SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SEGUIMIENTO DE LAS RECOMENDACIONES REALIZADAS EN EL INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE VILA-REAL DEL AÑO 2020

Situación a 31 de diciembre de 2021

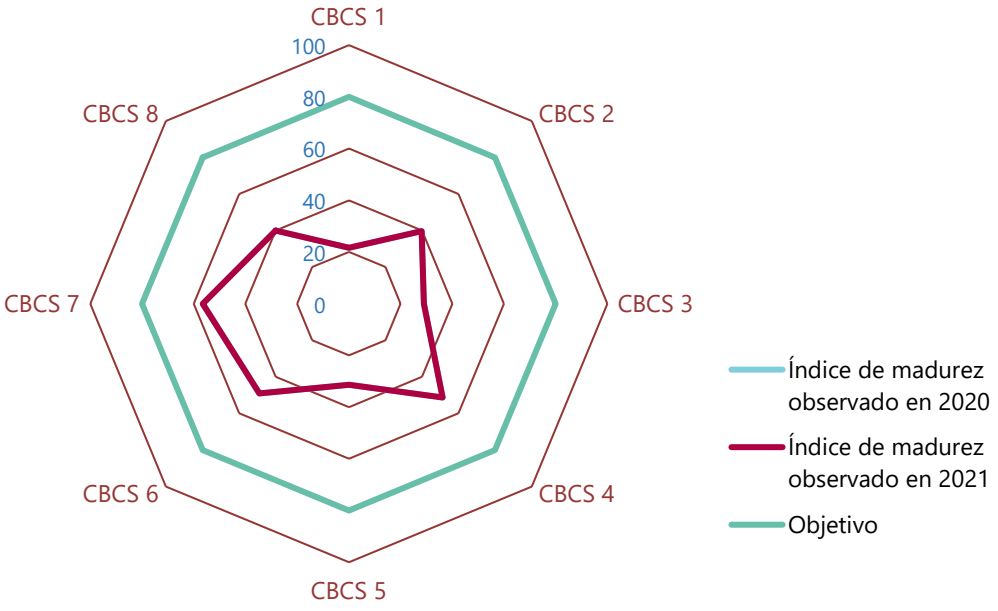
RESUMEN

La transformación digital que están experimentando todas las Administraciones públicas y su interconexión a través de complejas redes informáticas las expone de forma cada vez más intensa a amenazas provenientes del ciberespacio. Esto origina un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y, por tanto, a la información que manejan. De hecho, las entidades locales han sido uno de los objetivos más afectados por las recientes oleadas de ciberataques.

Atendiendo a esta realidad, y en sintonía con su actual plan estratégico, la Sindicatura de Comptes ha realizado un trabajo de seguimiento de los controles básicos de ciberseguridad (CBCS) del Ayuntamiento de Vila-real respecto a la situación mostrada en la auditoría del año 2020.

Conclusiones

No se ha realizado ningún progreso para mejorar la ciberseguridad desde nuestra anterior auditoría y no se ha atendido ninguna de nuestras recomendaciones para ello. Por lo tanto, el índice de madurez general de los controles básicos de ciberseguridad, cuyo objetivo sería alcanzar un 80%, muestra el mismo valor del 39,8% señalado en la auditoría del año 2020, por lo que el nivel de efectividad en los controles analizados continúa siendo muy deficiente y refleja un nivel de riesgo inaceptable para una entidad pública de la importancia del Ayuntamiento de Vila-real. La entidad debe adoptar medidas urgentes para reconducir la situación y deben implantarse mejoras para alcanzar los niveles exigidos por el Esquema Nacional de Seguridad para la protección de los sistemas de información.



El Ayuntamiento de Vila-real no tiene establecida una estructura de gobernanza de la ciberseguridad, tal como exige la normativa, y un adecuado sistema de control interno. Esta situación debe ser prontamente subsanada y los órganos superiores del Ayuntamiento, como responsables del sistema de control, deben reforzar de forma decidida el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

Asimismo, nuestra revisión también ha puesto de manifiesto un grado de cumplimiento insuficiente en cuanto a la adecuación a las normas legales relacionadas con la seguridad de la información. El informe señala diversos aspectos sobre los que se debe actuar para su pronta subsanación. Respecto del Esquema Nacional de Seguridad, el Ayuntamiento debe realizar la designación de las personas para los roles definidos en la política de seguridad y constituir los órganos allí descritos.

También hemos realizado una serie de recomendaciones con el propósito de contribuir a subsanar las deficiencias observadas y mejorar los procedimientos de gestión de la ciberseguridad del Ayuntamiento. Entre ellas aconsejamos implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa, identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte, ubicar las copias de seguridad secundarias en un local correctamente acondicionado y finalizar y formalizar un procedimiento unificado para gestión de usuarios con privilegios de administración.

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.

Informe de seguimiento de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Vila-real del año 2020

Situación a 31 de diciembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

El artículo 6 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, incluye entre sus funciones, además de las referidas al control externo de la gestión económico-financiera del sector público valenciano y de sus cuentas, aquellas que de acuerdo con el ordenamiento jurídico sean convenientes para asegurar adecuadamente el cumplimiento de los principios financieros, de legalidad, de eficacia, de economía y de transparencia, exigibles al sector público, así como la sostenibilidad ambiental y la igualdad de género. Por otra parte, el artículo 11 de la misma ley establece que, en el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para **verificar la seguridad y fiabilidad de los sistemas informáticos** que soportan la información económico-financiera, contable y de gestión.

En la guía de auditoría GPF-OCEX 5311, "Ciberseguridad, seguridad de la información y auditoría externa", del *Manual de fiscalización* de la Sindicatura de Comptes, se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las Administraciones públicas, razón por la que los auditores públicos les deben prestar cada vez más atención. En línea con lo anterior, **en el Plan Estratégico de la Sindicatura de Comptes para el periodo 2019-2022 se señala la ciberseguridad como una de las áreas de alto riesgo y prioritarias para llevar a cabo la tarea fiscalizadora**.

En 2019 y 2020 la Sindicatura de Comptes realizó sendas auditorías sobre la situación de los controles básicos de ciberseguridad (CBCS) de los 15 ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes y el 9 de julio de 2020 el Consell de la Sindicatura de Comptes aprobó el *Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Vila-real, Ejercicio 2020*. Posteriormente, el Consell de la Sindicatura incluyó en los programas anuales de actuación de 2021 y 2022 realizar un trabajo de seguimiento de la situación de los controles básicos de ciberseguridad de ese ayuntamiento y de los otros 14 ayuntamientos analizados.

La necesidad de una adecuada ciberhigiene

Adicionalmente, la crisis provocada por la epidemia de COVID-19 y las medidas tecnológicas adoptadas por las Administraciones públicas han puesto de manifiesto con absoluta claridad la total dependencia de la Administración respecto de los sistemas de información y comunicaciones y el fuerte aumento de la superficie de exposición frente a las ciberamenazas. Para hacer frente a esta realidad, las entidades públicas deben implementar controles sobre la seguridad de la información y las comunicaciones de acuerdo con las directrices establecidas en el Esquema Nacional de Seguridad (ENS), tanto por obligación legal como por razones de autoprotección y supervivencia.

En estos entornos actuales de administración electrónica avanzada adquieren todo su sentido conceptos como la ciberresiliencia y la ciberhigiene. Por ciberresiliencia puede

entenderse la capacidad de una entidad para evitar o resistir y recuperarse de un ciberataque en un tiempo razonable para continuar prestando sus servicios. La ciberhigiene es un principio fundamental[1] relacionado con la seguridad de la información y equivale a establecer medidas rutinarias sencillas para minimizar los riesgos de las ciberamenazas. De manera análoga a lo que ocurre con la higiene personal, las buenas prácticas de ciberhigiene pueden impulsar una mayor inmunidad en las entidades que las aplican, lo que reduce el riesgo frente a un ciberataque.

Por tanto, la existencia de unos controles eficaces de ciberseguridad es un elemento esencial para la prestación de servicios públicos en una Administración tecnológicamente avanzada. En este sentido, consideramos que la implantación de los controles básicos de ciberseguridad (CBCS) –en definitiva, un subconjunto de las medidas de seguridad obligatorias exigidas por el ENS– constituye una medida básica de ciberhigiene para las Administraciones públicas.

