SINDICATURA DE COMPTES

Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Vila-real

Ejercicio 2020

INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE VILA-REAL

EJERCICIO 2020

RESUMEN

La auditoría realizada por la Sindicatura de Comptes sobre los controles básicos de ciberseguridad del Ayuntamiento de Vila-real en el ejercicio 2020 ha concluido que, con carácter general, el grado de cumplimiento existente en la gestión de esta materia es de un 49,8% respecto al nivel establecido como objetivo. Esto implica que, aunque existe cierto nivel de efectividad en los controles analizados, es insuficiente y existen claras posibilidades de mejora.

Por otra parte, la valoración de la auditoría sobre el cumplimiento de los aspectos de legalidad representa un índice del 50,0% respecto al nivel establecido como objetivo, una cifra que el órgano fiscalizador considera bastante insatisfactoria.

Este trabajo se enmarca dentro de las auditorías realizadas a los controles básicos de ciberseguridad de los municipios con población superior a 50.000 habitantes de la Comunitat Valenciana, incluidas en los programas anuales de actuación de 2019 y 2020 de la Sindicatura. Con sus valoraciones, la Sindicatura verifica si el marco de ciberseguridad aplicado sobre los sistemas de información garantiza un nivel de control adecuado, incluyendo la protección de la información que gestionan los ayuntamientos y la continuidad de los servicios públicos ofrecidos.

En este sentido, la crisis sanitaria y socioeconómica mundial causada por la pandemia de COVID-19 que marca nuestra realidad en el momento de publicar este informe, ha puesto de manifiesto la total dependencia que tiene la gestión pública de los sistemas de información y las comunicaciones (SIC). Esto hace que administraciones públicas y ayuntamientos sean más vulnerables frente a los ciberataques y que, por tanto, mantener un sólido sistema de protección frente a ellos y una adecuada ciberhigiene sea más necesario que nunca.

Con el propósito de mejorar la gestión de la ciberseguridad en el ente auditado, además del informe con los resultados obtenidos en el trabajo, la Sindicatura ha trasladado al Ayuntamiento de Vila-real el análisis detallado de las deficiencias identificadas y las recomendaciones orientadas a subsanarlas. La mejora de los controles de ciberseguridad requerirá actuaciones e inversiones, tanto en medios materiales como personales, que tienen que ser adecuadamente planificadas. En este sentido, la Sindicatura de Comptes prevé realizar el seguimiento de las recomendaciones como parte del Programa Anual de Actuación de 2021.

La Sindicatura considera que es necesario que los máximos órganos responsables del Ayuntamiento (Pleno, alcalde y la concejalía responsable de las TIC) tomen conciencia de la necesidad de conseguir los niveles exigidos por la normativa para la protección de los sistemas de información ante la multiplicidad de amenazas existentes, a fin de garantizar la consecución de los objetivos de la entidad, la prestación adecuada de servicios a los ciudadanos y la protección de la información y del resto de los activos de los sistemas de información.

NOTA

Este resumen pretende ayudar a la comprensión de los resultados de nuestro Informe y facilitar la labor a los lectores y a los medios de comunicación. Recomendamos su lectura para conocer el verdadero alcance del trabajo realizado.

ÍNDICE **Página**

.

1. INTRODUCCIÓN

En virtud de lo dispuesto en el artículo 8.3 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y según lo previsto en el Programa Anual de Actuación de 2020 (PAA2020) se ha efectuado una auditoría sobre la situación en 2020 de los controles básicos de ciberseguridad (CBCS) de los ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes, entre los que se encuentra el Ayuntamiento de Vila-real.

La realidad de nuestro entorno cercano y del resto de la sociedad española y mundial en el momento de elaborar este informe es la de una crisis sanitaria y socioeconómica sin precedentes provocada por la epidemia del COVID-19. Entre otras muchas cuestiones, esta crisis ha puesto de manifiesto que gran parte de las administraciones públicas y ayuntamientos han sido capaces de continuar en marcha confiando en gran medida en el buen funcionamiento y la eficacia de los sistemas de información y las comunicaciones (SIC).

Esta circunstancia ha mostrado con absoluta claridad la total dependencia de los SIC que existe actualmente en la gestión pública, lo que hace que nuestras administraciones sean más vulnerables frente a los ciberataques y que, por tanto, mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos sea más necesario que nunca.

2. RESPONSABILIDADES DE LOS ÓRGANOS MUNICIPALES EN RELACIÓN CON LOS CONTROLES DE CIBERSEGURIDAD

Los órganos municipales (el Pleno, el alcalde, la Junta de Gobierno y la Secretaría General) son los responsables de que existan unos adecuados controles sobre los sistemas de información y las comunicaciones. De acuerdo con sus competencias deben garantizar que el funcionamiento de la Entidad resulta conforme con las normas aplicables y que los controles internos proporcionan una garantía razonable de que los datos, la información y los activos de los sistemas de información cumplen las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el Esquema Nacional de Seguridad (ENS)[1]:

- Confidencialidad: Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

- Integridad: Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea

[1] Véase el anexo I del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.

- Disponibilidad: Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.

- Autenticidad: Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

- Trazabilidad: Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

La responsabilidad de la Sindicatura de Comptes es concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación sobre su diseño y eficacia operativa, sobre el cumplimiento de la normativa básica relativa a la seguridad de la información y, en su caso, formular recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control. Para ello, hemos llevado a cabo el trabajo de conformidad con los *Principios fundamentales de fiscalización de las instituciones públicas de control externo* y con las normas técnicas de fiscalización aprobadas por el Consell de la Sindicatura recogidas en el *Manual de fiscalización* de la Sindicatura de Comptes. Dichos principios exigen que cumplamos los requerimientos de ética, así como que planifiquemos y ejecutemos la auditoría con el fin de obtener una evaluación de los CBCS.

