ASUNTO: Informe de la Cámara de Cuentas en relación a *Ciberseguridad y revisión de la seguridad en los procedimientos informáticos.*

Sobre el asunto de referencia, queremos matizar o puntualizar algunas de las apreciaciones o afirmaciones que forman parte de dicho informe, por lo que se emite el siguiente

INFORME:

✓ *Apartado 66.- El Ayuntamiento de Jerez de la Frontera no se ajusta al Esquema Nacional de Seguridad (ENS), al no cumplir con las 75 medidas requeridas en el Anexo II del Real Decreto 3/2010, de 8 de enero. El objeto del ENS es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.*

1. El Esquema Nacional de Seguridad, ha sufrido un proceso de evolución continua desde su primer desarrollo en 2010 (RD 3/2010, de 8 de enero, RD 951/2015 y RD 311/2022). La obligación de adecuación de las administraciones públicas a las medidas del ENS se sujetó a un plazo establecido en la DT única del RD 951/2015

   *"**Disposición transitoria única. Adecuación de sistemas**.: Las entidades incluidas dentro en el ámbito de aplicación del presente real decreto dispondrán de un plazo de veinticuatro meses contados a partir de la fecha de la entrada en vigor del presente real decreto, para la adecuación de sus sistemas a lo dispuesto en el mismo. "*

   ***"Disposición final única. Entrada en vigor**: El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».""*

   Por tanto, habiendo sido publicado dicho RD en el BOE núm. 264, de 4 de noviembre de 2015, su entrada en vigor fue el 5 de noviembre de 2015 y el plazo de adecuación a las medidas del ENS venció el 5 de noviembre de 2017.

   Consultada la Web del ENS, se comprueba qué administraciones públicas cumplían con el ENS en 2018: https://ens.ccn.cni.es/es/allcategories-es-es/12-categoria-es-es/105-entidades-certificadas-sector-publico

   - ✓ En la Administración del Estado: 2 organismos
   - ✓ Entre todas las Comunidades Autónomas: 3 organismos
   - ✓ En la Junta de Andalucía: Ningún organismo
   - ✓ De los 8.122 municipios: 4 municipios, ninguno andaluz

     Ayto. de Alcobendas__19/09/2018
     Ayto. de Avilés_____20/07/2018
     Ayto. de Utebo_____03/12/2018
     Ayto. de Valencia_____20/12/2018

2. Según la información detallada en el punto anterior, la situación del Ayuntamiento de Jerez en relación a la implantación de todas las medidas del ENS era similar al resto de Administraciones. No obstante, el Ayuntamiento de Jerez de la Frontera ya con fecha muy anterior a 2018 tenía implementada un gran volumen de medidas de ciberseguridad, que se han ido ampliando sucesivamente año a año. Incluso podemos afirmar que en 2018 contábamos con medidas incluidas en el ENS. De hecho, a esa Cámara se aportó informe de auditoría de la empresa START UP del año 2017, mediante correo electrónico enviado el jueves, 21 de noviembre de 2019 8:04.

3. En dicho informe, la Cámara de Cuentas indica:

"Política de seguridad: El Ayuntamiento dispone de una política de seguridad basada en los criterios de la guía del CCN-STIC-805 Política de Seguridad de la Información, pero no ha sido aprobada por el comité de seguridad ni ha sido difundida a todo el personal del ayuntamiento."

Hemos de señalar que el Ayuntamiento contaba desde 2015 con Documento de Seguridad y ***fue difundido a todo el personal municipal por cuanto está publicado en la Intranet Municipal desde el año 2015****, en cuyo contenido se incluye el protocolo de seguridad y de protección de datos, a la que tienen acceso todos los empleados municipales.*

Además de lo anterior, debemos indicar que el Ayuntamiento se encuentra inmerso en los trabajos de adaptación al ENS, destacándose lo siguiente:

- ✓ Actualmente se está trabajando con la empresa Tic4You para la Adecuación al ENS, expediente de contratación aprobado por Junta de Gobierno Local, en sesión ordinaria celebrada el día 19 de agosto de 2021,

- ✓ También han sido aprobadas tanto la Política de Seguridad con la Norma de Regulación del Comité de Seguridad de la Información, en Junta de Gobierno Local en sesión ordinaria celebrada el día 31 de mayo de 2022.

