

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 PATERNA DEL AÑO 2019**

Situación a 31 de diciembre de 2021



RESUMEN

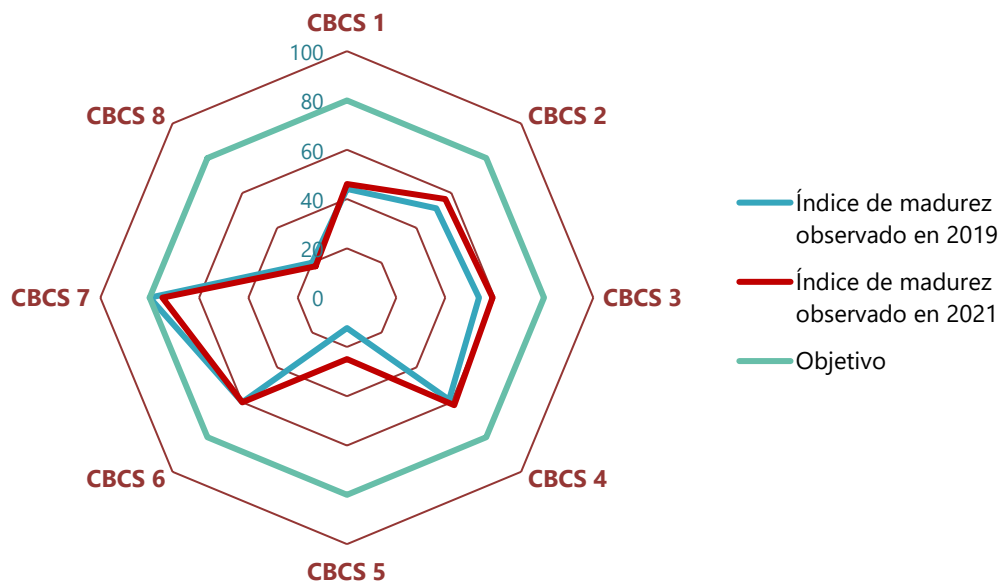
La transformación digital que están experimentando todas las Administraciones públicas y su interconexión a través de complejas redes informáticas las expone de forma cada vez más intensa a amenazas provenientes del ciberespacio. Esto origina un incremento de los riesgos asociados a los sistemas de información 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 Paterna respecto a la situación mostrada en la auditoría del año 2019.

Conclusiones

El Ayuntamiento ha realizado determinadas acciones desde nuestra anterior auditoría y se han atendido, aunque parcialmente, algunas de nuestras recomendaciones.

El índice de madurez general de los controles básicos de ciberseguridad, cuyo objetivo sería alcanzar un 80%, muestra un valor del 50,2%, que supone una escasa mejora respecto del 47,5% recogido en nuestra auditoría de 2019, por lo que el nivel de efectividad en los controles analizados sigue siendo insuficiente. El Ayuntamiento debe adoptar las medidas necesarias para alcanzar los niveles exigidos por el Esquema Nacional de Seguridad para la protección de los sistemas de información, especialmente en aquellos controles que presentan deficiencias significativas.





Existe cierto nivel de compromiso y concienciación con la seguridad por parte de los miembros del departamento TIC y de los órganos superiores; no obstante, diversas circunstancias indican que la gobernanza de la ciberseguridad no puede considerarse efectiva, situación que debe ser subsanada.

Es preciso que el comité de seguridad de la información, órgano imprescindible para su coordinación, se reúna regularmente con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna. Además, los roles establecidos en la política de seguridad del Ayuntamiento deben definirse correctamente y ejercer sus funciones de manera efectiva.

Es necesaria la implantación de una cultura en materia de ciberseguridad que afecte a todos los niveles de la organización y que debe ser impulsada por la dirección en forma de planes estratégicos que definan objetivos y medidas concretas, incluyendo planes periódicos de formación y concienciación para los trabajadores.

Asimismo, nuestra revisión también ha puesto de manifiesto un grado muy deficiente de cumplimiento en cuanto a la adecuación a las normas legales relacionadas con la seguridad de la información, que ya fueron identificadas en nuestro trabajo de 2019 y no han sido corregidas. El informe señala los incumplimientos normativos sobre los que se debe actuar. A este respecto, el Ayuntamiento ha adjudicado en 2022 un contrato para subsanar dichos incumplimientos.

También hemos realizado una serie de recomendaciones con el propósito de contribuir a corregir las deficiencias observadas y mejorar los procedimientos de gestión de la ciberseguridad del Ayuntamiento. Entre ellas, además de actualizar los procedimientos de manera que describan las acciones y controles implantados, recomendamos la implantación de soluciones para restringir el acceso de dispositivos físicos no autorizados a la red corporativa, actualizar los sistemas obsoletos, el uso de una herramienta de gestión centralizada de vulnerabilidades, parches y actualizaciones y la aplicación de seguridad por defecto a todos los sistemas y aplicaciones críticas de la entidad.

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 la lectura del informe completo 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 Paterna del año 2019**

Situación a 31 de diciembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana



ÍNDICE (con hipervínculos)

1. Introducción	3
2. Responsabilidades de los órganos superiores del Ayuntamiento en relación con los controles de ciberseguridad	4
3. Responsabilidad de la Sindicatura de Comptes	4
4. Conclusiones	5
5. Recomendaciones y medidas para el cumplimiento de la legalidad	8
Apéndice 1. Metodología aplicada	19
Apéndice 2. Situación de los controles básicos de ciberseguridad	36
Apéndice 3. Buenas prácticas destacables	48
Acrónimos y glosario de términos	51
Trámites de alegaciones	54
Aprobación del Informe	55



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 a 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 20 de febrero de 2020 el Consell de la Sindicatura de Comptes aprobó el [Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Paterna, Ejercicio 2019](#). 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 fundamental¹ 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 Paterna. Ejercicio 2019.

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 2019, 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

Aunque se han atendido parcialmente algunas recomendaciones de nuestra anterior auditoría, el índice de madurez general de los controles básicos de ciberseguridad continúa siendo insuficiente y debe mejorar para alcanzar los niveles establecidos por el ENS.

El Ayuntamiento tiene en marcha un conjunto de proyectos que, si se ejecutan y gestionan adecuadamente, contribuirán a mejorar los niveles de ciberseguridad de sus sistemas de información.

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 50,2%**, 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.