Ámbito objetivo

La auditoría se ha centrado en el análisis de la situación de los ocho CBCS:

CBCS 1	Inventario y control de dispositivos físicos
CBCS 2	Inventario y control de *software* autorizado y no autorizado
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades
CBCS 4	Uso controlado de privilegios administrativos
CBCS 5	Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores
CBCS 6	Registro de la actividad de los usuarios
CBCS 7	Copias de seguridad de datos y sistemas
CBCS 8	Cumplimiento normativo

Dada la naturaleza del objeto material a revisar –la gran amplitud, complejidad y diversidad de los sistemas de información de un ente local de tamaño grande-, ha sido necesario delimitar y concretar qué sistemas se iban a analizar. En este sentido, hemos analizado las aplicaciones que soportan dos de los procesos de gestión más relevantes a efectos de la Sindicatura, como son la gestión contable y presupuestaria y la gestión tributaria y recaudatoria. La revisión ha incluido los controles relacionados con las aplicaciones informáticas que los soportan.

Además, por su importancia para el buen funcionamiento de los sistemas de información y la ciberseguridad, hemos analizado también una selección de los siguientes tipos de elementos:

- controlador de dominio
- *software* de virtualización
- equipos de usuario
- elementos de la red de comunicaciones (*router*, *switches*, punto de acceso a red wifi, etc.)
- elementos de seguridad (*firewall*, IPS, *proxy* de correo, *proxy* de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.)

Metodología

Esta auditoría de los controles básicos de ciberseguridad ha sido realizada por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI), siguiendo la metodología establecida en la guía *GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad* (integrada en el *Manual de fiscalización* de la Sindicatura de Comptes).

Hemos evaluado la situación de los CBCS utilizando el modelo de nivel de madurez de los procesos ya que, además de ser un sistema ampliamente aceptado, permite establecer objetivos y realizar comparaciones entre entidades distintas y ver la evolución a lo largo del tiempo. La metodología utilizada está plenamente alineada con lo establecido por el ENS y es de aplicación obligatoria en todos los entes públicos.

En el apéndice se proporciona un mayor detalle de la metodología utilizada.

Confidencialidad

Dado que la información utilizada en la auditoría y los resultados detallados de la misma tienen un carácter sensible y pueden afectar a la seguridad de los sistemas de información, los resultados detallados de cada uno de los controles solo se comunican con carácter confidencial a los responsables del Ayuntamiento para que puedan adoptar las medidas

correctoras que consideren precisas. En el presente informe los resultados se muestran de forma sintética.

Limitación al alcance de la revisión

El alcance específico del presente trabajo de revisión de controles básicos de ciberseguridad se encuentra condicionado por la organización funcional del Ayuntamiento.

Tal y como se establece en el "Documento de seguridad de los sistemas de información y de administración electrónica del Ajuntament de Vila-real", el Ayuntamiento dispone de sistemas centralizados, gestionados por el Servicio de Nuevas Tecnologías (SNT), y sistemas descentralizados, gestionados de manera autónoma por los servicios correspondientes, sin control del SNT. Esta norma establece que los responsables de los sistemas descentralizados deben gestionar determinados procesos de seguridad, como:

- el inventario de *hardware* y *software*
- la gestión de usuarios y privilegios administrativos
- la realización de copias de seguridad

Los sistemas descentralizados de los que hemos tenido conocimiento son:

- La Servicio Municipal de Deportes.
- La Policía Local.
- Servicio de Telecomunicaciones.
- Servicios Públicos Municipales.

Existen por tanto determinados procesos de seguridad sobre los sistemas descentralizados cuya responsabilidad no está definida (todos excepto los tres indicados).

La provisión del servicio de Internet y de infraestructura física de red la realiza el Servicio de Telecomunicaciones del Ayuntamiento, tanto para los sistemas centralizados como para los descentralizados. La conmutación y el enrutamiento de los sistemas centralizados se realiza desde la infraestructura del SNT, mientras que los sistemas descentralizados los proporcionados por el Servicio de Telecomunicaciones.

El presente trabajo únicamente ha comprendido el análisis de los controles de seguridad implantados sobre los sistemas centralizados y de aquellos controles implantados en sistemas descentralizados de la Policía Local. Por tanto, los controles y procesos de seguridad no revisados, no han sido considerados a efectos de puntuación de cada uno de los CBCS, aunque consideramos que su valoración no tendría un efecto positivo sobre los indicadores obtenidos.

4. CONCLUSIONES

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el grado de control existente en la gestión de los CBCS señalados en el apartado 3, alcanza un índice de madurez del 39,8%, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*; es decir, los procesos de control existen, pero su gestión no está correctamente organizada.

En el cuadro siguiente se muestran de forma detallada los resultados de la evaluación realizada para cada uno de los CBCS.

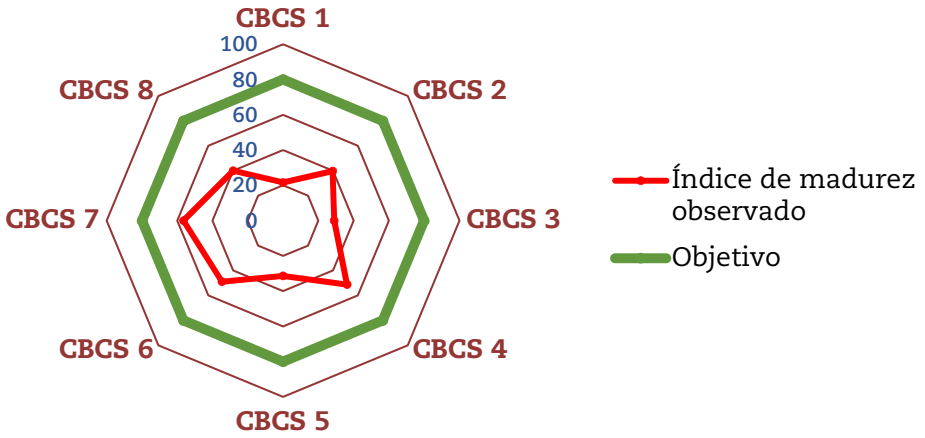
Cuadro 1. Índice y nivel de madurez de los CBCS del Ayuntamiento

Control	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	21,6%	N1	27,0%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	39,8%	N1	49,7%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	29,0%	N1	36,2%
CBCS 4 Uso controlado de privilegios administrativos	51,3%	N2	64,1%
CBCS 5 Configuraciones seguras del *software* y *hardware*	31,4%	N1	39,2%
CBCS 6 Registro de la actividad de los usuarios	49,0%	N1	61,3%
CBCS 7 Copias de seguridad de datos y sistemas	56,5%	N2	70,6%
CBCS 8 Cumplimiento normativo	40,0%	N1	50,0%
Índice/Nivel global del Ayuntamiento	**39,8%**	**N1**	**49,8%**
Índice/Nivel requerido u objetivo	**80,0%**	**N3**	**100,0%**

Los sistemas de información revisados están clasificados como de categoría de seguridad MEDIA. Así, acorde con esta categoría, el nivel de madurez requerido por el ENS y que también lo aplicamos para los CBCS en esta auditoría es *N3, proceso definido* y un índice de madurez del 80%.