- ✓ Con fecha 12 de julio de 2022 la Junta de Gobierno Local efectuó los nombramientos de los miembros del Comité de Seguridad de la Información, que se ha constituido en sesión de 27 de julio.

- ✓ Se ha conseguido una subvención del PRTR-NG-EU mediante Resolución de 18/05/2022 del Director General de Cooperación Autonómica, por importe de 792.550,00€, para el Proyecto: "*Mejora de la Ciberseguridad y apoyo al cumplimiento del ENS en el Ayuntamiento de Jerez de la Frontera: despliegue de un Centro de Operaciones de Ciberseguridad, tareas de concienciación y formación, y realización de auditorías de seguridad*", que permitirá continuar con todas las actuaciones necesarias en orden a conseguir la certificación de cumplimiento del ENS.

✓ *Apartado 67.- "Las medidas que deben cumplir los organismos se dividen en tres Marcos, esto es: el Marco organizacional que determina la política de seguridad, siendo el Pleno el responsable de aprobarla. Para poder llevar a cabo la citada política se debe desarrollar el Marco Operacional. En último lugar, y como complemento se encuentran las medidas de protección. "*

Debemos indicar que la Política de Seguridad ha sido aprobada por Junta de Gobierno Local, siguiendo las indicaciones de la empresa Tic4You, órgano municipal competente en un municipio de gran población, como es Jerez de la Frontera.

- ✓ *Apartado 68.- "De acuerdo con lo manifestado por parte del responsable de área Informática, el Ayuntamiento de Jerez de la Frontera se ha categorizado como nivel Alto. según el Anexo I del Esquema Nacional de Seguridad, lo que implica que ha de cumplir con lo descrito en las categorías Alta del Anexo II del mencionado Esquema según su artículo 2 "Selección de medidas de seguridad".*

A fecha del informe de la Cámara de Cuentas aún no estaba categorizado formalmente, por lo que entendemos se trata de una opinión personal del anterior responsable del servicio. Actualmente estamos trabajando con la empresa Tic4You sobre dicha categorización, este documento está aún pendiente de aprobación por el Comité de Seguridad de la Información, pero en dicho documento se categoriza como NIVEL MEDIO, por lo que no aplicarían las medidas de NIVEL ALTO.

- ✓ *A89 "De las 31 medidas que exige el Anexo II del ENS dentro del Marco operacional, el Ayuntamiento incumple 24 de ellas, como se detalla en el cuadro nº 26:*

Como se ha indicado en el apartado anterior, el informe de la Cámara de Cuentas ha considerado de aplicación las medidas de NIVEL ALTO, cuando según los trabajos que estamos realizando la correcta sería aplicar las medidas de NIVEL MEDIO.

A continuación analizamos las disconformidades establecidas en dichos cuadros (las medidas sombreadas en azul, no aplican a NIVEL MEDIO), con los comentarios en relación a dichas medidas sombreados en gris:

INCUMPLIMIENTOS MARCO OPERACIONAL	
MEDIDA	**INCUMPLIMIENTO**
4.1.1	Carece de documento de análisis de riesgo aprobado formalmente.
	Análisis de Riesgos en proceso, está prácticamente finalizada y en breve se someterá a la aprobación por parte del Comité de Seguridad
4.1.2	Carece de un Sistema de gestión de seguridad de la información.
	En proceso de implantación del ENS
4.1.3	Las adquisiciones de nuevos componentes no han atendido al documento de análisis de riesgos, al no estar formalmente aprobado.
4.1.5	No se siguen las directrices de la Instrucción técnica de Seguridad en lo que respecta a los componentes certificados
	No se aplica en categoría MEDIA
4.2.1	Se permite la utilización de identificadores genéricos.
	Son pocos casos y están en proceso de eliminación
4.2.2	No se dispone de la posibilidad de controlar los accesos, no se activan los registros y no se revisan.
	Se controla el acceso a los recursos, tanto por AD como por BBDD. Los registros de auditoría de acceso están activados. No se revisan periódicamente
4.2.3	Se incumple la auditoría o supervisión de cualquier otra función, dentro del sistema de control de acceso.
4.2.4	La gestión de los derechos de acceso se establece solo por perfiles genéricos.