2. RESPONSABILIDADES DE LOS ÓRGANOS SUPERIORES DEL AYUNTAMIENTO EN RELACIÓN CON LOS CONTROLES DE CIBERSEGURIDAD

Los órganos superiores del Ayuntamiento (en particular el alcalde y la Junta de Gobierno) son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones. De acuerdo con sus competencias, deben garantizar que el funcionamiento de la entidad resulte conforme con las normas aplicables y que los controles internos proporcionen una garantía razonable de que la información, los servicios y los sistemas de información que les dan soporte cumplan las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el Esquema Nacional de Seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

De acuerdo con lo previsto en los programas anuales de actuación de 2021 y 2022 hemos realizado el seguimiento de la situación de los controles básicos de ciberseguridad y de las recomendaciones efectuadas en el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Vila-real. Ejercicio 2020.

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.

[1] *Review of Cyber Hygiene Practices*, European Union Agency for Cybersecurity (ENISA), 2016.

La presente auditoría se ha centrado en el análisis de la situación actualizada a 31 de diciembre de 2021 de los ocho CBCS revisados en la auditoría del año 2020, relacionados con las aplicaciones y sistemas que soportan el proceso contable-presupuestario, la gestión tributaria y recaudatoria y otros sistemas de interés general.

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 seguridad limitada sobre la situación de los CBCS revisados.

Consideramos que la evidencia de auditoría obtenida proporciona una base suficiente y adecuada para fundamentar nuestras conclusiones sobre el estado de los controles básicos de ciberseguridad, de acuerdo con el alcance limitado que se ha señalado.

Los procedimientos realizados en una auditoría de seguridad limitada son reducidos en comparación con los que se requieren para obtener una seguridad razonable, pero se espera que el nivel de seguridad sea, conforme al juicio profesional del auditor, significativo para los destinatarios del informe. La seguridad limitada no garantiza que una auditoría realizada de conformidad con los *Principios fundamentales de fiscalización de los órganos de control externo* y con las normas técnicas de fiscalización recogidas en el *Manual de fiscalización* de la Sindicatura de Comptes siempre detecte un incumplimiento significativo cuando exista.

En el apéndice 1 se proporciona un mayor detalle de la metodología utilizada. En el apéndice 2 se detallan los hallazgos de la auditoría que sustentan las conclusiones y las recomendaciones de este informe.

4. CONCLUSIONES

No se ha realizado ningún progreso para mejorar la ciberseguridad desde nuestra anterior auditoría y no se ha atendido ninguna de nuestras recomendaciones para ello.

El índice de madurez general de los controles básicos de ciberseguridad continúa siendo muy deficiente y refleja un nivel de riesgo inaceptable para una entidad pública de la importancia del Ayuntamiento de Vila-real.

La entidad debe adoptar medidas urgentes para reconducir la situación

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 controles básicos de ciberseguridad alcanza un **índice de madurez general 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.

Los resultados detallados obtenidos para cada uno de los CBCS y su evolución se muestran en el cuadro 1.

Cuadro 1. Índice de madurez de los controles básicos de ciberseguridad

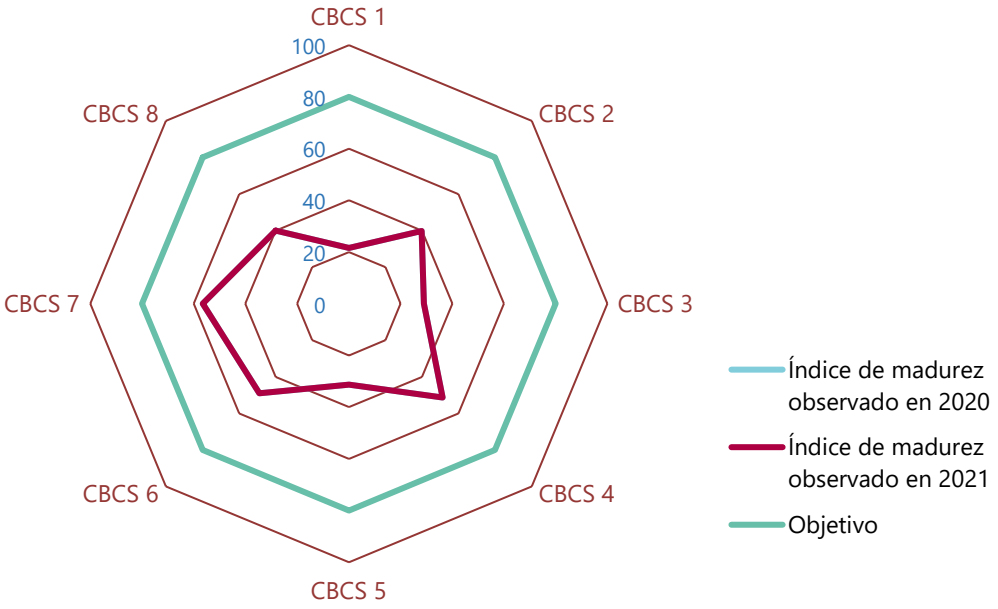
Control	2020			2021		
	Índice de madurez	Nivel de madurez	Índice de cumplimiento	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	*21,6%*	***N1***	*27,0%*	*21,6%*	***N1***	*27,0%*
CBCS 2 Inventario y control de *software* autorizado y no autorizado	*39,8%*	***N1***	*49,7%*	*39,8%*	***N1***	*49,7%*
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	*29,0%*	***N1***	*36,2%*	*29,0%*	***N1***	*36,2%*
CBCS 4 Uso controlado de privilegios administrativos	*51,3%*	***N2***	*64,1%*	*51,3%*	***N2***	*64,1%*
CBCS 5 Configuraciones seguras del *software* y *hardware*	*31,4%*	***N1***	*39,2%*	*31,4%*	***N1***	*39,2%*
CBCS 6 Registro de la actividad de los usuarios	*49,0%*	***N1***	*61,3%*	*49,0%*	***N1***	*61,3%*
CBCS 7 Copias de seguridad de datos y sistemas	*56,5%*	***N2***	*70,6%*	*56,5%*	***N2***	*70,6%*
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	*40,0%*	***N1***	*50,0%*	*40,0%*	***N1***	*50,0%*
General	39,8%	***N1***	49,8%	39,8%	***N1***	49,8%

El índice de cumplimiento de los CBCS es del 49,8% que resulta de comparar el indicador de madurez con el nivel requerido u objetivo que tiene el sistema según el ENS, que es el 80% o *N3 proceso definido*. Este índice no ha mejorado desde nuestro anterior informe y la comparación de los resultados detallados del presente trabajo con los obtenidos en el año 2020 no muestra ninguna mejora en ningún control, dado el nulo grado de atención a nuestras recomendaciones (véase apartado 5 siguiente).

El nivel de efectividad en los controles analizados es muy deficiente y refleja un nivel de riesgo inaceptable; por tanto, deben implantarse mejoras para alcanzar los niveles exigidos por el ENS. En el apartado 5 se realizan las recomendaciones pertinentes con esa finalidad.

De una forma más sintética y gráfica, la situación observada de los controles queda reflejada en el gráfico 1, tanto en la presente auditoría como en la realizada en el año 2020. El gráfico no muestra la línea azul de 2020, ya que como no se ha mejorado nada, dicha línea está bajo la línea roja de 2021.

Gráfico 1. Índice de madurez de los controles básicos de ciberseguridad



Nuestra auditoría y los indicadores reflejan la situación a 31 de diciembre de 2021.

El Ayuntamiento de Vila-real no tiene establecida una estructura de gobernanza de la ciberseguridad, tal como exige la normativa y un adecuado sistema de control interno.

Esta situación debe ser prontamente subsanada y, además, se debe reforzar de forma decidida el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información

Los órganos superiores del Ayuntamiento (en particular el alcalde y la Junta de Gobierno) son los responsables de que existan unos controles de seguridad adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

El compromiso y concienciación con la ciberseguridad también debe extenderse a la dirección[2] (tal como queda definida en el glosario al final de este informe), que son los responsables de articular y facilitar la ejecución de las actividades establecidas por la alta dirección en materia de ciberseguridad.