En consecuencia, el índice de cumplimiento de los CBCS alcanzado es del 49,8% (el objetivo es el 100%), que resulta de comparar el indicador de madurez observado con el nivel requerido u objetivo que debe tener el sistema según el ENS.

Gráfico 1. Índice de madurez de los CBCS



A la vista de los resultados obtenidos en la revisión, se concluye que, aunque existe cierto nivel de efectividad en los controles analizados, existen claras posibilidades de mejora. Por tanto, es necesario que los máximos órganos responsables del Ayuntamiento (Pleno, alcalde y la concejalía responsable de las TIC) tomen conciencia de la necesidad de alcanzar los niveles exigidos por la normativa para la protección de los sistemas de información frente a la multiplicidad de amenazas existentes, con objeto de garantizar la consecución de los objetivos de la entidad, la adecuada prestación de servicios a los ciudadanos y la protección de la información y del resto de los activos de los sistemas de información. Esta cultura de ciberseguridad se debe trasladar a todos los niveles y departamentos del Ayuntamiento.

La mejora de los controles de ciberseguridad requerirá de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas.

Además, la revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel de cumplimiento bastante insatisfactorio. Los máximos órganos de dirección del Ayuntamiento tienen la responsabilidad de garantizar un nivel adecuado de cumplimiento de las normas legales y deben impulsar las medidas necesarias para subsanar la situación.

Hemos confirmado que el SNT no considera los sistemas descentralizados en ninguno de sus procesos de control de seguridad, y la única obligación formal para los responsables de estos sistemas descentralizados es el inventariado, la gestión de usuarios y privilegios y la realización de copias de seguridad. En consecuencia, existen numerosos controles sobre los que la responsabilidad de su aplicación se encuentra indefinida. Por el alcance fijado en nuestra revisión, los efectos de esta circunstancia no han sido considerados al cuantificar el índice de madurez.

Hemos observado que, contrariamente a lo establecido en la normativa interna, no se dispone de una relación o inventario de sistemas descentralizados autorizados. Tampoco existe un procedimiento de autorización para su creación e incorporación a la red corporativa, carencia que constituye un factor de riesgo por falta de control desde el punto de vista de la gestión integral de la seguridad.

Debido a la peculiar organización funcional de los sistemas de información en el ayuntamiento, consideramos como factor adicional de riesgo la carencia de un responsable de seguridad del conjunto de los sistemas de información del Ayuntamiento, tal y como exige el artículo 10 del Real Decreto 3/2010 (ENS), que vele por la aplicación homogénea de las medidas de seguridad del ENS en la totalidad de los sistemas de la entidad y particularmente en un entorno de sistemas descentralizados

5. SITUACIÓN DE LOS CONTROLES

A continuación, se detallan los principales aspectos surgidos en la revisión de cada uno de los CBCS del Ayuntamiento.

1. *Sobre el inventario y control de dispositivos físicos (CBCS 1)*

Hemos verificado que el Ayuntamiento realiza algunas acciones para el inventario y control de activos físicos de la entidad, si bien dichas acciones no garantizan un control efectivo sobre ellos.

La normativa de seguridad aprobada por la Junta de Administración Electrónica, Seguridad de la Información y Transparencia, del Ayuntamiento de Vila-real (JAESIT) recoge la obligación de los responsables de la información de cada sistema descentralizado de realizar el inventariado de los elementos de *hardware* que componen dichos sistemas, pero el procedimiento no ha sido desarrollado ni aprobado.

Esta norma no considera el inventariado de los equipos de usuario a excepción de ordenadores portátiles. Dicha carencia limita la posterior aplicación de otros controles de seguridad relevantes sobre dichos dispositivos no controlados. Así, los equipos *thinclients*, de uso mayoritario en el Ayuntamiento, no se encuentran inventariados por ningún sistema.

El SNT dispone de dos inventarios de gestión manual para la administración de determinados activos: un inventario de elementos del CPD, que es una herramienta crítica de administración y se mantiene correctamente actualizado, y un inventario de ordenadores portátiles e impresoras, que se encuentra en fase de implantación y únicamente dispone de información de activos de determinados departamentos.

Se ha evidenciado en la revisión de una muestra de los sistemas descentralizados más representativos, que los responsables de dichos sistemas disponen de inventarios de activos físicos. El inventariado de los elementos es en todos los casos un proceso manual no gestionable que no hace uso de herramientas específicas. El resultado del proceso no permite asegurar la existencia de inventarios completamente actualizados, siendo el nivel de actualización desigual para cada uno de los sistemas descentralizados.

Por otra parte, hemos constatado que no existe un control robusto que impida la conexión de dispositivos físicos no autorizados a los sistemas de información, dado que únicamente se han implantado controles de efectividad parcial.

En síntesis, existe un nivel de control insuficiente sobre el inventario de dispositivos físicos, y la valoración global del control alcanza un índice de madurez del 21,6%, que se corresponde con un nivel de madurez *N1, inicial/ad hoc;* es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 1 del 27,0%.

2. *Sobre el inventario y control de software autorizado (CBCS 2)*

Hemos analizado la gestión que realiza el Ayuntamiento sobre el inventario y control de *software* y hemos verificado que, si bien la responsabilidad del inventariado de *software* se encuentra establecida en la normativa de seguridad vigente, no existe un procedimiento formalmente aprobado que recoja las medidas de seguridad que se deben aplicar.

El Ayuntamiento ha virtualizado la totalidad de las aplicaciones municipales centralizadas, siendo el inventario de *software* el catálogo de aplicaciones de la herramienta de virtualización. La gestión de usuarios y derechos de acceso a dichas aplicaciones se realiza mediante un proceso adecuado que incluye la revisión y aprobación de permisos y que se encuentra recogido en un procedimiento que no ha sido aprobado.