Aunque el Ayuntamiento ha atendido de forma parcial nuestras recomendaciones y el índice de madurez general ha mejorado levemente desde el 47,5% identificado en nuestra auditoría de 2019, el índice de madurez actual sigue siendo insuficiente para garantizar un adecuado grado de seguridad y alcanzar el 80% requerido por el ENS.

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	2019			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	44,1%	N1	55,1%	46,1%	N1	57,6%
CBCS 2 Inventario y control de <i>software</i> autorizado y no autorizado	51,3%	N2	64,1%	56,5%	N2	70,6%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	53,6%	N2	67,0%	59,1%	N2	73,9%
CBCS 4 Uso controlado de privilegios administrativos	58,6%	N2	73,3%	61,7%	N2	77,1%
CBCS 5 Configuraciones seguras del <i>software</i> y <i>hardware</i>	12,4%	N1	15,5%	25,0%	N1	31,3%
CBCS 6 Registro de la actividad de los usuarios	60,0%	N2	75,0%	60,0%	N2	75,0%
CBCS 7 Copias de seguridad de datos y sistemas	80,0%	N3	100,0%	74,8%	N2	93,5%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	20,0%	N1	25,0%	18,0%	N1	22,5%
General	47,5%	N1	59,4%	50,2%	N2	62,7%

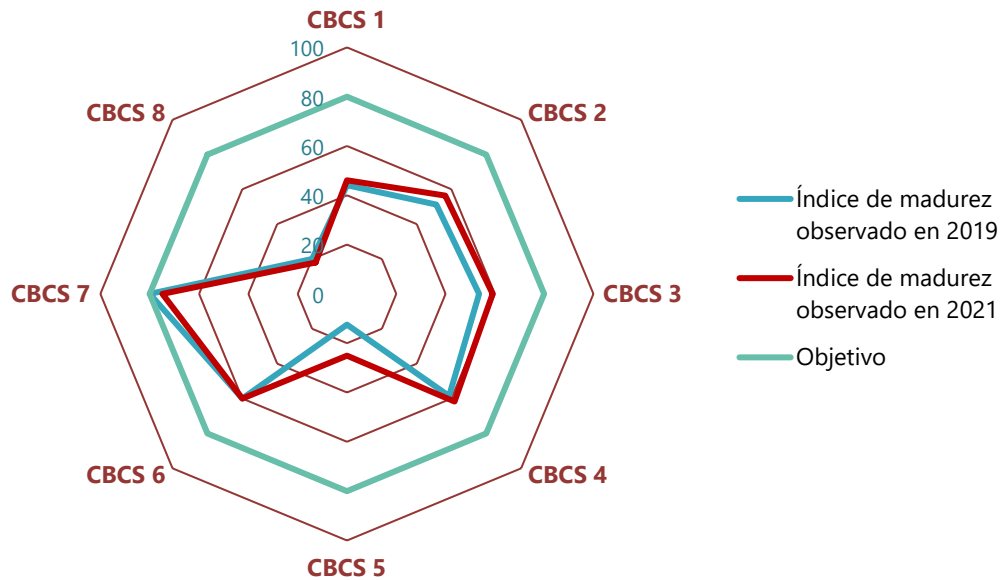
El índice de cumplimiento de los CBCS es del 62,7%, que resulta de comparar el indicador de madurez con el nivel requerido u objetivo que tiene el sistema según el ENS, que es el 80%.

La comparación de los resultados detallados del presente trabajo con los obtenidos en el año 2019 muestra una evolución dispar en los distintos controles, pero, en conjunto, la mejora es claramente insuficiente. La entidad debe aplicar medidas para reconducir la situación y alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información, particularmente sobre los controles que presentan deficiencias significativas y no alcanzan el nivel de madurez N2 (CBCS 1, CBCS 5 y CBCS 8). 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 de la presente auditoría como de la realizada en el año 2019.

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 Paterna no tiene establecida una adecuada gobernanza de la ciberseguridad, tal como exige la normativa y un adecuado sistema de control interno.

Esta situación debe ser prontamente subsanada, siendo los órganos superiores quienes deben impulsar el establecimiento de un adecuado sistema de gestión de 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 dirección² (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.

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



Consideramos que existen carencias que impiden que la gobernanza pueda considerarse efectiva, las más relevantes son:

- El Ayuntamiento dispone de una política de seguridad de la información y además tiene normativa y procedimientos al respecto. Sin embargo, esta normativa es de 2013 y está desactualizada.
- La falta de liderazgo e implicación en materia de ciberseguridad de los órganos superiores del Ayuntamiento, identificada en aspectos como la inexistencia de estrategias relacionadas con la seguridad de la información o los incumplimientos legales identificados en nuestro anterior trabajo de auditoría y que todavía no han sido subsanados.
- El comité de seguridad, órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas del Ayuntamiento, no se reúne y por tanto no ejerce sus funciones de manera efectiva.

Es necesario solventar de forma urgente las carencias identificadas, dado que afectan de manera negativa al 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 muy deficiente.

La revisión del cumplimiento de legalidad en materia relacionada con la seguridad de la información ha puesto de manifiesto un nivel de cumplimiento de la normativa muy deficiente. Existen incumplimientos significativos generalizados, 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, reformulamos las recomendaciones que se efectuaron en la auditoría de 2019, considerando, en su caso, las mejoras realizadas 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. Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa y actualizar el procedimiento para la gestión del inventario y el control de activos físicos, de manera que refleje el proceso y las medidas actualmente implantadas.

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

2. Elaborar y aprobar un procedimiento para la gestión integral del *software* de la entidad o actualizar los procedimientos existentes, de manera que contemple:
 - Las medidas actualmente implantadas, incluyendo las listas de *software* autorizado (listas blancas), las medidas técnicas que impiden la ejecución del *software* 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.
3. Revisar y actualizar los sistemas que todavía se encuentran fuera del período de soporte, especialmente aquellos ligados a procesos críticos de la entidad.

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

4. Elaborar y aprobar un procedimiento para la identificación y remediación de vulnerabilidades de manera que aplique de forma integral a la totalidad de sistemas del Ayuntamiento y que considere, además de las medidas implantadas, 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 el seguimiento de anuncios de los fabricantes y boletines en materia de seguridad.
 - La priorización de las vulnerabilidades identificadas basada en el análisis de los riesgos, así como la resolución y documentación, identificando fechas, prioridad, responsable, solución, etc.