Hemos podido verificar la existencia de un insuficiente nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del

[2] *Prontuario de ciberseguridad para entidades locales*, Centro Criptológico Nacional y Federación Española de Municipios y Provincias, abril 2021.

Ayuntamiento. No se ha atendido ninguna de nuestras recomendaciones y hemos constatado la falta de iniciativas por parte de la corporación para reconducir la situación.

Este hecho, junto a las relevantes carencias identificadas, nos permite afirmar que la gobernanza de la ciberseguridad del Ayuntamiento de Vila-real es prácticamente inexistente. Dichas carencias son:

- La falta de actividad de la Junta de Administración Electrónica, Seguridad de la Información y Transparencia, órgano imprescindible para coordinar la seguridad de la información en la entidad, que debe incluir representación de las áreas de la organización afectadas.

- La inexistencia de determinados roles clave en la organización, como el responsable de seguridad de la información. Consideramos como factor de riesgo crítico la carencia de un responsable de seguridad del conjunto de los sistemas de información del Ayuntamiento, 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.

- La ausencia de un marco normativo (uso correcto de equipos, servicios, instalaciones, usos indebidos, responsabilidades del personal) y procedimental (documentos que detallan cómo se realizan las tareas habituales, responsables, reporte de comportamientos anómalos) único para los cinco sistemas del Ayuntamiento, con el fin de garantizar una efectiva organización global de la seguridad de la información.

- La inacción de la corporación ante los riesgos identificados, a pesar de que la alta dirección ha sido conocedora de dichos riesgos a través del Pleno, al que se elevó el informe de la Sindicatura de Comptes del ejercicio 2020, y de las recomendaciones efectuadas por empresas especializadas en seguridad de la información contratadas por la corporación, indicando la necesidad de disponer de un plan director de ciberseguridad y del cumplimiento del ENS.

- La falta de personal y de dotación presupuestaria suficiente para atender la problemática de la seguridad de la información.

Es necesario, por tanto, solventar de forma urgente todas las carencias identificadas, que tienen un impacto negativo en el nivel de seguridad de la información del Ayuntamiento, y atender las recomendaciones efectuadas en el presente informe.

El grado de cumplimiento de la normativa relativa a la seguridad de la información es insuficiente

La revisión del cumplimiento de legalidad en materia relacionada con la seguridad de la información ha puesto de manifiesto un insuficiente nivel de cumplimiento de la normativa. Existen incumplimientos, que son señalados en el apartado 5, sobre los que se debe actuar para su pronta subsanación.

5. RECOMENDACIONES Y MEDIDAS NECESARIAS PARA EL CUMPLIMIENTO DE LA LEGALIDAD

Para subsanar las deficiencias de control identificadas por la Sindicatura en la presente auditoría y mejorar los niveles de control señalados en el apartado 4 anterior, reiteramos básicamente las recomendaciones que se efectuaron en la auditoría de 2020, ya que no se ha realizado ninguna mejora desde entonces. El Ayuntamiento deberá dedicar los esfuerzos y recursos necesarios para subsanar las deficiencias pendientes.

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 técnica 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 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

[3] Centro Criptológico Nacional.

[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 corresponden a "guías generales", "guías de entornos Windows" y "guías de otros entornos" respectivamente.

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, las copias de seguridad, la 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 normativo y gobernanza de la ciberseguridad (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.

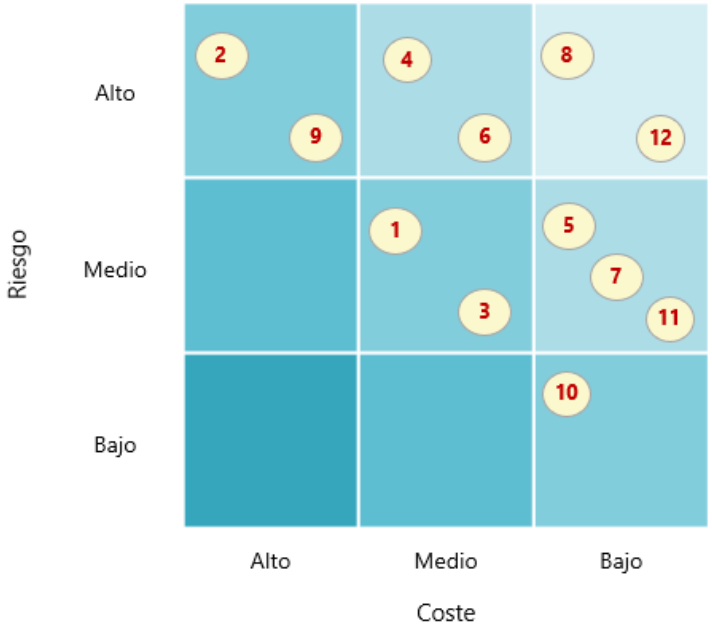
    - Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS del 13 de octubre de 2016.

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 gráfico 2 se muestra la clasificación de las recomendaciones según los criterios combinados de **riesgo potencial a mitigar** y **coste estimado de su implantación**. Este gráfico sigue igual con respecto al informe de 2020, considerando que no se ha realizado ninguna mejora desde entonces. No se incluyen los puntos 13 y 14 anteriores, ya que son medidas de obligado cumplimiento.

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



Actuaciones en curso

Aunque no se han tenido en cuenta en el cálculo de los indicadores mostrados en el apartado 4, hemos verificado que en el momento de finalización del trabajo de campo de la auditoría han sido iniciadas o planificadas algunas actuaciones en materia de ciberseguridad que atenderían parcialmente algunas de las recomendaciones anteriores. La implantación efectiva de estas actuaciones tendrá un impacto positivo, aunque muy limitado, en el nivel de ciberseguridad de la entidad. Dichas actuaciones son:

- Actualización de determinados componentes del sistema de copias. Entre las actuaciones planificadas se encuentra:
  - la sustitución del equipamiento que se encuentra fuera de servicio, cuya licitación ha sido iniciada e incluye los servicios de soporte técnico y mantenimiento del nuevo equipamiento.

  - la actualización de determinados componentes del sistema de copias, en fase de estudio, con objeto de mejorar el tiempo de copia y proporcionar restauraciones más confiables con mayor rapidez.

- Despliegue de servicios y herramientas proporcionados por el CSIRT-CV, como parte del Plan de Choque de Ciberseguridad para las Entidades Locales de la Comunitat Valenciana, y la adquisición y despliegue de soluciones financiadas mediante los fondos europeos Next Generation EU.

Seguimiento de recomendaciones anteriores

Hemos realizado un seguimiento de las recomendaciones efectuadas en el informe de auditoría del año 2020.

Tal como se muestra en el cuadro 2, de las recomendaciones realizadas en ese informe, no se ha atendido ninguna.

Cuadro 2. Seguimiento de recomendaciones

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior.	Estado de la recomendación	Consecuencia en el informe
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.	El inventario de ordenadores portátiles e impresoras, que es gestionado por la empresa que proporciona el mantenimiento se encontraba finalizado y actualizado en el momento de la revisión, pero este hecho no es considerado en el cálculo de los índices de madurez por haberse realizado con posterioridad al 31 de diciembre de 2021	**No aplicada**	Se mantiene la redacción.
2	Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Sin variación.	**No aplicada**	Se mantiene la redacción.
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.	Sin variación.	**No aplicada**	Se mantiene la redacción.
4	Identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte.	Sin variación.	**No aplicada**	Se mantiene la redacción.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior.	Estado de la recomendación	Consecuencia en el informe
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.	Sin variación.	**No aplicada**	Se mantiene la redacción.
6	Implantar herramientas que permitan la gestión unificada y automatizada de parches de seguridad y otras actualizaciones.	Sin variación.	**No aplicada**	Se mantiene la redacción.
7	Optimizar la explotación de la información proporcionada por la sonda del CCN, incluyendo los avisos proporcionados en el proceso de resolución de vulnerabilidades.	Sin variación.	**No aplicada**	Se mantiene la redacción.
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 técnica 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.	Sin variación.	**No aplicada**	Se mantiene la redacción.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior.	Estado de la recomendación	Consecuencia en el informe
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 de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN. 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.	Sin variación.	**No aplicada**	Se mantiene la redacción.
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.	Sin variación.	**No aplicada**	Se mantiene la redacción.
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.	La cabina de discos que realiza las copias de seguridad se encuentra fuera de servicio y sin contrato de mantenimiento, por lo que no se realizan copias de seguridad mediante este sistema No obstante, para compensar la pérdida de servicio producida por la avería, se realizan nuevas copias de seguridad de los sistemas críticos de la entidad. Estas copias son almacenadas en dispositivos tipo NAS (*network attached storage*) y se encuentran desconectadas de la red municipal.	**No aplicada**	Se mantiene la redacción.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior.	Estado de la recomendación	Consecuencia en el informe
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.	Sin variación.	**No aplicada**	Se mantiene la redacción.
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. - 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.	Sin variación.	**No aplicada**	Se mantiene la redacción.
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.	Sin variación.	**No aplicada**	Se mantiene la redacción.