El presente trabajo no ha incluido en su alcance la revisión del inventario de *software* de los sistemas descentralizados.

Por otra parte, se ha evidenciado la existencia de un elevado número de equipos con sistemas operativos fuera del periodo de soporte del fabricante, particularmente servidores, hecho que supone un grave riesgo para el sistema de información.

La gestión del licenciamiento y el mantenimiento de aplicaciones comerciales la realiza el Servicio de Nuevas Tecnologías mediante un

proceso adecuado y gestionable, pero no está formalizado por escrito.

La entidad cuenta con medidas orientadas a impedir el uso de *software* no autorizado en los sistemas centralizados que pueden considerarse efectivas.

Consideramos insuficiente el nivel de control sobre el inventario y el *software* autorizado, por lo que se deberán dedicar esfuerzos y recursos para mejorarlo. La valoración global del control alcanza un índice de madurez del 39,8%, que se corresponde con un nivel de madurez N1, *inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 2 del 49,7%.

3. *Sobre el proceso continuo de identificación y remediación de vulnerabilidades (CBCS 3)*

Hemos analizado la gestión de vulnerabilidades realizada por el Ayuntamiento y hemos observado que se efectúan algunas acciones con el objeto de identificar y remediar vulnerabilidades, pero dichas acciones no han sido implantadas de manera efectiva en todos los sistemas, ni han sido formalmente establecidas en un procedimiento aprobado.

La identificación y remediación de vulnerabilidades únicamente se realiza sobre determinados sistemas incluidos en nuestro alcance, bien de manera manual mediante la búsqueda y resolución de ciertas vulnerabilidades críticas, bien por parte de terceros mediante contratos de mantenimiento de determinados sistemas. En ningún caso se utilizan herramientas específicas para la identificación de vulnerabilidades. El proceso de priorización y resolución de estas vulnerabilidades es gestionado de manera informal y no se encuentra contemplado en un procedimiento.

Existen, por tanto, determinados sistemas sobre los que no se ha establecido ningún tipo de acción para la identificación y remediación de vulnerabilidades, hecho que constituye una importante deficiencia de control.

Sobre la aplicación de parches y actualizaciones de seguridad, de manera general, únicamente se aplican de modo sistemático sobre determinados sistemas cuya actualización se establece en contratos de mantenimiento con terceros. Para el resto de sistemas y particularmente para los sistemas Windows, no ha sido implantado un proceso de control sobre los parches y actualizaciones, carencia que puede suponer un grave riesgo para la seguridad de los sistemas de la entidad. No obstante, se ha evidenciado el compromiso del Servicio de Nuevas Tecnologías y Modernización por implantar una

herramienta para la gestión centralizada de actualizaciones de los sistemas Windows, si bien esta herramienta no se encontraba funcional y en producción.

Para aquellos sistemas descentralizados que no son gestionados por el SNT, no se han verificado las medidas implantadas dado que se encuentran fuera del alcance del trabajo.

Consideramos que existe un nivel de control insuficiente, por lo que se deberán dedicar esfuerzos y recursos para mejorarlo. La valoración global del control alcanza un índice de madurez del 29,0%, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 3 del 36,2%.

4. *Sobre el uso controlado de privilegios administrativos (CBCS 4)*

Hemos analizado las acciones que se realizan para el control de las cuentas de administración y hemos verificado que existe un control parcialmente efectivo.

La responsabilidad de la gestión de usuarios está establecida en la normativa de seguridad y se diferencia entre sistemas centralizados, gestionados por el SNT, y sistemas descentralizados, gestionados por los propios responsables de los sistemas. Se han implantado determinadas medidas efectivas para el control de cuentas de administración, pero estas medidas no han sido formalmente detalladas en un procedimiento aprobado y no se encuentran implantadas de manera homogénea en todos los sistemas.

La gestión de la asignación de privilegios administrativos en los sistemas incluidos en el alcance de la fiscalización se realiza con distinto grado de efectividad dependiendo del sistema. Para los sistemas incluidos en el dominio y aquellos que realizan la autenticación a través del directorio activo mediante SSO (*single sign on*) se ha evidenciado un uso adecuado de usuarios nominativos y del cumplimiento del criterio de mínimo privilegio.

Se ha detectado el uso de cuentas de administración no nominativas en dos de los sistemas incluidos en el alcance de la fiscalización, lo que impide la trazabilidad de las acciones en caso de incidentes y constituye la deficiencia más significativa detectada.

Dado que únicamente se han establecido técnicamente requisitos de autenticación en los sistemas Windows del dominio y en aquellos que han implementado SSO con el directorio activo, no se aplica una política de autenticación homogénea en todos los sistemas o la política aplicada no es robusta en todos los casos.

Se ha confirmado la existencia de identificadores diferenciados para un mismo usuario, dependiendo del tipo de tarea a desempeñar en el sistema, con objeto de limitar el uso de identificadores con privilegios administrativos en las tareas que no lo requieren.

Sobre la gestión de usuarios administradores en los sistemas descentralizados, se ha evidenciado un uso adecuado de usuarios nominativos y el cumplimiento del criterio de mínimo privilegio. Si bien con desigual efectividad en cada sistema, pueden considerarse establecidos controles sobre los mecanismos de autenticación y el registro de actividad. No obstante, no ha sido posible revisar la gestión de usuarios administradores de todos los sistemas descentralizados representativos del Ayuntamiento.

Consideramos que existe cierto nivel de control sobre las cuentas de usuarios administradores, pero hay posibilidades de mejora. La valoración global de este control alcanza un índice de madurez del 51,3%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados debidamente. Esto representa un índice de cumplimiento del CBCS 4 del 64,1%.

5. *Sobre las configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores (CBCS 5)*

Hemos analizado las acciones realizadas para el control de la configuración segura en aplicaciones y dispositivos y hemos verificado que no existe un procedimiento formalmente aprobado a tal efecto. Aunque la entidad aplica configuraciones de seguridad en determinados sistemas, dichas acciones no son suficientes para asegurar la efectividad del control.

Si bien se ha evidenciado que se dispone de plantillas para la configuración de determinados dispositivos, estas no tienen carácter de bastionado ni la seguridad por defecto es su objeto.