Adicionalmente, implantar alguna herramienta para la gestión centralizada de parches de seguridad y actualizaciones que aplique a todos los sistemas y aplicaciones de la entidad.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

5. Elaborar y aprobar un procedimiento de seguridad para la gestión de usuarios con privilegios de administración que incluya aspectos como el alta y baja de este tipo de cuentas, la política de autenticación, *log* de acciones, etc. y hacer extensivo dicho



procedimiento a los usuarios con privilegios de administración de todos los sistemas y aplicaciones de la entidad.

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

6. Elaborar y aprobar 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 Centro Criptológico Nacional³.

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 su revisión periódica, bien manualmente o mediante herramientas automatizadas de monitorización de la configuración.

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

7. Se deben formalizar y aprobar las acciones llevadas a cabo para el tratamiento de *logs* de auditoría de la actividad de los usuarios, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, la gestión de derechos de acceso al registro y la implantación y documentación del proceso de revisión de los *logs*.

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

8. Actualizar el procedimiento para la gestión de copias de seguridad de datos y sistemas de manera que describa, además de las acciones llevadas a cabo (datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas de restauración) y los requisitos de protección de las copias. Adicionalmente, realizar y documentar pruebas de restauración planificadas e implantar las soluciones previstas para la protección de las copias.

³ 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.



Sobre el cumplimiento normativo y gobernanza de la ciberseguridad (CBCS 8)

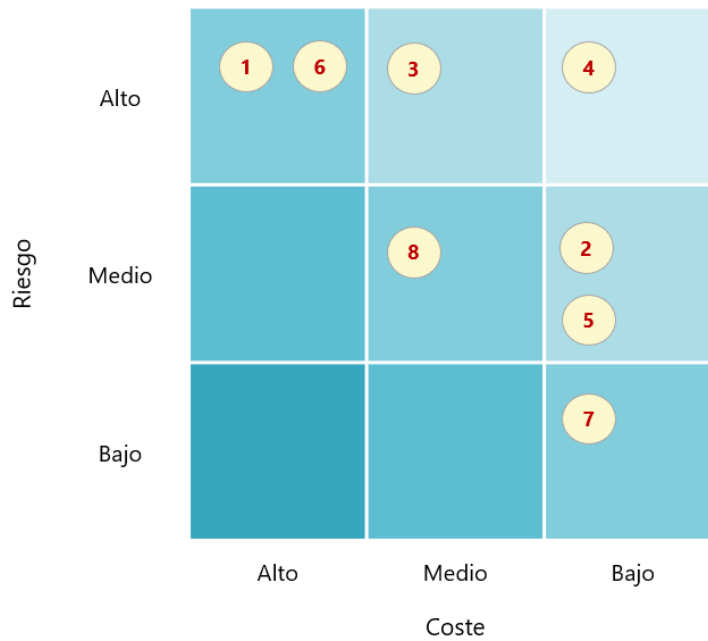
9. Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe:
 - Realizar las auditorías previstas en el artículo 34 del Real Decreto 3/2010.
 - Publicar en la sede 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.
 - Cumplimentar la Instrucción Técnica de Seguridad del Informe del Estado de la Seguridad, de la Secretaría de Estado de Administraciones Públicas (Informe INES).
10. 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:
 - Elaborar el registro de actividades de tratamiento con la información requerida por el RGPD y publicar dicho registro, conforme al artículo 31.2 de la Ley Orgánica 3/2018.
 - Realizar un análisis de riesgos sobre sus tratamientos de datos personales y, en su caso, las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.
 - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD.
 - Planificar y ejecutar auditorías en materia de protección de datos.
11. Llevar a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.

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 no ha sido modificado con respecto al informe de 2019, considerando que no se ha realizado ninguna mejora significativa desde entonces. No se incluyen los puntos 9, 10 y 11 anteriores, ya que son medidas de obligado cumplimiento.



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



Seguimiento de recomendaciones anteriores

Hemos realizado un seguimiento de las recomendaciones efectuadas en el informe de auditoría del año 2019.

Tal como se muestra en el cuadro 2, de las once recomendaciones realizadas en ese informe, seis no se han atendido y cinco lo han sido solo parcialmente.



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 Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Sin variación. Además se debe actualizar el procedimiento correspondiente.	No aplicada	Se actualiza la redacción dada en 2019
2 Elaborar y aprobar un procedimiento para la gestión integral del <i>software</i> de la entidad o modificar los procedimientos existentes, de manera que se contemple, adicionalmente a las acciones actualmente implantadas: <ul style="list-style-type: none"> - La elaboración de listas de <i>software</i> autorizado (listas blancas), la implantación de las medidas técnicas que impidan la ejecución del no autorizado y la realización de revisiones periódicas de <i>software</i>. - La definición de un plan de mantenimiento de la totalidad del <i>software</i> utilizado, incluyendo tanto aquel cuyo mantenimiento se realiza directamente por el Ayuntamiento como el <i>software</i> cuyo mantenimiento se realiza por empresas contratadas con esa finalidad. 	<p>El Ayuntamiento ha realizado algunas acciones que incrementan el nivel de control sobre el inventario de <i>software</i>, aunque de manera limitada.</p> <p>El departamento TIC ha implantado medidas para impedir la ejecución de <i>software</i> no autorizado, pero estas son parcialmente efectivas y no han sido establecidas en un procedimiento formalmente aprobado.</p> <p>No se dispone de un plan de mantenimiento integral de <i>software</i>.</p>	Aplicada parcialmente	Se actualiza la redacción dada en 2019
3 Revisar y actualizar todos los sistemas que se encuentran fuera del período de soporte.	El Ayuntamiento ha renovado parte de los equipos de usuario. No obstante, sigue habiendo sistemas obsoletos conectados a la red corporativa.	Aplicada parcialmente	Se actualiza la redacción dada en 2019
4 Modificar el procedimiento actual de gestión y mantenimiento de activos, incluyendo el proceso de gestión de vulnerabilidades de manera que se aplique de forma integral a la totalidad de sistemas del Ayuntamiento considerando, como mínimo, los siguientes aspectos: <ul style="list-style-type: none"> - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas, el análisis previo a la entrada en producción de los sistemas y el seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad. - La priorización basada en el análisis de los riesgos, la resolución y la documentación de las vulnerabilidades tratadas. 	<p>El Ayuntamiento ha implantado algunas herramientas destinadas a la identificación de vulnerabilidades, como microCLAUDIA y CARMEN del CCN y CSIRT-CV. No obstante, siguen vigentes algunas de las carencias identificadas durante el trabajo de 2019.</p> <p>No se utilizan herramientas que permitan la gestión centralizada de parches y actualizaciones (que sí eran utilizadas durante nuestra anterior revisión), cosa que impacta en el índice de madurez del control y amplía la recomendación.</p>	Aplicada parcialmente	Se actualiza la redacción anterior



Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
<p>Modificar la actual normativa de control de acceso o 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:</p> <p>5</p> <ul style="list-style-type: none"> - La eliminación, siempre que sea posible desde el punto de vista técnico, de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos. - Cuando existan razones de índole técnico que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas. - La política de autenticación a aplicar a este tipo de cuentas. 	<p>El Ayuntamiento ha subsanado parte de las deficiencias detectadas durante nuestra anterior auditoría, pero sigue habiendo posibilidades de mejora para garantizar la efectividad del control.</p> <p>Las acciones implantadas han de establecerse en un procedimiento formalmente aprobado.</p>	<p>Aplicada parcialmente</p>	<p>Se actualiza la redacción dada en 2019</p>
<p>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 Centro Criptológico Nacional.</p> <p>6</p> <p>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.</p>	<p>Aunque existen algunas acciones que mejoran ligeramente el índice de madurez del control, como la seguridad mejorada en los equipos nuevos o el <i>backup</i> de los ficheros de configuración de determinados sistemas, se mantienen nuestras recomendaciones anteriores.</p>	<p>No aplicada</p>	<p>Se mantiene la redacción</p>



Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
<p>7 Aprobar formalmente un procedimiento para el tratamiento de <i>logs</i> de auditoría de la actividad de los usuarios, 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 <i>logs</i>. Para la revisión de <i>logs</i> es aconsejable centralizarlos en sistemas dedicados a tal efecto.</p>	<p>El departamento TIC ha habilitado el registro de acciones en distintos sistemas, que son analizados y centralizados en un SIEM gestionado conjuntamente por los técnicos y por una empresa externa. Sin embargo, la puesta en marcha es posterior al 31 de diciembre de 2021, por lo que no ha sido considerado para el cálculo del índice de madurez del control, pero sí para reformular la recomendación.</p> <p>No existe un procedimiento aprobado y actualizado que recoja las acciones implantadas.</p>	<p>No aplicada</p>	<p>Se actualiza la redacción dada en 2019.</p>
<p>8 Ampliar el alcance del procedimiento existente de copia de seguridad de forma que contemple la realización de pruebas periódicas de recuperación, estableciendo, como mínimo, periodicidad de las pruebas, alcance y personal necesario.</p>	<p>Si bien el proceso implantado en el Ayuntamiento para la copia de seguridad de aplicaciones y sistemas era efectivo durante nuestra anterior revisión, la inexistencia de determinadas medidas de control hace disminuir ligeramente este índice.</p> <p>El Ayuntamiento tiene prevista la implantación de un centro <i>offline</i> de almacenamiento para subsanar las carencias existentes.</p>	<p>Aplicada parcialmente</p>	<p>Se actualiza la redacción dada en 2019.</p>
<p>9 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:</p> <ul style="list-style-type: none"> - Realizar las auditorías previstas en el artículo 34 del Real Decreto 3/2010. - 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. 	<p>El Ayuntamiento no ha cumplimentado la Instrucción Técnica de Seguridad del Informe del Estado de la Seguridad (Informe INES).</p> <p>La situación de los demás aspectos revisados es la misma que en nuestra anterior auditoría, aunque existen acciones en curso destinadas a subsanar los incumplimientos detectados.</p> <p>El Ayuntamiento ha licitado y adjudicado un proyecto para la adecuación al ENS, que se encuentra en ejecución y no ha sido considerado en el cálculo de los índices de madurez por haberse iniciado con posterioridad al 31 de diciembre de 2021.</p>	<p>No aplicada</p>	<p>Se actualiza la redacción dada en 2019.</p>



Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
<p>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:</p> <ul style="list-style-type: none"> - Nombrar un DPD de acuerdo con lo previsto en el artículo 37.1.a) del RGPD. - Elaborar el registro de actividades de tratamiento con la información requerida por el RGPD y publicar dicho registro, conforme al artículo 31.2 de la Ley Orgánica 3/2018. - Realizar un análisis de riesgos sobre sus tratamientos de datos personales y, en su caso las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD. - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD. - Planificar y ejecutar auditorías en materia de protección de datos. 	<p>El Ayuntamiento ha licitado y adjudicado un proyecto para cumplir con los requisitos establecidos por la normativa.</p> <p>Las acciones llevadas a cabo no han sido consideradas en el cálculo de los índices de madurez por haberse iniciado con posterioridad al 31 de diciembre de 2021, aunque sí han sido tenidas en cuenta para reformular nuestras recomendaciones.</p> <p>En 2022 se ha nombrado el DPD.</p>	<p>No aplicada</p>	<p>Se actualiza la redacción dada en 2019</p>
<p>11 Llevar a cabo la auditoría del registro de facturas exigida por la Ley 25/2013, de 27 de diciembre.</p>	<p>Sin variación en 2021.</p>	<p>No aplicada</p>	<p>Se mantiene la redacción</p>



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 actuaciones en materia de ciberseguridad en diversos ámbitos que atenderían algunas de las recomendaciones anteriores. Estas actuaciones se encuentran alineadas con los objetivos del Ayuntamiento para la adecuación al ENS y algunas se han iniciado como consecuencia de las recomendaciones realizadas en la auditoría del año 2019. La implantación efectiva de estas actuaciones tendrá un impacto positivo en el nivel de ciberseguridad de la entidad.