APÉNDICE 1
Metodología aplicada

Introducción

Cada vez un mayor número de aspectos de la gestión pública se realizan con el soporte y apoyo de complejos sistemas informatizados, y la conectividad por internet se ha convertido en una característica fundamental de dichos sistemas de información. Esta circunstancia ha traído aparejado un gran crecimiento de las amenazas de todo tipo provenientes del ciberespacio, mayores riesgos de ciberseguridad y se han multiplicado los incidentes de seguridad de los que son víctimas los sistemas de información y comunicaciones de las entidades públicas, con graves repercusiones potenciales –y en muchos casos, reales– tanto económicas como en la prestación de los servicios públicos.

Las entidades locales, y los ayuntamientos en particular, no son ajenas a esta problemática de la ciberseguridad en su propia operatoria, por lo que deben implementar controles sobre la seguridad de la información y las comunicaciones de acuerdo con las directrices establecidas en el Esquema Nacional de Seguridad, que es **de obligado cumplimiento**.

Por dichas razones, es imperativo que los responsables de los ayuntamientos gestionen los riesgos asociados con el funcionamiento y uso de los sistemas de información que se utilizan para desarrollar y prestar los servicios públicos. Así mismo, deben establecer controles de ciberseguridad adecuados para mantener los sistemas de información protegidos frente a las amenazas de seguridad y evitar la interrupción en los servicios prestados a los ciudadanos y ayuntamientos.

La gestión de los riesgos de ciberseguridad comprende una amplia gama de actividades orientadas a proteger los sistemas de información y los datos frente a accesos no autorizados y otras amenazas cibernéticas, detectar anomalías e incidentes que les afecten negativamente y mitigar su impacto, y también responder y recuperarse de incidentes.

Aun cuando la adopción de medidas de seguridad adecuadas hace más resilientes a las organizaciones frente a los ciberataques, el análisis de los incidentes ocurridos que se realiza en los informes INES[5] del CCN revela que las organizaciones no siempre implementan ni tan siquiera las medidas más básicas que podrían haber evitado o mitigado el daño causado. Por otro lado, el hecho de que los ciberataques permanezcan en muchos casos sin ser detectados durante mucho tiempo puede ser evidencia de que las medidas básicas no están correctamente implementadas.

En definitiva, la existencia de unos controles eficaces de ciberseguridad es un elemento esencial para la prestación de servicios públicos de una Administración tecnológicamente avanzada. En este sentido consideramos que **la implantación de los controles básicos de ciberseguridad (CBCS)** –un subconjunto de las medidas de seguridad obligatorias exigidas por el ENS– **constituye una medida básica de ciberhigiene** para las Administraciones públicas.

[5] Informe Nacional del Estado de Seguridad de los Sistemas de las TIC del CCN.

Objetivo de la auditoría

De acuerdo con lo previsto en los programas anuales de actuación de 2021 y 2022, nuestro objetivo ha sido realizar el seguimiento de la situación de los controles básicos de ciberseguridad y de las recomendaciones efectuadas en el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Vila-real. Ejercicio 2020, y obtener una seguridad limitada y concluir sobre la situación de los controles básicos de ciberseguridad revisados. Para ello hemos evaluado tanto su diseño[6] como su eficacia operativa[7] para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte. También hemos revisado el cumplimiento de la normativa básica relativa a la seguridad de la información.

Asimismo, hemos formulado recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control, teniendo en consideración las mejoras introducidas desde nuestra anterior auditoría.

La presente auditoría se ha centrado en el análisis de la situación actualizada de los ocho CBCS revisados en la auditoría del año 2020, relacionados con las aplicaciones y sistemas que soportan el proceso contable-presupuestario, la gestión tributaria y recaudatoria y otros sistemas de interés general.

Alcance

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*
CBCS 6	Registro de la actividad de los usuarios
CBCS 7	Copias de seguridad de datos y sistemas
CBCS 8	Cumplimiento normativo y gobernanza de ciberseguridad

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

[6] La evaluación del diseño de un control implica la consideración por el auditor de si el control, de manera individual o en combinación con otros controles, es capaz de prevenir de modo eficaz, o de detectar y corregir, la materialización de los riesgos previstos. Es decir, es capaz de cumplir el objetivo de control.

[7] El auditor comprueba que el control existe y que la entidad lo está utilizando.

aplicaciones que soportan los procesos de gestión contable y presupuestaria y la gestión tributaria y recaudatoria, así como los controles que tienen implantados.

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

- controlador de dominio
- software de virtualización
- equipos de usuario (una muestra)
- elementos de la red de comunicaciones (una muestra)
- elementos de seguridad (una muestra)

El alcance específico del presente trabajo de seguimiento de recomendaciones ha estado 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 son:

- El Servicio Municipal de Deportes
- La Policía Local
- El servicio de telecomunicaciones
- Los servicios públicos municipales

Existen, por tanto, determinados procesos de seguridad sobre los sistemas descentralizados cuya responsabilidad no está definida (todos excepto los tres indicados previamente), circunstancia que representa un factor de riesgo adicional.

El presente trabajo únicamente ha comprendido la revisión de recomendaciones sobre los sistemas centralizados. 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.

Ámbito temporal

En cuanto al ámbito temporal del trabajo, las conclusiones se refieren a la situación de los controles a 31 de diciembre de 2021, fecha sobre la que se han calculado los indicadores del Informe, ya que hasta entonces ha sido admitida cualquier evidencia disponible. Por tanto, con carácter general el Informe refleja la situación en ese momento, ya que es frecuente que, desde que se inicia el trabajo de campo, determinadas deficiencias observadas y señaladas a los gestores sean subsanadas y son consideradas de esta forma en las conclusiones y en los indicadores.

Adicionalmente, los hallazgos de la auditoría, las conclusiones y el borrador previo del informe son discutidos con los responsables de la entidad auditada, de acuerdo con lo establecido en nuestro *Manual de fiscalización*.

Metodología

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 y 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 seguridad limitada sobre la situación de los CBCS revisados.

Somos independientes de la entidad auditada, de conformidad con los requerimientos de ética y protección de la independencia exigidos por la normativa reguladora de la actividad de auditoría de los órganos de control externo y por el artículo 8 de la LSC.

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 práctica de fiscalización GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad (CBCS)".

Hemos evaluado la situación de los CBCS utilizando el modelo de nivel de madurez de los procesos, definido en el apéndice 1 de la citada guía, ya que, además de ser un sistema ampliamente aceptado, permite establecer objetivos, realizar comparaciones entre entidades distintas y ver la evolución a lo largo del tiempo.

La guía práctica de fiscalización de los OCEX 5313

La guía práctica de fiscalización de los OCEX GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad", fue aprobada por la Conferencia de Presidentes de los Órganos de Control Externo el 12 de noviembre de 2018, y forma parte del *Manual de fiscalización* de la Sindicatura de Comptes, 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. 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 escoger los más relevantes se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security (CIS)[8], que define, prioriza y clasifica veinte controles de ciberseguridad según su importancia para hacer frente a las ciberamenazas. Su ventaja principal es que están orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. Según el CIS, con carácter general, las organizaciones que apliquen solo los cinco primeros controles pueden reducir su riesgo ante ciberataques alrededor del 85%. Si se implementan los veinte controles el riesgo se puede reducir un 94%.