Existe, por tanto, un deficiente nivel de control en la aplicación de configuraciones seguras en dispositivos y *software*, por lo que se deberán dedicar esfuerzos y recursos para mejorarla. La valoración global del control alcanza un índice de madurez del 31,4%, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un índice de cumplimiento del CBCS 5 del 39,2%.

6. Sobre el registro de la actividad de los usuarios (CBCS 6)

Hemos analizado los procedimientos aplicados por el Ayuntamiento para el registro de la actividad de los usuarios en los distintos sistemas y hemos verificado que, aunque se dispone de ciertos controles relacionados con este procedimiento, estos no han sido formalmente establecidos y aprobados.

En la normativa aprobada han sido recogidas únicamente las obligaciones del Ayuntamiento con respecto al almacenamiento y revisión de registros de acceso de los sistemas que traten datos personales de especial protección.

Hemos verificado que el registro de actividad se encuentra activado en los sistemas del alcance de la revisión, si bien se mantiene la configuración por defecto que define el fabricante.

El Ayuntamiento dispone de dos sistemas para la gestión centralizada de registros de actividad de determinados activos, lo que supone una mejora de la configuración básica por defecto de los *logs* de auditoría. No obstante, estas herramientas no integran todos los sistemas relevantes desde el punto de vista de la ciberseguridad y la revisión de dichos registros de actividad se realiza de forma informal, no procedimentada.

Por tanto, existe un deficiente nivel de control y su valoración alcanza un índice de madurez del 49,0%, que se corresponde con un nivel de madurez N1, inicial/ad hoc; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados debidamente. Esto representa un índice de cumplimiento del CBCS 6 del 61,3%.

7. Sobre la copia de seguridad de datos y sistemas (CBCS 7)

El Ayuntamiento realiza diversas acciones para el control de las copias de seguridad de los datos y sistemas. La responsabilidad de la realización de copias de seguridad se encuentra establecida en la normativa de seguridad vigente y el proceso se encuentra correctamente definido e implantado, pero no ha sido recogido en un procedimiento formalmente aprobado.

Las políticas de copia aplicadas a los sistemas ubicados en los servidores centrales del Ayuntamiento han sido desarrolladas de acuerdo con las necesidades identificadas desde el propio SNT y se aplican de manera efectiva. No obstante, el resultado de los trabajos de copia es revisado mediante un proceso manual que no se encuentra adecuadamente definido y gestionado.

Se ha confirmado que el SNT realiza de forma sistemática pruebas de recuperación planificadas como parte de un proceso de pruebas en entorno de preproducción para la implantación de nuevos sistemas y gestión de cambios.

Asimismo, las medidas implantadas para la protección de las copias del SNT pueden considerarse eficaces. No obstante, se ha evidenciado que las copias de seguridad ubicadas en un edificio que actúa como nodo secundario de la red municipal, han sido emplazadas en un local que no dispone de todas las condiciones de adecuación física requeridas, a pesar de existir en el mismo edificio locales correctamente acondicionados para tal fin.

La normativa de seguridad aprobada recoge la obligación de los responsables de la información de cada sistema descentralizado de realizar, almacenar, verificar y recuperar las copias de dichos sistemas. Se ha evidenciado la existencia de copias de seguridad de datos y sistemas en aquellos sistemas descentralizados que lo requieren. En algunos, la gestión de copias se encuentra externalizada, y en el resto, las copias de seguridad no se encuentran protegidas con todos los recursos técnicos disponibles en el Ayuntamiento.

Existe cierto nivel de control sobre las copias de seguridad de datos y sistemas, pero existen posibilidades de mejora. La valoración global del control alcanza un índice de madurez del 56,5%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados debidamente. Esto representa un índice de cumplimiento del CBCS 7 del 70,6%.

8. *Sobre el cumplimiento de la legalidad (CBCS 8)*

El Ayuntamiento ha incurrido en un nivel elevado de incumplimientos legales, alguno de ellos graves, por lo que la valoración global sobre el cumplimiento de los aspectos de legalidad que hemos verificado[2] es que el Ayuntamiento alcanza un índice de madurez del 40,0%. Esto se corresponde con un nivel de madurez *N1*, que indica que existen incumplimientos significativos generalizados de la normativa. Esto representa un índice de cumplimiento del CBCS 8 del 50,0%.

[2] ENS, RGPD, Ley Orgánica 3/2018, de 5 de diciembre y Ley 25/2013, de 27 de diciembre, de Impulso de la Factura Electrónica.

En relación con el ENS

El Ayuntamiento dispone de una política de seguridad aprobada por el órgano superior competente que precisa objetivos y misión de la organización, marco legal y normativo, definición de roles y funciones, estructura organizativa y el proceso de aprobación y revisión.

Se han constituido los órganos definidos en la política de seguridad, particularmente la Junta de Administración Electrónica, Seguridad de la Información y Transparencia, del Ayuntamiento de Vila-real (JAESIT).

Se ha cumplimentado y remitido el Informe del Estado de la Seguridad (Informe INES).

Se han realizado las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010.

Sin embargo:

- No ha elaborado una declaración de aplicabilidad ni ha adoptado las medidas de seguridad allí descritas.

- No se han publicado en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes previstos en el ENS.

- No se ha realizado la designación de las personas para los roles definidos en la política de seguridad. La carencia de un responsable de seguridad del conjunto de los sistemas de información, tal y como exige el artículo 10 del Real Decreto 3/2010 (ENS), que vele por la aplicación homogénea de medidas de seguridad en la totalidad de los sistemas de la entidad y particularmente en un entorno de sistemas descentralizados, representa un factor de riesgo importante.

En materia de protección de datos personales

Se ha nombrado un delegado de protección de datos (DPD) de acuerdo con lo previsto en el artículo 37.1 a) del RGPD.

Se ha elaborado el registro de actividades de tratamiento de la información requerida por el RGPD y se ha publicado dicho registro, conforme al artículo 31.2 de la Ley Orgánica 3/2018.

Se ha realizado un análisis de riesgos sobre sus tratamientos de datos personales y las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.

Se han ejecutado auditorías de cumplimiento en materia de protección de datos.

En relación con la Ley de Factura Electrónica

Se han llevado a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.