Enumeramos a continuación aquellas actuaciones que se encuentran en ejecución al emitir este informe y que por su relevancia deben ser destacadas:

- En 2021 se adjudicaron cuatro lotes del “Contrato de servicio para la gestión de la infraestructura y seguridad de las TIC del Ayuntamiento de Paterna”, que incluyen el mantenimiento, actualización, licenciamiento, asesoramiento y asistencia técnica de la infraestructura, seguridad, *software* y comunicaciones de las TIC del Ayuntamiento, que incluye, entre otros:
 - Auditorías de ciberseguridad de determinados sistemas críticos.
 - Actualización de versiones de determinados sistemas.
 - Campañas de formación y concienciación a los trabajadores.
 - Implantación de doble factor de autenticación en determinados sistemas.
 - Horas de soporte/formación al personal del departamento.
 - *Hacking* ético.
 - Implantación de nuevos servicios y mejoras de los existentes.
- Finalización de la implantación de la herramienta SIEM y explotación de su información, proyecto que se encuentra en fase de ejecución durante el segundo semestre de 2022; el Ayuntamiento recibe informes periódicos y mantiene reuniones para la subsanación de incidentes.
- Adjudicación en 2022 del “Contrato de servicio de auditoría de revisión y adecuación de cumplimiento del ENS y normativa en materia de protección de datos personales y prestación de las funciones asociadas a la figura del delegado de protección de datos”, del que se han realizado algunas acciones durante el segundo semestre de 2022, como las reuniones iniciales del ENS o el nombramiento del DPD.



- El Ayuntamiento ha iniciado en 2022 un proyecto con las subvenciones recibidas mediante los fondos europeos del plan de recuperación, transformación y resiliencia Next Generation EU. El proyecto incluye:
 - La puesta en marcha de un centro de operaciones de ciberseguridad (SOC). El proyecto cuenta con la instalación de un agente de monitorización de puestos y servidores, la integración de un sistema de alerta temprana sobre el del CSIRT-CV, la implantación de un EDR y aspectos de formación.
 - La aplicación de las medidas de protección para cumplimiento del ENS, tales como la adecuación de infraestructuras, la protección de la información (centro de almacenamiento *offline*) y las comunicaciones y aspectos de formación.



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 INES⁴ 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.

⁴ 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 Paterna. Ejercicio 2019 y obtener una seguridad limitada y concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación tanto sobre su diseño⁵ como sobre su eficacia operativa⁶ para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte, así como sobre el cumplimiento de la normativa básica relativa a la seguridad de la información.

También formulamos 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 2019 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

⁵ 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.

⁶ 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)

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)⁷, 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:

⁷ 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 <i>software</i> 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 <i>software</i> y <i>hardware</i>	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) señala⁸ 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 ciberriesgos⁹.

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 día¹⁰.

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

[Review of Cyber Hygiene Practices](#), ENISA, diciembre de 2016. Véase página 14.

⁹ 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.

¹⁰ 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 <i>hardware</i>	CBCS 1
2. Tener un registro de todo el <i>software</i> 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 <i>hardware</i> 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 <i>software</i> autorizado	Gestionar activamente todo el <i>software</i> en los sistemas, de forma que solo se pueda instalar y ejecutar <i>software</i> 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 <i>software</i> y <i>hardware</i> 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 <i>logs</i> de auditoría)	Recoger, gestionar y analizar <i>logs</i> de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	CBCS 6-1: Activación de <i>logs</i> de auditoría	El <i>log</i> 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 <i>logs</i> : Retención y protección	Los <i>logs</i> 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 <i>logs</i>	Los <i>logs</i> 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 <i>logs</i> de auditoría, de forma que se facilite su revisión.
		CBCS 6-4: Monitorización y correlación	La entidad dispone de un SIEM (<i>security information and event management</i>) o una herramienta de analítica de <i>logs</i> para realizar correlación y análisis de <i>logs</i> .
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	<p>Cubre al 100% con el objetivo de control y:</p> <ul style="list-style-type: none">- 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	<p>En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100% y:</p> <ul style="list-style-type: none">- 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	<p>Cubre de forma muy limitada el objetivo de control y:</p> <ul style="list-style-type: none">- Se sigue un procedimiento, aunque este puede no estar formalizado.- El resultado de las pruebas de implementación y de eficacia no es satisfactorio. <p>Cubre en líneas generales el objetivo de control, pero:</p> <ul style="list-style-type: none">- 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	<p>No cubre el objetivo de control.</p> <p>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).</p>

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. <i>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.</i>
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. <i>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.</i>
N3 Proceso definido	80	Los procesos están estandarizados, documentados y comunicados con acciones formativas. <i>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.</i>
N4 Gestionado y medible	90	La dirección controla y mide el cumplimiento de los procedimientos y adopta medidas correctoras cuando se requiere. <i>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.</i>
N5 Optimizado	100	Se siguen buenas prácticas en un ciclo de mejora continua. <i>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.</i>



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 ha 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 son¹¹:

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%.

¹¹ 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.¹²

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**¹³.

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

¹² Véase el [glosario de la Information Systems Audit and Control Association \(ISACA\)](#).

¹³ 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 ciberseguridad¹⁴. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información¹⁵ 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 TIC¹⁶, 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.

¹⁴ [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.

¹⁵ [UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información](#), apartado 3.4.

¹⁶ [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 Paterna. Ejercicio 2019.

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 la auditoría

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 a la situación en la que se encontraba el control en nuestra anterior auditoría. Se ha contratado un servicio de auditoría que incluirá la revisión y actualización de todos los procedimientos.

El Ayuntamiento adjudicó, a principios de 2021, un contrato de renovación de equipos de usuario. El departamento TIC ha realizado una revisión completa de sus activos y la actualización del inventario; además, ha desarrollado guías de instalación para el nuevo equipamiento y utiliza hojas de entrega que detallan quiénes son los responsables de cada equipo.

Se dispone de un nuevo sistema MDM para la gestión y administración de dispositivos móviles, pero nos han indicado que en el momento de la revisión este sistema no está completamente operativo ni integra la totalidad de dispositivos existente en la entidad.

Sobre el control de dispositivos físicos no autorizados, se han aplicado determinadas medidas de seguridad para impedir las conexiones no autorizadas, pero estas tienen una efectividad muy limitada, por lo que mantenemos nuestra recomendación al respecto.

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 46,1%**, 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 57,6%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 44,1%; por tanto, se ha producido una leve mejora de 2 puntos en ese índice.

CBCS 2. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) todo el *software*, 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 ha realizado algunas acciones que mejoran el control sobre el inventario y el *software* autorizado, sin embargo, deben seguir trabajando para alcanzar los niveles exigidos por el ENS. Además, las acciones realizadas para el control de *software* no se encuentran establecidas en un procedimiento actualizado y formalmente aprobado.