Se escogieron los siete CBCS más relevantes y se añadió un octavo relacionado con el cumplimiento normativo, por su importancia en una Administración pública. En este informe hemos destacado, además, los aspectos relacionados con la gobernanza de ciberseguridad establecidos en el ENS y en el RGPD.

Alineación de los CBCS con el Esquema Nacional de Seguridad

Dado que el ENS es de obligado cumplimiento para todos los entes públicos, se ha tenido especial cuidado en que la metodología de auditoría de los controles básicos de ciberseguridad estuviera plenamente alineada con el ENS. Esa 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 son requeridos por el ENS. De este modo, los ocho controles básicos de ciberseguridad presentan una correspondencia (no exacta) con las siguientes referencias del ENS:

[8] Center for Internet Security, <www.cisecurity.org>.

Cuadro 3. 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*	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 normativo y gobernanza de la ciberseguridad	

* Estas siglas identifican a cada una de las medidas de seguridad del anexo I del ENS.

Los CBCS como medidas de ciberhigiene

La European Union Agency for Cybersecurity (ENISA) señala[9] que "la ciberhigiene es un principio fundamental relativo a la seguridad de la información y, como analogía con la higiene personal, es el equivalente a establecer simples medidas rutinarias para minimizar los riesgos de las ciberamenazas. La suposición subyacente es que las buenas prácticas de ciberhigiene pueden proporcionar inmunidad en las entidades que las aplican", reduciendo los ciberriesgos[10].

Sintetizando, la ciberhigiene se refiere al conjunto de prácticas y acciones básicas que una organización debe implantar para hacer frente a los riesgos de ciberseguridad más comunes y generalizados a los que se enfrenta hoy en día[11].

En esa dirección, ENISA establece diez puntos de acción para una adecuada ciberhigiene. Como se observa en el cuadro 4, de los siete CBCS, sin contar el de cumplimiento

[9] *Review of Cyber Hygiene Practices*, ENISA, diciembre de 2016. Véase página 14.

[10] Según expertos citados en el informe *DOD Needs to Take Decisive Actions to Improve Cyber Hygiene* de la US Government Accountability Office (2020), hasta el 90% de los ciberataques podrían evitarse implantando adecuadas medidas de ciberhigiene.

[11] Carnegie Mellon University *Software* Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* <https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf>, 2017.

normativo, cinco son coincidentes con los puntos de acción prioritarios recomendados por ENISA como buenas prácticas de ciberhigiene.

Cuadro 4. Puntos de acción de ENISA

ENISA	CBCS
1. Tener un registro de todo el *hardware*	CBCS 1
2. Tener un registro de todo el *software* para asegurarse de que está correctamente parcheado	CBCS 2
3. Utilizar guías de configuración segura y bastionado para todos los dispositivos	CBCS 5
4. Gestionar los datos que entran y salen de la red	–
5. Escanear todos los correos electrónicos entrantes	–
6. Minimizar los usuarios administradores	CBCS 4
7. Realizar copias de seguridad de datos regularmente y hacer pruebas de restauración	CBCS 7

A los efectos de este trabajo, consideramos que los CBCS constituyen un conjunto de prácticas y acciones básicas para mantener una adecuada ciberhigiene.

También puede consultarse nuestro Informe de auditoría de los controles básicos de ciberseguridad de los mayores ayuntamientos de la Comunitat Valenciana. Ejercicios 2019 y 2020, en cuyo apartado 5 explicamos por qué son importantes los CBCS.

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

Utilizamos los controles básicos de ciberseguridad como criterios de auditoría o criterios de evaluación. Los CBCS son controles globales formados por 26 subcontroles detallados, tal como se muestra en el siguiente cuadro. Todas nuestras comprobaciones tienen como objetivo contrastar la situación real de los subcontroles en la entidad frente a las buenas prácticas recogidas en la GPF-OCEX 5313, en las que se especifica con el máximo detalle los aspectos comprobados en cada control.

Cuadro 5. Los CBCS y sus subcontroles

Control	Objetivo del 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 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.
		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 del 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, 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 normativo y gobernanza de ciberseguridad	La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación y tiene establecida una adecuada gobernanza de ciberseguridad.	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.

Evaluación de los resultados del trabajo

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

Subcontroles

Los CBCS son controles globales compuestos por varios controles detallados o subcontroles (tal como puede verse en el cuadro 5 anterior), de los que hemos revisado tanto su diseño como su eficacia operativa.

El trabajo de auditoría consiste básicamente en evaluar cada subcontrol en función de los resultados de las pruebas realizadas y de las evidencias obtenidas. Cada subcontrol se evalúa según la escala mostrada en el siguiente cuadro:

Cuadro 6. Evaluación de los subcontroles

Evaluación	Descripción
Control efectivo	Cubre al 100% 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

Para determinar la situación global de cada control 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 CCN, usando una escala que se resume en el siguiente cuadro.

Cuadro 7. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El control 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 sí 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 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 comprobación de su aplicación práctica.

Para evaluar el nivel de madurez de cada control se han tenido en cuenta los resultados obtenidos en la revisión de los subcontroles que lo forman.

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.

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.

A fin de poder determinar el impacto que tendría sobre la organización un incidente de este tipo, y de poder establecer la categoría del sistema, se deben tener en cuenta las **cinco dimensiones de la seguridad** que los controles de ciberseguridad deben garantizar:

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 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.

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[12]:

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 considerados a los efectos del ENS como de categoría MEDIA y el nivel de madurez requerido u objetivo es *N3, proceso definido,* y un índice de madurez del 80%.

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%.

[12] *Guía de seguridad de las TIC. CCN-STIC 824. Informe Nacional del Estado de Seguridad de los Sistemas TIC.*

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 un resumen del estado de las medidas de seguridad de los entes auditados:

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

- El **índice de cumplimiento** analiza igualmente el nivel de madurez alcanzado, pero en relación con 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.

Gobernanza de ciberseguridad

A los efectos del presente trabajo, se entenderá por gobernanza de la seguridad de la información y las comunicaciones o de ciberseguridad (términos que utilizamos de forma indistinta en este informe) el conjunto de responsabilidades y actividades realizadas por la alta dirección con el objetivo de proporcionar una dirección estratégica en esta materia, garantizar que se logren los objetivos, verificar que el riesgo se gestione adecuadamente y comprobar que se utilicen los recursos de la entidad de una forma responsable.[13]

Los principales elementos de una adecuada gobernanza de ciberseguridad están implícitos en el ENS y la normativa relativa a la protección de datos de carácter personal, normas que revisamos en el CBCS 8. Dada su importancia nuclear para la ciberresiliencia de la entidad destacamos de forma explícita nuestra evaluación de la gobernanza existente.

La gobernanza es el proceso de establecer y mantener un marco de referencia, y apoyar la estructura y los procesos de gestión para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los datos.

Es más que una mera cuestión técnica, por lo que **exige un liderazgo efectivo, procesos sólidos y estrategias en consonancia con los objetivos de la organización**[14].

La responsabilidad sobre dicho proceso es de la alta dirección, que, en el caso de las entidades locales, corresponde a su presidente y a la junta de gobierno. Ellos son los responsables de garantizar que el funcionamiento de la organización resulta conforme con las normas aplicables y de que existan unos adecuados controles sobre los sistemas de

[13] Véase el glosario de la Information Systems Audit and Control Association (ISACA).

[14] Véase el apartado 66 de *Análisis n.º 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE* del Tribunal de Cuentas Europeo.

información y las comunicaciones. La responsabilidad de la ejecución de las actividades establecidas por la alta dirección corresponde a los gestores, a la dirección ejecutiva.

La implicación de los órganos superiores es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información o de ciberseguridad[15]. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información[16] que debe materializarse en aspectos tales como:

- De acuerdo con el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, debe formularse la **política de seguridad de la información (PSI) que debe ser aprobada por el titular del órgano superior** de la entidad. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización, así como, en su caso, a proveedores y terceros.