6. RECOMENDACIONES Y MEDIDAS PARA EL CUMPLIMIENTO DE LA LEGALIDAD

Como resultado de la auditoría realizada procede efectuar las recomendaciones que se señalan a continuación, para cuya atención el Ayuntamiento deberá dedicar los esfuerzos y recursos necesarios. También se señalan las medidas para el cumplimiento de la legalidad que deben adoptarse.

Sobre el inventario y control de dispositivos físicos (CBCS 1)

1) Aprobar formalmente un procedimiento para la gestión del inventario y el control de activos físicos que recoja el proceso completo, incluyendo las revisiones periódicas de *hardware*, actualizando debidamente el inventario e incluyendo las fechas de dichas revisiones.

   A la hora de garantizar un nivel de actualización adecuado del inventario, es aconsejable primar el uso de herramientas para la detección y actualización automática de los elementos del sistema de información frente a procedimientos manuales.

2) Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.

Sobre el inventario y control de software autorizado (CBCS 2)

3) Elaborar y aprobar un procedimiento para la gestión integral del *software* de la entidad que contemple:

   - La elaboración de listas de *software* autorizado (listas blancas), la implantación de las medidas técnicas que impidan la ejecución del no autorizado y la realización de revisiones periódicas de *software*.

   - La definición de un plan de mantenimiento de la totalidad del *software* utilizado en el Ayuntamiento.

4) Identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte.

Sobre el proceso continuo de identificación y remediación de vulnerabilidades (CBCS 3)

5) Aprobar un procedimiento de identificación y remediación de vulnerabilidades que formalice y amplíe el proceso actual, que se aplique a la totalidad de sistemas del Ayuntamiento y que considere, como mínimo, los siguientes aspectos:

   - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas, el análisis previo a la entrada en producción de los sistemas y las acciones actualmente establecidas de seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad.

   - La priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.

6) Implantar herramientas que permitan la gestión unificada y automatizada de parches de seguridad y otras actualizaciones.

7) Optimizar la explotación de la información proporcionada por la sonda del CCN[3], incluyendo los avisos proporcionados en el proceso de resolución de vulnerabilidades.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

8) Formalizar un único procedimiento unificado de gestión de usuarios con privilegios de administración que establezca las directrices para todos los sistemas de la entidad y que incluya:

   - La eliminación, siempre que sea posible desde el punto de vista técnico, de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos.

   - Cuando existan razones de índole técnico que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas.

Sobre las configuraciones seguras del software y hardware (CBCS 5)

9) Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones

[3] Centro Criptológico Nacional

de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN[4].

Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la revisión periódica de los cambios realizados, bien mediante procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.

Sobre el registro de la actividad de los usuarios (CBCS 6)

10) Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de actividad de usuario que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Para la revisión de *logs* es aconsejable la centralización de estos en sistemas dedicados a tal efecto.

Sobre la copia de seguridad de datos y sistemas (CBCS 7)

11) Aprobar formalmente un procedimiento para la gestión de copias de seguridad de datos y sistemas que defina, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas de restauración y los requisitos de protección de las copias.

12) Ubicar las copias de seguridad localizadas en el nodo secundario de la red municipal en el local correctamente acondicionado para tal fin disponible en el mismo edificio.

Sobre el cumplimiento de la legalidad (CBCS 8)

13) Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe:

- Designar las personas para los roles definidos en la política de seguridad y constitución de los órganos allí descritos.

- Elaborar una declaración de aplicabilidad y adoptar las medidas de seguridad allí descritas.

[4] Las guías STIC (seguridad de las tecnologías de la información y de las comunicaciones) están estructuradas en series. Las series a las que hace referencia la recomendación corresponde a "guías generales", "guías de entornos Windows" y "guías de otros entornos" respectivamente.

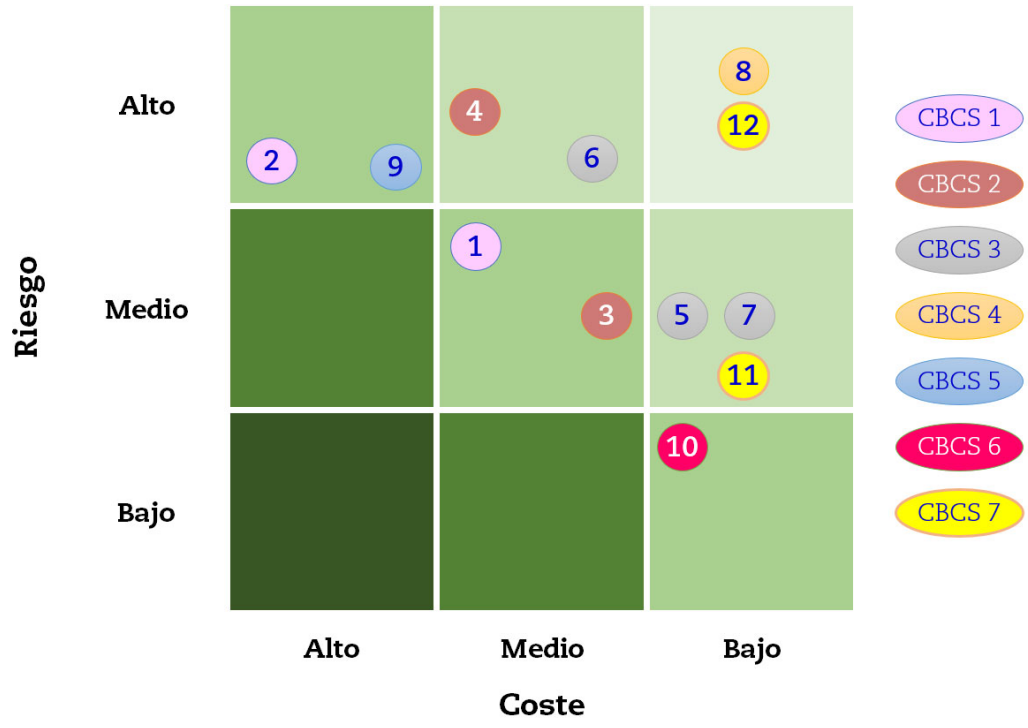
- Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS del 13 de octubre de 2016.

14) En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular, debe aplicar la totalidad de medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico 2 se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación. No se incluyen las medidas a implantar 13) a 14) por ser exigencias legales.