El departamento TIC ha sustituido la mayoría de equipos de usuario cuyos sistemas operativos estaban obsoletos y sin soporte del fabricante mediante el proyecto de actualización descrito en el CBCS 1. No obstante, siguen existiendo sistemas obsoletos conectados a la red corporativa que, aunque no es un número significativo, representan un riesgo y deberían actualizarse.

Aunque no se dispone de ninguna aplicación que impida totalmente la ejecución de *software* no autorizado en los sistemas de la entidad, existen medidas compensatorias que proporcionan cierta efectividad del control:

- Aplicación de políticas de seguridad a los equipos de usuario para impedir instalaciones a usuarios sin privilegios de administración.
- Listado de aplicaciones a instalar en todos los equipos incluido en los procedimientos internos del departamento TIC. Aunque no es una lista blanca formalmente aprobada, los procedimientos internos del departamento TIC incluyen el listado de aplicaciones para los equipos nuevos, que es definido por los técnicos atendiendo a las necesidades de la organización.
- El *software* de inventario, el antivirus y el *firewall* tienen opciones para impedir la ejecución de aplicaciones no autorizadas, pero el bloqueo de *software* no autorizado en dichas aplicaciones no es completamente efectivo.

Existen acciones previstas, como la migración de las bases de datos de aplicaciones críticas obsoletas o la implantación de un sistema EDR, que mejorarán el control una vez implantadas.

El Ayuntamiento no dispone de un plan de mantenimiento que describa la gestión integral de *software*, que incluya tanto el contratado como el resto utilizado en el Ayuntamiento.

Existe un insuficiente nivel de control sobre el inventario y control de *software* autorizado, siendo el **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 2 del 70,6%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 51,3%, por tanto, se ha producido una leve mejora de 5,2 puntos en ese índice.



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 ha realizado determinados cambios en el control de vulnerabilidades; sin embargo, el índice de madurez del control no refleja estas mejoras. Esto es debido a que en uno de los subcontroles evaluados no se realizan las acciones que garanticen la efectividad del control.

El Ayuntamiento ha realizado el despliegue de la herramienta microCLAUDIA del CCN en los sistemas y equipos de usuario de la entidad, herramienta que proporciona protección contra código dañino de tipo *ransomware*, que además se incluye en la maqueta de equipos de usuario. También han desplegado la solución CARMEN, ofrecida por el CCN-CERT y gestionada por el CSIRT-CV, que alerta mediante informes periódicos de anomalías en la red. Los técnicos del departamento de informática aplican medidas acordes con los resultados de dichos informes, aunque no documentan las actuaciones en la herramienta de *ticketing*. Las alertas de CARMEN se envían al correo del responsable, si bien deberían llegar a todos los integrantes del departamento.

Una de las buenas prácticas llevadas a cabo por el departamento TIC es la contratación de una empresa que realiza la vigilancia del sistema SIEM del Ayuntamiento, informando periódicamente de las deficiencias detectadas y manteniendo reuniones para subsanarlas, aunque se ha implantado durante el ejercicio 2022 y no ha sido valorado para el presente informe por no encontrarse dentro del periodo auditado.

Una de las carencias detectadas durante la revisión es la no utilización de un gestor centralizado para la aplicación de parches y actualizaciones. Aunque existen controles compensatorios (aplicación de directivas para forzar a los equipos a buscar y descargar actualizaciones o la instalación manual de estas), la inexistencia de un gestor centralizado impide tener una visión global del conjunto de sistemas, existiendo un desconocimiento de aquellos que no se están actualizando.

Aunque algunas de las acciones relacionadas con el control de vulnerabilidades estaban establecidas en un procedimiento aprobado, el Ayuntamiento debe actualizar los procedimientos con las acciones llevadas a cabo.

La valoración global sobre este control alcanza un **índice de madurez del 59,1%**, 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 3 del 73,9%**.



La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 53,6%, por tanto, se ha producido una leve mejora de 5,5 puntos en ese índice.

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 ha realizado determinados cambios en el uso controlado de los privilegios administrativos respecto de la situación observada en la revisión anterior, pero todas las acciones deben recogerse en procedimientos formalmente aprobados.

El departamento TIC ha revisado los usuarios administradores en los sistemas críticos, eliminando los usuarios genéricos no nominativos y las cuentas no utilizadas, subsanando así la deficiencia detectada en 2019.

Además de la revisión de usuarios en los distintos sistemas, el departamento TIC ha establecido, para cada uno de los administradores, el uso de cuentas con distintos niveles de privilegios, que utilizan en función del trabajo a realizar.

El control existente sobre los usuarios administradores debe establecerse en un procedimiento formalmente aprobado y las acciones implantadas (identificación, control de accesos, mecanismos de autenticación, registro de acciones, etc.) deben aplicarse de manera homogénea en todos los sistemas y aplicaciones de la entidad.

Existe cierto nivel de control sobre las cuentas con privilegios administrativos y la valoración global del control supone un **índice de madurez del 61,7%**, 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 77,1%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 58,6%, por tanto, se ha producido una leve mejora de 3,1 puntos en el índice de madurez del control.

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 ploten servicios y configuraciones vulnerables.

Situación del control

El departamento TIC ha desarrollado un procedimiento que describe las acciones realizadas para la instalación de equipos nuevos, que incluye aspectos relacionados con las configuraciones seguras de *software* y *hardware*, aunque es un documento interno del departamento y no está formalmente aprobado.

El procedimiento anterior describe los trabajos sobre las máquinas previamente a su entrada en producción, e incluye aspectos de seguridad como revisar que las políticas de seguridad se apliquen correctamente o la implantación de la seguridad mejorada con un aplicativo propio de la marca de los equipos. Sin embargo, esta funcionalidad únicamente está habilitada en los equipos de nueva adquisición.

El departamento TIC dispone de repositorios donde se almacenan configuraciones de algunos sistemas, como los *firewall* o *switches*, y además el procedimiento de copias de seguridad establece la ubicación, responsables y periodicidad de dichas copias.

No se dispone de sistemas para la monitorización de cambios no autorizados en las configuraciones ni las acciones llevadas a cabo para impedir cambios no autorizados están documentadas y aprobadas en un procedimiento de gestión de cambios.