- Asignar los roles y responsabilidades en materia de seguridad de la información. Los órganos superiores de la entidad deben nombrar al **responsable de la información** (que puede tratarse de una persona o un órgano colegiado), al **responsable del servicio** (que puede ser el mismo que el anterior), al **responsable de la seguridad** y al **responsable del sistema**.

  El procedimiento de nombramiento formal de los responsables mencionados debe constar en la política de seguridad de la información de la entidad.

- Autorizar la implementación y operación de un **comité de seguridad TIC**.

  La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[17], que se constituye como un órgano colegiado, algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad, y es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio. Su composición debe constar en la PSI.

- **Proporcionar los recursos materiales y humanos** necesarios y asegurar que se implantan programas de concienciación, formación y capacitación.

  El mantenimiento actualizado y la mejora de los controles de ciberseguridad requerirá de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas.

[15] *Guía de iniciación a actividad profesional implantación de sistemas de gestión de la seguridad de la información (SGSI) según la norma ISO 27001*, Colegio Oficial de Ingenieros de Telecomunicación.

[16] *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información*, apartado 3.4.

[17] *Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC*, CCN, enero de 2021.

- Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.
- Dirigir las revisiones periódicas de la PSI y velar por la realización de las auditorías internas de seguridad.

Seguimiento de las recomendaciones

En el presente trabajo se ha realizado el seguimiento de las recomendaciones recogidas en el apartado 6 del Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Vila-real. Ejercicio 2020.

En la valoración de la situación actual, se ha seguido la GPF-OCEX 1735, "Las recomendaciones y su seguimiento", que propone la siguiente categorización:

Cuadro 8. Situación de las recomendaciones

Total o sustancialmente aplicada	Si el ente fiscalizado ha adoptado las medidas correctoras, razonables y proporcionadas en la esfera de sus competencias, que permiten considerar que la recomendación ha surtido sus efectos y no ha quedado pendiente de resolución ninguna cuestión de importancia significativa. En estos casos se entenderá que la recomendación se ha cumplido razonablemente. Además, se ha obtenido evidencia suficiente que acredita las medidas adoptadas.
Aplicada parcialmente	Si el ente fiscalizado ha tomado en consideración las recomendaciones y ha realizado actuaciones encaminadas a corregir las deficiencias, debilidades o insuficiencias que se han puesto de manifiesto, pero solamente en un estado incipiente, en una parte de ellas o en algunos aspectos, lo que no permite considerar que la recomendación se ha cumplido razonablemente.
No aplicada	Si el ente fiscalizado no ha realizado las actuaciones encaminadas a corregir las deficiencias, debilidades o insuficiencias que se han puesto de manifiesto o bien lo ha hecho insuficiente o inadecuadamente de forma que la recomendación sigue sin aplicarse.
Sin validez en el marco actual	Se incluyen aquellas recomendaciones que, aunque válidas y pertinentes cuando se emitió el informe y para el ejercicio fiscalizado, y aun siendo aceptadas y reconocidas por el ente fiscalizado, no pueden aplicarse en el contexto actual, al no darse las circunstancias que lo permitan o la misma casuística que entonces, es decir, no se dan en el momento actual los supuestos de los hechos en función de los cuales se efectuó la recomendación en el pasado. La recomendación ha devenido inaplicable.
No verificada	Se incluyen en esta categoría las recomendaciones que, aunque aceptadas o incluso aplicadas y corregidas por el ente fiscalizado, necesitarían obligatoriamente de alguna prueba adicional para contrastar lo manifestado por el ente fiscalizado que exceden el alcance previsto en el trabajo.

En el cuadro 2 se muestran las recomendaciones contenidas en el citado informe con los comentarios relativos al seguimiento realizado y la situación a 31 de diciembre de 2021.

Comunicación y confidencialidad

Nos comunicamos con los responsables de la entidad en relación, entre otras cuestiones, con el alcance y el momento de realización de la auditoría planificados y los hallazgos significativos de la auditoría, así como con cualquier deficiencia significativa de los controles internos que identificamos en el transcurso de esta

Dado que la información utilizada en la auditoría tiene un carácter sensible y puede afectar a la seguridad de los sistemas de información, los resultados con el máximo detalle de cada uno de los controles revisados 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.

APÉNDICE 2
Situación de los controles básicos de ciberseguridad

CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) los dispositivos físicos conectados en la red, de forma que solo los dispositivos autorizados tengan acceso a la red.

Situación del control

El Ayuntamiento no ha realizado cambios significativos respecto del inventario y control de dispositivos físicos que observamos en la revisión anterior.

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 en este periodo.

El Servicio de Nuevas Tecnologías (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 es gestionado por la empresa externa que proporciona el mantenimiento, inventario que se encontraba en fase final de implantación a 31 de diciembre de 2021 y ha sido completado en el momento de la revisión.

Por otra parte, no ha sido implantado un control robusto que impida la conexión de dispositivos físicos no autorizados a los sistemas de información desde la anterior revisión.

El nivel de control sobre el inventario y el control de activos físicos es insuficiente, y su valoración global alcanza un **índice de madurez del 21,6%,** que se corresponde con un **nivel N1 de madurez *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%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 2. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) todo el *software* en la red, 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.

Situación del control

El Ayuntamiento no ha realizado cambios significativos respecto al inventario y control de *software* autorizado que observamos en la revisión anterior.

Si bien la responsabilidad del inventariado de *software* se encuentra establecida en la normativa de seguridad vigente, el Ayuntamiento no ha aprobado un procedimiento que recoja las medidas de seguridad sobre el inventario y control de *software* que se deben aplicar.

El Ayuntamiento virtualiza 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.

Por otra parte, se evidenció la existencia de un elevado número de equipos con sistemas operativos fuera del periodo de soporte del fabricante, particularmente servidores, que no han sido actualizados a versiones adecuadas en este periodo, hecho que supone un grave riesgo para el sistema de información.

La gestión del licenciamiento y el mantenimiento de aplicaciones comerciales la realiza el SNT mediante un proceso adecuado y gestionable, pero no está formalizado en procedimiento aprobado.

El trabajo anterior no incluyó en su alcance el análisis del inventario de *software* de los sistemas descentralizados, por lo que no hemos realizado ninguna revisión sobre estos sistemas en el presente trabajo.

Existe un insuficiente nivel de control sobre el inventario y control de *software* autorizado, siendo el **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%**.

No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

Objetivo del control

Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.

Situación del control

El Ayuntamiento no ha realizado cambios significativos respecto al proceso de identificación y remediación de vulnerabilidades que observamos en la revisión anterior.

Sobre la gestión de vulnerabilidades realizada por el Ayuntamiento en el anterior trabajo se observó que se efectuaban 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 establecidas en un procedimiento aprobado.

La identificación y remediación de vulnerabilidades únicamente se realizaba 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. Dicha gestión no ha sido extendida al resto de sistemas del Ayuntamiento. El proceso de priorización y resolución de estas vulnerabilidades es gestionado de manera informal y no ha sido incluido en un procedimiento aprobado.

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.

Para aquellos sistemas descentralizados que no son gestionados por el SNT, no se verificaron las medidas implantadas en el trabajo anterior. Por tanto, no se ha realizado ninguna revisión dado que se encuentra fuera del alcance del trabajo.

El nivel de control es insuficiente y la valoración global sobre este 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%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 4. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

Objetivo del control

Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir la asignación y uso de privilegios administrativos en los sistemas de información.

Situación del control

El Ayuntamiento no ha realizado cambios significativos respecto al uso controlado de privilegios administrativos que observamos en la revisión anterior.

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 identificaron en la anterior revisión 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. Además, no se aplica una política de autenticación homogénea en todos los sistemas o la política aplicada no es robusta en todos los casos.

No ha sido corregido el uso de cuentas de administración no nominativas en determinados sistemas, lo que impide la trazabilidad de las acciones en caso de incidentes y constituye la deficiencia más significativa detectada en este control.

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, no hemos realizado ninguna revisión adicional sobre los sistemas descentralizados que se analizaron en el anterior trabajo.