Gráfico 2. Riesgos que se atienden y coste de implantación de las recomendaciones



Además de las recomendaciones anteriores, junto con el detalle al máximo nivel de las deficiencias de seguridad observadas, se ha comunicado a los responsables del Ayuntamiento otras recomendaciones con una relación de riesgo potencial a mitigar y coste de su implantación menos favorable que las anteriores.

APÉNDICE. Metodología aplicada

1. La GPF-OCEX 5313 y el Esquema Nacional de Seguridad

La presente auditoría está basada en la Guía práctica de fiscalización de los OCEX ***GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad*** aprobada por la Conferencia de Presidentes de los Órganos de Control Externo el 12/11/2018, que forma parte del *Manual de fiscalización* de la Sindicatura de Comptes y que puede consultarse en nuestra web. Para mayor detalle sobre la metodología utilizada nos remitimos a esa guía.

El contenido de la GPF-OCEX 5313, fundamentalmente relacionado con la auditoría de la seguridad de los sistemas de información, es coherente con los postulados del ENS, que es de obligado cumplimiento para todos los entes públicos. Esta alineación facilita la realización de las auditorías de ciberseguridad por parte de la Sindicatura y coadyuva a la implantación del ENS en los entes auditados, ya que prácticamente todos los subcontroles o controles detallados que verifica la Sindicatura están exigidos por el ENS.

No obstante, dada la amplitud del ENS, que está formado por 75 medidas de seguridad, para su inclusión en los CBCS se seleccionó una serie limitada de controles. Para seleccionar los más relevantes se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security (CIS[5]), que prioriza y clasifica los controles según su importancia para hacer frente a las ciberamenazas.

Los 20 controles de seguridad críticos del CIS son un conjunto conciso y priorizado de acciones de ciberdefensa, orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. La versión 7 de los controles CIS clasifica los seis primeros controles como básicos y son los que se han utilizado como referencia en la GPF-OCEX 5313 para establecer los controles básicos de ciberseguridad (CBCS) de los OCEX. A ellos se añadió el relativo a las copias de seguridad de datos y sistemas -por su importancia para la recuperación frente a un desastre o ataque exitoso y por tanto para garantizar una razonable ciber-resiliencia- y un octavo CBCS relacionado con el cumplimiento normativo, por su importancia en una administración pública.

[5] Center for Internet Security, www.cisecurity.org.

Los ocho controles básicos de ciberseguridad debidamente referenciados con el ENS son:

Cuadro 2. Los CBCS y el ENS

Control		Medida de seguridad del ENS
CBCS 1	Inventario y control de dispositivos físicos	op.exp.1
CBCS 2	Inventario y control de *software* autorizado y no autorizado	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	op.acc.4 op.acc.5
CBCS 5	Configuraciones seguras del *software* y *hardware*, dispositivos móviles, portátiles, equipos de sobremesa y servidores	op.exp.2 op.exp.3
CBCS 6	Registro de la actividad de los usuarios	op.exp.8 op.exp.10
CBCS 7	Copias de seguridad de datos y sistemas	mp.info.9
CBCS 8	Cumplimiento de la legalidad	ENS RGPD/LOPD Ley 25/2013

2. Criterios de auditoría: los controles básicos de ciberseguridad y sus subcontroles

Los CBCS son controles globales formados por varios subcontroles detallados que se muestran en la siguiente tabla. Todas nuestras comprobaciones tienen por finalidad contrastar su situación real en la entidad con las buenas prácticas recogidas en la GPF-OCEX 5313, que se resumen en el siguiente cuadro.

Los aspectos que se comprueban en cada CBCS se especifican con el máximo detalle en la GPF-OCEX 5313.

En cuanto a los índices o niveles objetivo que debe alcanzarse en cada CBCS y subcontrol, véase el apartado 4 siguiente.

Cuadro 3. Los CBCS y sus subcontroles

Control	Objetivo de control	Subcontrol	
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.
		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	Gestionar activamente todo el *software* en los sistemas, de forma que sólo 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.
		CBCS 2-2: SW soportado por el fabricante	El SW utilizado por la entidad tiene soporte del fabricante. En caso contrario, se marca en el inventario como fuera de soporte.
		CBCS 2-3: Control de SW no autorizado	La entidad dispone de mecanismos que impiden la instalación y ejecución de SW no autorizado.
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	CBCS 3-1: Identificación de vulnerabilidades	Existe un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que estas son identificadas en tiempo oportuno.
		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 ordenadores, redes y aplicaciones.	CBCS 4-1: Inventario y control de cuentas de administración	Los privilegios de administración están limitados adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita su correcto control.
		CBCS 4-2: Cambio de contraseñas por defecto	Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares, se cambian antes de la entrada en producción del sistema.
		CBCS 4-3: Uso dedicado de cuentas de administración	Las cuentas de administración solo se realizan 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.

Control	Objetivo de control	Subcontrol	
CBCS 5 Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Establecer, implantar y gestionar la configuración de seguridad de los dispositivos móviles, portátiles, servidores y de sobremesa, mediante un proceso de control de cambios y gestión de la configuración riguroso, con el objetivo de prevenir ataques mediante la explotación de servicios y configuraciones vulnerables.	CBCS 5-1: Configuración segura	La entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y SW
		CBCS 5-2: Gestión de la configuración	La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.
CBCS 6 Registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría)	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.
		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 riesgos de seguridad del sistema. Se dispone de mecanismos para la centralización de los *logs* de auditoría, de forma que se facilite su revisión.
		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*.
CBCS 7 Copia 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.
		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 de Legalidad	La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación.	CBCS 8-1: Cumplimiento del ENS	La Entidad cumple con los requerimientos establecidos en el ENS.
		CBCS 8-2: Cumplimiento de la LOPD/RGPD	La Entidad cumple con los requerimientos establecidos en la LOPD/RGPD
		CBCS 8-3: Cumplimiento de la Ley 25/2013	La Entidad cumple con los requerimientos establecidos en la Ley 25/2013, de 27 de diciembre.