Existe, por tanto, un deficiente nivel de control en la aplicación de configuraciones seguras en dispositivos y *software*, por lo que se deben dedicar esfuerzos y recursos para mejorar el control. La valoración global del control alcanza un **índice de madurez del 25,0%**, que se corresponde con un **nivel de madurez N1, inicial/ad hoc**; es decir, el proceso existe, pero no se gestiona o la gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 5 del 31,3%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 12,4%; por tanto, se ha producido una mejora de 12,6 puntos en el índice de madurez del control.

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 tenía habilitados, durante nuestro trabajo anterior de auditoría, los registros de actividad en los sistemas revisados y existía cierto nivel de control en



funcionamiento, pero los controles se aplicaban de manera informal y no están establecidos en un procedimiento formalmente aprobado.

Aunque el Ayuntamiento ha realizado cambios que mejoran significativamente la situación observada durante nuestra anterior auditoría, estos cambios han sido implantados en 2022, por lo que no han sido considerados al calcular el índice de madurez del control.

Se ha contratado la implantación de un sistema SIEM que incluye parte de los sistemas de la entidad, y la formación y reporte de anomalías por parte de la empresa adjudicataria. El servicio contratado es 24/7¹⁷ y la empresa genera informes mensuales que son analizados en reuniones con el personal del departamento TIC, quienes corrigen las vulnerabilidades detectadas. Estas vulnerabilidades se introducen automáticamente en el gestor de *tickets* como incidencias. Además, el departamento TIC documenta las reuniones, contratos y actas en un gestor de expedientes.

El departamento TIC ha habilitado el registro de las acciones en el *software* utilizado para la gestión de usuarios administradores que comparten los miembros del departamento TIC.

El Ayuntamiento sigue sin un procedimiento aprobado que defina una política para los registros de auditoría (sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso a los *logs*, etc.).

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 60,0%**, 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 6 del 75,0%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,0%; por tanto, a fecha 31 de diciembre de 2021, no se ha producido ninguna mejora respecto de la situación anterior.

CBCS 7. COPIA DE SEGURIDAD DE DATOS Y SISTEMAS

Objetivo del control

Utilizar procesos y herramientas para realizar copias de seguridad de la información crítica con una metodología que permita la recuperación de la información en tiempo oportuno.

Situación del control

El Ayuntamiento ha realizado algunos cambios respecto a la situación observada en la revisión anterior. Aunque se han aplicado algunas acciones de mejora, existen

¹⁷ 24 horas, 7 días a la semana.



circunstancias que hacen que el control no alcance el mismo nivel de madurez que alcanzaba en 2019.

Durante nuestro anterior trabajo de auditoría observamos la existencia de un buen nivel de control sobre las copias de seguridad de datos y sistemas, dado que se realizaban casi todas las acciones evaluadas: realización de copias, realización de determinadas pruebas de restauración planificadas, protección de *backups* y el proceso estaba correctamente documentado. Sin embargo, durante el presente trabajo, hemos observado que alguna de las prácticas que en aquel momento se valoró como efectiva ha dejado de llevarse a cabo. Por ejemplo, han dejado de utilizarse copias de seguridad desconectadas. Aunque existen controles compensatorios (los servidores de copia únicamente son accesibles desde ciertas máquinas), existe cierto nivel de riesgo que no existía con las copias de seguridad desconectadas.

Aunque el objetivo del Ayuntamiento es implantar un centro *offline* de almacenamiento, que ha sido incluido en el "expediente para la contratación del suministro, instalación y puesta en marcha de un centro de operaciones de ciberseguridad y aplicación de las medidas de protección para cumplimiento del ENS, financiado por plan de recuperación, transformación y resiliencia - Unión Europea Next Generation", a fecha 31 de diciembre de 2021 dicha mejora no se encontraba implantada y no se ha considerado en el cálculo del índice de madurez a esa fecha.

Adicionalmente, una de las carencias detectadas es la revisión del estado de las copias únicamente por parte de uno de los técnicos responsables. Dicha práctica conlleva el riesgo de no realizar correctamente las copias y no advertirlo en caso de ausencia de la persona que habitualmente realiza el trabajo.

La valoración global del control existente sobre las copias de seguridad es que el Ayuntamiento alcanza un **índice de madurez del 74,8%**, 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 93,5%**, lo que implica un empeoramiento respecto de nuestra anterior auditoría.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 80,0%; por tanto, ha disminuido en 5,2 puntos el índice de madurez del control.

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

No se han realizado las auditorías previstas en el artículo 34 del Real Decreto 3/2010 ni, en consecuencia, se han publicado 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.

Nuestro informe de auditoría de los CBCS del año 2019 se dio a conocer al Pleno del Ayuntamiento en sesión ordinaria celebrada el 28 de octubre de 2020, en el que se acordó el inicio de un expediente de contratación para subsanar los incumplimientos legales detectados. Dicha contratación, adjudicada en julio de 2022, incluye un proyecto destinado al cumplimiento del ENS.

Además de los incumplimientos advertidos en nuestro anterior trabajo, el Ayuntamiento no ha cumplimentado y remitido el Informe del Estado de la Seguridad (Informe INES) correspondiente al ejercicio fiscalizado.

Cumplimiento del RGPD

En cuanto al cumplimiento en materia de protección de datos personales, durante la revisión realizada en el año 2019 detectamos deficiencias significativas, como la inexistencia del rol del DPD en el Ayuntamiento, ausencia del registro de actividades del tratamiento o de un análisis de riesgos en este campo, entre otras.

Pese a nuestras recomendaciones de 2019, el Ayuntamiento ha seguido incumpliendo la normativa en esta materia, por lo que ha recibido un aviso de la AEPD para subsanar su situación.

En la licitación para el cumplimiento del ENS adjudicada en 2022, el Ayuntamiento ha incluido la contratación de servicios relacionados con la protección de datos de carácter personal, como el nombramiento del DPD, realizado en 2022, aunque pendiente de notificar a la AEPD.

Siguen existiendo, por tanto, incumplimientos significativos que se deben subsanar:

- No se ha finalizado y publicado el registro de actividades de tratamiento, conforme al artículo 31.2 de la Ley Orgánica 3/2018.
- No se han realizado los análisis de riesgos sobre los tratamientos de datos personales y, en su caso, las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.
- No se han aplicado las medidas organizativas y técnicas necesarias para proteger los datos personales, requeridas por el artículo 24.1 del RGPD.
- No se han ejecutado auditorías de cumplimiento en materia de protección de datos.



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

Cumplimiento de la legalidad del registro de facturas

No se han realizado las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.