	Los derechos de acceso atienden a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar
4.2.5	No se emplea el doble factor de autenticación en ninguno de sus sistemas.
	En proceso de implantación para los accesos remotos por VPN
4.2.6	No se registran los accesos con éxitos y/o los fallidos, tras la autenticación de los usuarios.
	Se registran en los logs del AD
	No se informa al usuario del último acceso con su identidad.
4.2.7	Falta establecimiento formal de los permisos a los usuarios que se conectan de forma remota.
	No es así,a los usuarios en VPN se les aplican los mismos permisos que si trabajasen en local
4.3.4	Carece de un procedimiento formal sobre la aplicación de actualizaciones de seguridad.
	Se aplican y revisan periódicamente los parches de seguridad pendientes, pendiente de aprobación de procedimiento formal por el Comité de Seguridad
4.3.5	Carece de un procedimiento formal sobre la gestión del cambio.
	En proceso de elaboración para su aprobación por el Comité de Seguridad
4.3.7	Carece de un procedimiento formal de gestión de incidentes.
	En proceso de elaboración para su aprobación por el Comité de Seguridad
4.3.8	Carece de un registro de la actividad de los usuarios.
	Se revisan periódicamente los registros de actividad buscando patrones anormales. En proceso de licitación de herramienta SIEM
4.3.9	Carece de un registro de la gestión de incidentes.
	Se lleva registro de incidentes a través de la herramienta LUCIA del CCN-CERT
4.3.10	Al carecer de registros de la actividad, se incumple la obligatoriedad de su protección.
	No se aplica en categoría MEDIA
4.3.11	Al no cumplir la medida de los componentes certificados, no se cumple esta medida.
4.4.1	Carece de gestión formal de los acuerdos de servicio con los proveedores.
	Se incluyen en los pliegos los SLAs requeridos
4.4.2	Al no existir una gestión formal de los acuerdos de servicio con los proveedores, esta medida no se cumple.
4.4.3	Carece de medios alternativos en la gestión del servicio.
	No se aplica en categoría MEDIA

4.5.2	Carece de un Plan de Continuidad aprobado formalmente.
	No se aplica en categoría MEDIA
4.5.3	Al carecer de Plan de Continuidad, incumple la obligación de realizar pruebas periódicas del mismo.
	No se aplica en categoría MEDIA
4.6.2	Carece de un Sistema de Métricas.
	Se pueden sacar métricas de los incidentes reportados en LUCIA, así como de otras incidencias reportadas en nuestro sistema de gestión interna (SIM)

INCUMPLIMIENTOS MEDIDAS DE PROTECCIÓN	
MEDIDA	**INCUMPLIMIENTO**
5.1.8	Se incumple la medida por disponer únicamente de una réplica de los datos y del soporte del directorio activo.
	No se aplica en categoría MEDIA. Aun así, se dispone de un CPD de respaldo con una réplica de los datos. Se dispone de varias versiones de las copias de seguridad, así como datos fuera de línea en soporte LTO
5.2.1	Al carecer del análisis de riesgos aprobado, se incumple la medida en relación a la caracterización del puesto de trabajo.
	Se ha definido la responsabilidad de los usuarios finales en la Normativa "SGSI.NS.18 Uso de infraestructuras TIC y de Medios Tecnológicos", pendiente de aprobar por el Comité de Seguridad. Faltan otros aspectos que se definirán en la Normativa "SGSI.NS.04 Seguridad de los Recursos Humanos"
5.2.2	Carece de un régimen disciplinario en el sentido previsto en esta medida.
	Al ser una administración pública, contamos con el régimen disciplinario establecido para los empleados públicos, Además se especifican las medidas disciplinarias en la Normativa "SGSI.NS.18 Uso de infraestructuras TIC y de Medios Tecnológicos", que próximamente va a aprobar por el Comité de Seguridad.
5.2.4	No se realizan cursos de formación específica para el personal en el campo de la ciberseguridad.
	Se remite información periódicamente al respecto sobre avisos, alertas y concienciación a todo el personal. Se van a realizar jornadas formativas, pendientes de licitación para llevar a cabo esta formación
5.2.5	Carece de personal alternativo para dar servicio, al carecer de medios alternativos para darlos.
	No se aplica en categoría MEDIA
5.3.2	Carece de un procedimiento de cancelación de las sesiones abiertas pasado cierto tiempo de inactividad
	No se aplica en categoría MEDIA. SI SE CUMPLE LO QUE APLICA EN CATEGORIA MEDIA: El puesto de trabajo se bloquea al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso
5.3.3	Carece de medidas de control de manipulación, en cuanto a la protección de los portátiles
	No se aplica en categoría MEDIA. Se cumplen los requisitos exigidos para categoría media