Existe un cierto nivel de control sobre las cuentas con privilegios administrativos, pero hay posibilidades de mejora. La valoración global del control muestra 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 documentalmente. Esto representa un **índice de cumplimiento de este CBCS 4 del 64,1%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 5. CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE

Objetivo del control

Establecer una configuración base segura del *software* y *hardware* 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.

Situación del control

El Ayuntamiento no ha realizado cambios significativos respecto a las configuraciones seguras de *software* y *hardware* que observamos en la revisión anterior. Hemos verificado que no ha sido formalmente aprobado un procedimiento desde nuestra anterior auditoría. Aunque la entidad aplica configuraciones de seguridad en determinados sistemas, dichas acciones no son suficientes para asegurar la efectividad del control.

Si bien 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%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 6. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

Objetivo del control

Recoger, gestionar y analizar los registros de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.

Situación del control

El Ayuntamiento no ha realizado cambios significativos respecto al registro de la actividad de los usuarios que observamos en la revisión anterior.

En la anterior auditoría se analizaron las acciones del Ayuntamiento para el control de la actividad de los usuarios en los sistemas y, aunque se dispone de ciertas medidas relacionadas, hemos constatado que en este periodo no han sido formalmente establecidas en un procedimiento escrito y aprobado.

Hemos verificado que el registro de actividad se encuentra activado en los sistemas incluidos en el alcance de la revisión, si bien se sigue manteniendo 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.

La valoración global del control existente sobre el registro de la actividad de los usuarios es que la organización alcanza un **índice de madurez del 49,0%,** 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 6 del 61,3%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 7. COPIA DE SEGURIDAD DE DATOS Y SISTEMAS

Objetivo del control

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.

Situación del control

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. Estas pruebas de preproducción permiten la comprobación de copias de seguridad de sistema críticas, y son adecuadamente documentadas.

Asimismo, las medidas implantadas para la protección de las copias del SNT pueden considerarse eficaces. No obstante, tal y como se identificó en la anterior revisión, las copias de seguridad, ubicadas en un edificio que actúa como nodo secundario de la red municipal, están emplazadas en un local que no dispone de todas las condiciones de adecuación física requeridas.

Durante la realización del trabajo de revisión nos han indicado que la cabina de discos que realiza las copias de seguridad está fuera de servicio y sin contrato de mantenimiento, por lo que no se realizan copias de seguridad adicional mediante este sistema.

Como medida compensatoria, se realizan semanalmente copias de seguridad desconectadas de la red en dispositivos tipo NAS (*network attached storage*) de los sistemas

críticos dependientes del SNT que es responsabilidad del Departamento de informática, con el objeto de disponer de una copia de seguridad adicional. Una vez realizada la copia en el dispositivo NAS, se desconecta de la red y, verificada su integridad, se guarda en un lugar seguro.

En el caso de ser infectado el sistema por un virus de tipo *ransomware*, el sistema de copias semanal desconectado permite la restauración del sistema afectado con una pérdida máxima de datos de una semana.

La valoración global del control existente sobre las copias de seguridad es que el Ayuntamiento 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 documentalmente. Esto representa un **índice de cumplimiento del CBCS 7 del 70,6%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 8. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD

Objetivo del control

Asegurar el cumplimiento de la normativa básica en materia de seguridad de la información, lo que incluye el establecimiento de una adecuada gobernanza de ciberseguridad.

Situación del control

Cumplimiento del ENS

Desde la revisión realizada en el año 2020, el Ayuntamiento no ha realizado acciones que hayan mejorado el nivel de cumplimiento exigido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

Además, no han sido designados determinados roles y responsabilidades en seguridad de la información, particularmente el responsable de seguridad de la información, deficiencia crítica en un entorno de sistemas descentralizados.

En consecuencia, siguen vigentes las carencias identificadas y las recomendaciones realizadas en el informe precedente.

Cumplimiento del RGPD

En cuanto al cumplimiento en materia de protección de datos personales, sigue vigente el nombramiento del DPD y su notificación a la Agencia Española de Protección de Datos.

No se ha realizado ninguna auditoría en materia de protección de datos en la que se especifiquen las medidas técnicas y organizativas que se han adoptado para dar cumplimiento a las obligaciones de la legislación vigente

Cumplimiento de la legalidad del registro de facturas

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

Indicadores

En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad incluidos en la revisión no se modifica con respecto al informe emitido en el año 2020, alcanzando el Ayuntamiento un **índice de madurez del 40,0%**, 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 8 del 50,0%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

Gobernanza de ciberseguridad

El Ayuntamiento de Vila-real no tiene establecida una estructura de gobernanza de la ciberseguridad, tal como exige la normativa y un adecuado sistema de control interno.

Los órganos superiores del Ayuntamiento son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

Si bien en la auditoría hemos observado la existencia de un cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los gestores y responsables de las áreas implicadas, **existen carencias relevantes que permiten afirmar que la gobernanza de la ciberseguridad del Ayuntamiento de Vila-real es prácticamente inexistente** y que existe un **insuficiente nivel de compromiso** y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento. Las carencias más relevantes identificadas son las siguientes:

- La falta de actividad de la Junta de Administración Electrónica, Seguridad de la Información y Transparencia, órgano imprescindible para coordinar la seguridad de la información en la entidad, que debe incluir representación de las áreas de la organización afectadas.

  Esta circunstancia ocasiona la falta de coordinación y comunicación entre los diferentes responsables de los sistemas de información que existen en el Ayuntamiento.

- La inexistencia de determinados roles clave en la organización, como el responsable de seguridad de la información. Debido a la organización funcional de los sistemas de

información en el Ayuntamiento, diferenciados en sistemas centralizados y descentralizados, consideramos como factor de riesgo crítico la carencia de un responsable de seguridad del conjunto de los sistemas de información del Ayuntamiento, 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.

- Ausencia de un marco normativo y procedimental único para los cinco sistemas del Ayuntamiento. No se ha desarrollado el marco normativo (uso correcto de equipos, servicios, instalaciones, usos indebidos, responsabilidades del personal) y procedimental (documentos que detallan cómo se realizan las tareas habituales, responsables, reporte de comportamientos anómalos) requerido en el ENS para garantizar una efectiva organización global de la seguridad de la información.

  Esta situación repercute negativamente en la valoración de los controles, dado que la ineficiencia de controles en cualquiera de las áreas repercute en el riesgo y la valoración global del control.

- La inacción de la corporación ante los riesgos identificados, siendo la alta dirección conocedora de dichos riesgos a través del Pleno en el que se elevó el informe publicado por la Sindicatura de Comptes sobre los controles básicos de ciberseguridad del Ayuntamiento de Vila-real del ejercicio 2020, y de las recomendaciones efectuadas por empresas especializadas en seguridad de la información contratadas por la corporación, indicando la necesidad de disponer de un plan director de ciberseguridad y del cumplimiento del Esquema Nacional de Seguridad.

- La falta de atención a relevantes carencias o situaciones de riesgo sobrevenidas, debido a la falta de personal y de dotación presupuestaria para su tratamiento.

Resulta, por tanto, necesaria la solución urgente de las carencias identificadas, que tienen un impacto negativo en el nivel de seguridad de la corporación. En ese sentido, los órganos de gobierno ostentan la responsabilidad de liderar y ser ejemplarizantes en sus acciones y decisiones, como parte de un proceso de concienciación de la entidad.

Alguna medida parcial e insuficiente se ha adoptado recientemente, tal como se ha señalado anteriormente.

APÉNDICE 3
Buenas prácticas destacables

Introducción

Con carácter general, si una entidad alcanza una valoración del 80% en el índice de madurez de un control significa que está aplicando de forma razonable las buenas prácticas en materia de seguridad de la información establecidas en el ENS o en las guías profesionales correspondientes, que se sintetizan en el cuadro 5 de este informe. En otro caso, la entidad debe adoptar medidas para mejorar su ciberseguridad y alcanzar dicha meta.

Adicionalmente a la valoración de los controles básicos de ciberseguridad, es conveniente destacar determinados aspectos, prácticas, soluciones técnicas o sistemas que han sido identificados o revisados durante la realización de la auditoría y que destacan en relación con el estado del arte sobre una determinada materia. Estos aspectos proporcionan, por su singularidad, un conocimiento adicional que facilita la interpretación, contextualización y evaluación de los resultados obtenidos en los procedimientos de auditoría para la valoración de los controles.