Indicadores

En resumen, y aunque se está trabajando en subsanar la situación, la valoración global sobre el cumplimiento de los aspectos de legalidad a fecha 31 de diciembre de 2021 ha empeorado respecto al informe emitido en el año 2019 (20,0%), alcanzando el Ayuntamiento un **índice de madurez del 18,0%**, 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 22,5%**.

La disminución en el índice de madurez respecto de la situación observada durante nuestra anterior auditoría es debida a que, además seguir vigentes los incumplimientos observados en nuestro anterior trabajo, el Ayuntamiento no ha emitido el informe INES correspondiente al ejercicio fiscalizado.

Como ya se ha señalado, para subsanar la situación, el Ayuntamiento ha adjudicado en julio de 2022 un contrato para realizar las tareas de adecuación al ENS y a la normativa de protección de datos de carácter personal. Las mejoras introducidas mediante este contrato no han sido consideradas para el cálculo de los índices de madurez por haberse realizado con posterioridad al 31 de diciembre de 2021.

Gobernanza de la ciberseguridad

El Ayuntamiento de Paterna no tiene establecida una adecuada gobernanza de la seguridad de la información.

Existe cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los miembros del departamento TIC y de los órganos superiores del Ayuntamiento, que se observa en aspectos como:

- El Ayuntamiento dispone de una política de seguridad aprobada, que se completa con un marco normativo y procedimental, pero esta documentación no está actualizada.
- La existencia de apoyo al departamento TIC, tanto político como en forma de recursos económicos y humanos.

Sin embargo, determinadas circunstancias indican que la gobernanza no puede considerarse efectiva. Basamos esta afirmación en las siguientes carencias relevantes:

- La falta de liderazgo en materia de ciberseguridad de los órganos superiores del Ayuntamiento.



La organización no dispone de planes ni estrategias elaboradas y aprobadas por los órganos superiores en relación con la seguridad de la información, ni impulsa las medidas de seguridad necesarias, incluyendo la formación y concienciación de sus trabajadores. Son los miembros del departamento TIC, por propia iniciativa y sin el respaldo del comité de seguridad de la información, quienes implantan las medidas necesarias relacionadas con la ciberseguridad e impulsan el cumplimiento de la normativa en esta materia.

- La falta de atención a los incumplimientos legales identificados durante nuestro anterior informe de auditoría. A fecha 31 de diciembre de 2021, el Ayuntamiento seguía sin nombrar al DPD ni atender a ninguno de los incumplimientos que señalábamos. En julio de 2022 el Ayuntamiento ha contratado un "Servicio de auditoría de revisión y adecuación al ENS y normativa de protección de datos personales".
- La necesidad de que el comité de seguridad de la información funcione de forma efectiva, órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas del Ayuntamiento.

Es en el comité de seguridad donde deben tomarse las decisiones concretas en materia de seguridad de la información, aprobando las medidas pertinentes e impulsando las acciones a llevar a cabo. Aunque este órgano está definido en la política de seguridad aprobada por el Ayuntamiento, no ejerce sus funciones de manera efectiva. El Comité debe reunirse periódicamente y, en una entidad del tamaño del Ayuntamiento de Paterna y dada la complejidad de sus sistemas, recomendamos que se haga al menos mensualmente.

- La política de seguridad de la información y las normas y procedimientos de seguridad no están actualizadas.

El Ayuntamiento dispone de política de seguridad de la información aprobada en 2013, que además se completaba con un marco normativo (uso correcto de equipos, servicios, instalaciones, aplicaciones autorizadas, control físico de accesos, etc.) y procedimental (procedimientos que detallan cómo se realizan las tareas habituales, responsables, etc.). No obstante, esta documentación debe ser actualizada con los procesos actualmente implantados.

- Algunos de los roles en materia de seguridad no están correctamente definidos.

El rol de responsable de seguridad se corresponde con la responsable del departamento TIC y esto es incompatible. De acuerdo con el ENS y la guía CCN-STIC 801, el responsable de la seguridad "deberá ser una persona física, jerárquicamente independiente del responsable del sistema". Si el responsable de seguridad está legitimado para determinar, supervisar y pronunciarse sobre la idoneidad de las medidas de seguridad adoptadas, este rol no puede recaer sobre la persona encargada de su implantación y explotación diaria.



- Falta de agilidad administrativa, particularmente en la gestión de las contrataciones, que disminuye la capacidad de reacción ante situaciones de riesgo y limita las oportunidades de mejora.



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.



Implantación de una herramienta SIEM

El registro de acciones de los distintos sistemas y dispositivos es recogido por la herramienta de analítica de *logs* implantada a tal efecto, que además del análisis de *logs* detecta comportamientos anómalos mediante la correlación de eventos.

La herramienta SIEM es revisada 24/7 por una empresa contratada a tal efecto, que revisa diariamente y emite informes sobre el estado de los sistemas del Ayuntamiento. Además, se mantienen reuniones periódicas entre los técnicos del departamento TIC y la empresa, en las que se revisan las incidencias detectadas y se proponen correcciones, además de registrarse en actas todas las decisiones.



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.



Cibervigilancia / Vigilancia digital: Vigilancia digital es un servicio de detección de amenazas y rastreo de información sensible a través de internet basado en inteligencia artificial que facilita a las empresas adecuar su estrategia de negocio y mejorar el proceso de toma de decisiones.

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.

EDR¹⁸: Un sistema EDR, acrónimo en inglés de *Endpoint Detection Response*, es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

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

¹⁸[Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa](#), Instituto Nacional de Ciberseguridad (INCIBE)



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.

vSOC (*virtual Security Operations Center*): Centro de operaciones de ciberseguridad (SOC) virtual. El proyecto vSOC para entidades locales en la Comunidad Valenciana es una herramienta cedida por el Centro Criptológico Nacional y gestionada por el CSIRT-CV que permite controlar la seguridad de los ayuntamientos desde un único punto o centro de operaciones de ciberseguridad virtual.



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 responsable del sistema, la responsable de seguridad y una representante designada por la secretaria general, 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, este 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 11 de enero de 2023, aprobó este informe de auditoría.



Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Informe seguimiento recomendaciones CBCS Paterna 2019_cas - SEFYCU 3783220

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 3RFP KVVQ 4PNK 9CZP

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 - 17/01/2023 7:45
VICENT CUCARELLA TORMO