3. *Confianza en las auditorías del ENS*

Dado que los CBCS están alineados con el ENS, cuando su revisión se realice en entidades que hayan pasado la auditoría de seguridad obligatoria establecida en el artículo 34 del Real Decreto 3/2010 por el que se aprueba el ENS, la revisión podrá basarse, en la medida de lo posible, en los resultados de dicha auditoría y determinadas comprobaciones podrán darse por cumplidas.

Para depositar confianza en dichas auditorías externas de seguridad, deberán cumplir con los requisitos legalmente establecidos como son, entre otros, que las entidades certificadoras estén acreditadas y constar en la sección "Entidades de certificación acreditadas de la página web del CCN (es necesario su acreditarlas si se pretende certificar el cumplimiento del ENS). Cuando se haya depositado confianza en estas auditorías se señalará expresamente en el informe.

4. Evaluación de los resultados del trabajo

Los resultados del trabajo se analizan y evalúan a dos niveles: subcontroles y CBCS.

Subcontroles

Los CBCS son controles globales compuestos por varios controles detallados o subcontroles (tal como puede verse en el apartado 2 anterior), de los que hemos revisado su diseño y eficacia operativa.

El trabajo de auditoría consiste básicamente en evaluar cada subcontrol en función de los resultados de las pruebas realizadas y las evidencias obtenidas, o bien de la información proporcionada en el informe de auditoría del ENS, si existe y si confiamos en él. Cada subcontrol se evalúa según la escala mostrada en el siguiente cuadro:

Cuadro 4. Evaluación 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 éste 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).

Nivel de madurez de los CBCS

Para determinar la situación global de cada control básico de ciberseguridad hemos utilizado el modelo de nivel de madurez de los procesos de control de acuerdo con lo establecido en la *GPF-OCEX 5313*, que a su vez está basada en la *Guía de seguridad CCN-STIC 804* del Centro Criptológico Nacional, usando una escala, según se resume en el siguiente cuadro.

Cuadro 5. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El CBCS no está siendo aplicado en este momento.
N1 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.*
N2 Repetible, pero intuitivo	50	Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas. No hay 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.*
N3 Proceso definido	80	Los procesos están estandarizados, documentados y comunicados con acciones formativas. *Se dispone de un catálogo de procesos que se mantiene actualizado. Estos 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.*
N4 Gestionado y medible	90	La dirección controla y mide el cumplimiento de 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 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*

Nivel	Índice	Descripción
		confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.
N5 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.*

La evaluación que realizamos sobre el nivel de madurez no se ha basado únicamente en los procesos teóricos o en los procedimientos aprobados, sino también en la verificación de su aplicación práctica.

Para evaluar el nivel de madurez de cada CBCS se han tenido en cuenta los resultados obtenidos en la revisión de los subcontroles que lo forman y considerando la ponderación o importancia relativa que les asignamos para el cumplimiento del objetivo de control del CBCS.

Este modelo proporciona una base sólida para formarse una idea general de la situación en la entidad revisada en relación con los controles de ciberseguridad y el cumplimiento de la legalidad en esta materia. También permite comparar resultados entre distintos entes y entre distintos periodos.

5. Nivel de madurez mínimo requerido en función de la categoría de los sistemas de información auditados

A los sistemas de las tecnologías de la información y la comunicación de los organismos del sector público obligados al cumplimiento del ENS se les asigna una categoría en función de la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

La categoría de un sistema será de aplicación a todos los sistemas empleados para la prestación de los servicios de la administración electrónica y soporte

del procedimiento administrativo general de un ente.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se deben tener en cuenta las cinco dimensiones de la seguridad:

Confidencialidad	Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Integridad	Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.
Disponibilidad	Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
Autenticidad	Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Trazabilidad	Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO.

Teniendo en cuenta lo anterior, se definen tres categorías de sistemas de información:

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

La categoría de un sistema de información, en materia de seguridad, modula el equilibrio entre la importancia de la información que maneja, de los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

De acuerdo con la categoría de cada sistema, los niveles mínimos de exigencia o de madurez requeridos son[6]:

Categoría del sistema	Nivel mínimo de exigencia/madurez requerido
BÁSICA	N2 – Reproducible, pero intuitivo (50%)
MEDIA	N3 – Proceso definido (80%)
ALTA	N4 – Gestionado y medible (90%)

Los sistemas auditados en el presente informe están clasificados como de categoría MEDIA.

Por tanto, hemos analizado si los resultados obtenidos de acuerdo con el modelo de nivel de madurez alcanzan el nivel mínimo de exigencia requerido en el ENS, que en el presente caso es el *N3 – Proceso definido* y un índice de madurez del 80%.

6. Indicadores globales

A efectos del ENS, la guía CCN-STIC-824 contempla una serie de indicadores agregados capaces de aportar información resumida sobre el estado de la seguridad en los organismos públicos. Dichos indicadores han sido adaptados para su aplicación a los CBCS ya que permiten llevar a cabo tanto un resumen del estado de las medidas de seguridad de cada ayuntamiento a los efectos del ENS, como de los CBCS:

- El índice de madurez sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de CBCS.

- El índice de cumplimiento analiza igualmente el nivel de madurez alcanzado, pero en relación a la exigencia aplicable en cada caso, teniendo en cuenta la categoría del sistema. Es decir, compara el índice de madurez con el nivel mínimo exigido para dicha categoría en el ENS, que en la presente auditoría es N3 (80%) para todos los casos.

[6] Informe nacional del estado de seguridad de los sistemas de las tecnologías de la información y la comunicación, de 2018, apartado 3.1. En los diferentes perfiles se evalúan los controles mediante un nivel de exigencia, también conocido como nivel de madurez, y se fija el nivel mínimo de exigencia requerido.

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, el borrador previo del Informe de auditoría se discutió con los técnicos responsables del área de sistemas de información del Ayuntamiento de Vila-real para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

Posteriormente, en cumplimiento del artículo 16 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre, y del artículo 55.1.c) del Reglamento de Régimen Interior de la Sindicatura de Comptes, así como del acuerdo del Consell de esta Institución por el que tuvo conocimiento del borrador del Informe de auditoría correspondiente al ejercicio 2020, el mismo se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Transcurrido dicho plazo no se han recibido alegaciones.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre, y del artículo 55.1.h) de su Reglamento de Régimen Interior y del Programa Anual de Actuación de 2020 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 9 de julio de 2020, aprobó este informe de auditoría.