5.3.4	Carece de medios alternativos para dar servicio, solo dispone de réplica de datos y del soporte del directorio activo
	Se dispone de un CPD de respaldo con una réplica de los datos así como con capacidad de replicar los servidores en caso de caída del CPD principal
5.4.1	Todos los cortafuegos son del mismo fabricante, por lo incumple la medida en cuanto al perímetro seguro.
	No se aplica en categoría MEDIA. Existe una única barrera de seguridad, cumpliendo con lo exigido en categoría MEDIA. No obstante, nos encontramos pendientes de licitación de una segunda barrera de diferente fabricante para mejorar la seguridad perimetral
5.4.2	Se desconocen los algoritmos con los que desarrollan los certificados.
	Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad, usando algoritmos acreditados por el CCN
5.4.3	Se incumple la medida por no proteger la autenticidad y la integridad
	Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad, usando algoritmos acreditados por el CCN
5.5.2	Se desconocen los algoritmos con los que desarrollan los certificados y no cumple los productos certificados
	Se está llevando control exhaustivo de los dispositivos removibles permitidos, así como el tipo de información almacenada, evitando el uso de los mismos para guardar información confidencial o secreta
5.5.4	Al quebrantarse la medida exigida de protección de claves criptográficas, se incumple esta medida de transporte.
5.5.5	Incumple la exigencia de que se empleen productos certificados para el borrado y destrucción de soportes de información.
5.6.1	No sigue una metodología de desarrollo seguro de las aplicaciones.
5.6.2	Incumple la media por no realizar análisis de vulnerabilidades, ni auditorías de códigos fuente.
	En proceso de licitación análisis de vulnerabilidades y test de penetración. Con respecto al paso previo a producción de las aplicaciones, las pruebas se realizan en un entorno aislado (pre-producción) y las pruebas de aceptación no se realizan con datos reales
5.7.2	Carece de un sistema de categorización de la información.
	En proceso de elaboración de la Normativa "SGSI.NS.02 Clasificación de la Información"
5.7.3	Carece de las condiciones en que ha de ser transmitida o almacenada la información.
	No se aplica en categoría MEDIA
5.7.4	Incumple la obligatoriedad de utilizar componentes certificados.
	No se aplica en categoría MEDIA

5.7.5	Incumple la exigencia de que los sellos de tiempo previenen la posibilidad del repudio posterior.
	No se aplica en categoría MEDIA
5.7.6	Incumple la obligación de retirar en la limpieza de documentos, toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores.
5.7.7	No se realiza copia de seguridad de las aplicaciones y sistemas operativos, ni se hacen copia de las claves.
	Se hacen copias de seguridad, tanto de aplicaciones como de sistemas operativos y datos
5.8.1	Al carecer de medidas para garantizar la confidencialidad, desprotege el cuerpo y los anexos del correo electrónico
	No se carecen de estas medidas, se disponen de medios para proteger a la organización frente a problemas que se materializan por medio del correo electrónico. Por otra parte en la Normativa "SGSI.NS.18 Uso de infraestructuras TIC y de Medios Tecnológicos" se recogen las normas de uso aceptable del correo electrónico corporativo, pendiente de aprobación
5.8.4	Carece de medios alternativos, más allá de la réplica de datos y el controlador del dominio, por lo que no pueden prestar servicio fuera de sus instalaciones.
	No se aplica en categoría MEDIA

En Jerez, a fecha de la firma