecnológico posterior a la emisión del Informe, se realizan los cambios necesarios en el memorándum detallado.

Adicionalmente, se modifican las conclusiones del Informe en el sentido ya detallado en la respuesta a la alegación primera.

IX. ALEGACIÓN NOVENA

Párrafos de referencia Conclusiones apartado III.9.

III.9. CUMPLIMIENTO NORMATIVO

34) 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. (Apartados V.9.1 y V.9.2)

35) No se ha podido verificar el cumplimiento de lo establecido en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas al no realizar la auditoría de sistemas anual del Registro Contable de Facturas. (Apartado V.9.3)

Alegación realizada

(34) Efectivamente el Ayuntamiento no está siguiendo las recomendaciones de ENS aunque ya se están dando los pasos para que todas las pautas y normativa está establecida y presente en un nuevo contrato para el año 2022.

(35) El consistorio tiene adjudicado, tal como exige la ley, el servicio de protección de datos del que hay nombrado a delegado. Igualmente el Ayuntamiento cuenta con un Registro Contable de Facturas.

En conclusión:

1. El Ayuntamiento muestra toda su disposición para colaborar tanto en este como en cualquier otro procedimiento.

2. Que en la actualidad se está trabajando para sacar a licitación pública el contrato de Mantenimiento de Sistemas Informáticos.

3. El Ayuntamiento está realizando el cambio de la red física a una red virtual que conseguirá una mayor seguridad ya que los elementos dejarán de ser físicos y estarán en un entorno más seguro.

4. El Ayuntamiento nunca ha recibido recomendaciones expresas, ni formación, ni plazos de adaptación para cumplir con las diferentes normativas regionales, nacionales ni europeas.

5. A pesar de los continuos ataques que se reciben en las ip´s diariamente el Ayuntamiento no ha tenido en los últimos 5 años ningún problema de vulneración de datos ni seguridad.

Contestación a la alegación

Lo indicado sobre la conclusión 34) refuerza el contenido del Informe.

Sobre lo alegado a la conclusión 35), con relación al nombramiento del DPD, debe señalarse que la conclusión 34) ya recoge este hecho y ha sido valorado para el cálculo del nivel de madurez del control.

Sobre la realización de la auditoría de sistemas anual exigida 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, el Ayuntamiento ha aportado el informe correspondiente en la fase de alegaciones, hecho que se refleja en el memorándum detallado y se procede a valorar para obtener el nivel de madurez alcanzado en este control.

Se realizan las siguientes modificaciones:

- **En la página 28, conclusión 35), donde dice "*No se ha podido verificar el cumplimiento de lo establecido en el artículo 12 de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas al no realizar la auditoría de sistemas anual del Registro Contable de Facturas"*, debe decir *"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".***

- **En la página 28, conclusión 36), donde dice "*El resultado de la evaluación del control es un nivel de madurez L0, 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"*, debe decir, "*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, en menor medida, la LOPDGDD, se alcanza el objetivo en lo relativo al registro contable de facturas."***