Además, dado el carácter positivo de los aspectos considerados en este apartado, su identificación puede, en determinados casos, constituir la base de sinergias entre Administraciones públicas de la misma naturaleza y con características similares, ya que pueden ser replicadas si se dan necesidades y problemáticas comunes.

El criterio para determinar si un aspecto es considerado buena práctica destacable es la existencia de una o varias de las siguientes circunstancias:

- soluciones o sistemas especialmente avanzados o efectivos desde el punto de vista tecnológico,
- procesos de gestión particularmente maduros, y
- soluciones o procesos poco frecuentes entre las entidades auditadas, pero de demostrada eficacia frente a las necesidades de la entidad, independientemente de su complejidad o innovación.

Los aspectos destacados a continuación, en general, han sido considerados en la evaluación de los CBCS. No obstante, algunos no forman parte de los CBCS tal como están definidos en la GPF-OCEX 5313, pero los comentamos por las razones antes indicadas. Cabe aclarar que la existencia de aspectos concretos particularmente relevantes no implica necesariamente que el control global disponga de la madurez requerida, ya que su valoración incluye la consideración de un conjunto de aspectos técnicos, organizativos y formales que se deben alcanzar individualmente y en conjunto, con un determinado nivel de efectividad y madurez.

Entorno de preproducción

El Ayuntamiento dispone de un entorno de preproducción que se encuentra explotado de manera particularmente efectiva. Este entorno es utilizado en diversos controles y subcontroles de seguridad, especialmente los siguientes:

- Gestión de cambios. El Ayuntamiento utiliza el entorno de preproducción para la ejecución de diversos procesos relacionados con la gestión de cambios en sistemas existentes, incluyendo actualizaciones críticas, y la puesta en operación de nuevos sistemas. La gestión realizada incluye tareas relativas a diversos subcontroles, entre los que se encuentran:

  - La realización de pruebas de testeo de los cambios en aplicaciones y sistemas. Incluyendo la realización de pruebas unitarias y pruebas de integración.

  - El uso de entornos para pruebas separados de producción, limitando o eliminando la afección al entorno de producción de posibles problemas en la fase de pruebas.

  - La aprobación del usuario en las pruebas de testeo, validando los cambios realizados.

  - El registro exhaustivo de cambios y solicitudes, facilitando la trazabilidad y seguimiento del proceso de cambio.

- Pruebas de recuperación de copias de seguridad. Como parte del proceso de realización de pruebas de testeo de los cambios en aplicaciones y sistemas, se realiza de manera frecuente la recuperación completa y puesta en operación de sistemas y componentes críticos, lo que permite:

  - Verificar la viabilidad de las copias existentes.

  - La preparación y entrenamiento del personal relacionado con la recuperación de datos y sistemas en caso de incidente de seguridad.

  - La ejecución, de manera informal, de procedimientos para la recuperación ante desastres.

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

ENS: Esquema Nacional de Seguridad

INES: Informe Nacional del Estado de la Seguridad

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

PSI: Política de seguridad de la información

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de gestión de seguridad de la información

SIC: Sistemas de información y comunicaciones

Alta dirección: A los efectos de este trabajo, nos referimos a los órganos superiores del Ayuntamiento (en particular, el alcalde o la alcaldesa y la Junta de Gobierno). Son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones y una adecuada gobernanza de ciberseguridad.

Ciberamenazas: Eventos con origen en internet que pueden desencadenar un incidente en la organización y producir daños materiales, pérdidas inmateriales en sus activos o la interrupción de un servicio.

Ciberhigiene: Conjunto de prácticas y acciones básicas que una organización debe implantar para hacer frente a los riesgos de ciberseguridad más comunes y generalizados a los que se enfrenta hoy en día. A los efectos de este trabajo, dicho conjunto de prácticas y acciones básicas son los CBCS.

Ciberresiliencia: Es la capacidad de un proceso, negocio, organización o nación para anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos cibernéticos que necesitan para funcionar. En el ámbito concreto del sector público, es la capacidad de un ente público para evitar o resistir y recuperarse de un ataque y continuar prestando sus servicios en un tiempo razonable.

Ciberseguridad: Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, así como de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Correlador de eventos: Correlar es el proceso de comparar diferentes fuentes de información de eventos, dando de esta manera sentido a eventos que, analizados por separado, no lo tendrían o pasarían desapercibidos. Un SIEM *(security information and event management)* o sistema de gestión de información y eventos de seguridad, va un paso más

allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes mediante técnicas de correlación compleja de eventos.

Dirección: Son los responsables de la ejecución de las actividades establecidas por la alta dirección en materia de ciberseguridad, es la dirección ejecutiva. En este grupo, a los efectos de este informe, se incluye al concejal responsable de los sistemas de información y las comunicaciones, al secretario general, al interventor general, a los funcionarios directores del departamento TIC y los jefes de área o servicio

Gobernanza de ciberseguridad: Según el Tribunal de Cuentas Europeo, la gobernanza de la seguridad de la información consiste en la creación de estructuras y políticas para garantizar la confidencialidad, integridad y disponibilidad de los datos. Es más que una mera cuestión técnica, por lo que exige un liderazgo efectivo, procesos sólidos y estrategias en consonancia con los objetivos de la organización. A los efectos de este informe le damos el mismo significado que a *gobernanza de la seguridad de la información*.

Normas de seguridad: Uniforman el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio y describirán: a) el uso correcto de equipos, servicios e instalaciones; b) lo que se considerará uso indebido, y c) la responsabilidad del personal con respecto al cumplimiento o violación de estas normas. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones; como regla general, estará disponible en la intranet corporativa de la entidad a través de una dirección URL. La normativa de seguridad de cada entidad trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y del desarrollo normativo de la política de seguridad de la entidad en cuestión, en segunda instancia.

Política de seguridad de la información: Es un documento de alto nivel que define lo que significa *seguridad de la información* en una organización de acuerdo con el artículo 11 del Real Decreto 3/2010 y articula la gestión continuada de la seguridad. Debe ser aprobada por el presidente o presidenta o la junta de gobierno de una entidad local o el consejo de administración de una sociedad. Debe estar accesible para todos los miembros de la organización y redactada de forma sencilla, precisa y comprensible. Conviene que sea breve, y que deje los detalles técnicos para otros documentos más precisos que ayuden a llevar a cabo lo propuesto: normas de seguridad y procedimientos de seguridad.

Procedimientos de seguridad: Abordan tareas concretas, indicando lo que hay que hacer, paso a paso. Detallan de forma clara y precisa: a) cómo llevar a cabo las tareas habituales, b) quién debe hacer cada tarea y c) cómo identificar y reportar comportamientos anómalos.

Sistema de gestión de seguridad de la información: Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos.

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, un borrador previo del Informe de auditoría se discutió con el concejal responsable de Innovación y nuevas tecnologías, con el secretario y vicesecretario del Ayuntamiento y con los responsables correspondientes del Departamento de Innovación e Informática, 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 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 a 2021, 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, y del artículo 55.1.h) de su Reglamento de Régimen Interior y de los programas anuales de actuación de 2021 y 2022 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 7 de septiembre de 2022, aprobó este informe de auditoría.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe seguimiento recomendaciones CBCS Vila-real del año 2020 - SEFYCU 3480618

Puede acceder a este documento en formato PDF - PAdES y comprobar su autenticidad en la Sede Electrónica usando el código CSV siguiente:

URL (dirección en Internet) de la Sede Electrónica: https://sindicom.sedipualba.es/

Código Seguro de Verificación (CSV): KUAA X9V2 LQCM LFZM QX2L

En dicha dirección puede obtener más información técnica sobre el proceso de firma, así como descargar las firmas y sellos en formato XAdES correspondientes.

Resumen de firmas y/o sellos electrónicos de este documento

Huella del documento para el firmante	Texto de la firma	Datos adicionales de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrónica - ACCV - 13/09/2022 7:34 VICENT CUCARELLA TORMO