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 VALÈNCIA DEL AÑO 2019

Situación a 31 de diciembre de 2021

RESUMEN

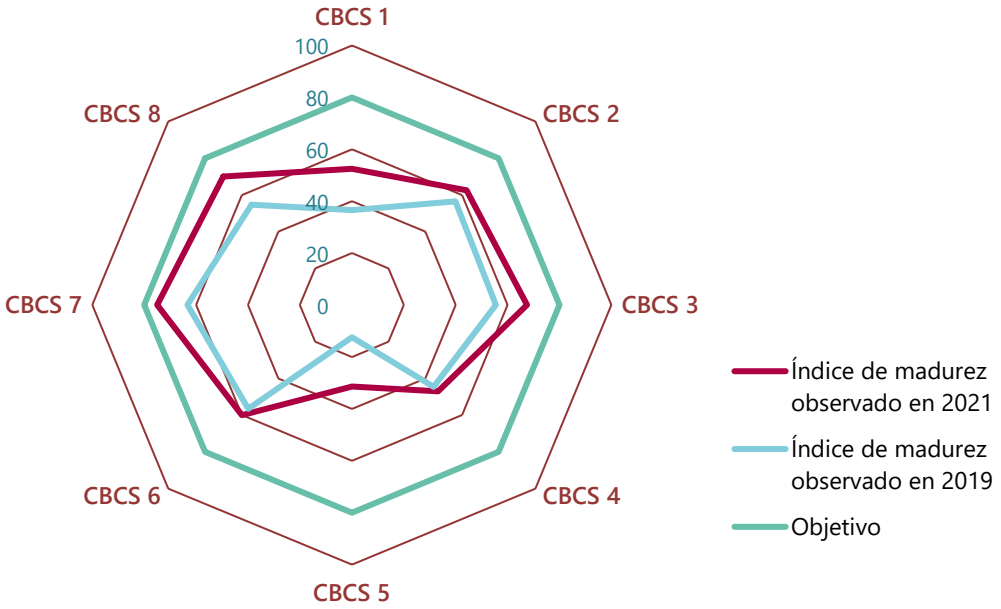
La transformación digital que están experimentando todas las Administraciones públicas y su interconexión a través de complejas redes informáticas las expone de forma cada vez más intensa a amenazas provenientes del ciberespacio. Esto origina un incremento de los riesgos asociados a los sistemas de información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

Conclusiones y recomendaciones

Aunque se han realizado progresos desde nuestra anterior auditoría y nuestras recomendaciones se han atendido parcialmente, el índice de madurez general de los controles básicos de ciberseguridad muestra un valor del 58,2% (47,5% en 2019), por lo que el nivel de efectividad en los controles analizados continúa siendo insuficiente y debe mejorar 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.

El Ayuntamiento tiene en marcha un conjunto de proyectos que, si se ejecutan y gestionan adecuadamente, contribuirán a mejorar sustancialmente los niveles de ciberseguridad de sus sistemas de información, aspecto crítico dado su tamaño y complejidad.



El Ayuntamiento de València tiene establecida una aceptable gobernanza de la ciberseguridad, pero tiene pendiente de constituir el comité de seguridad de la información.

Los órganos superiores del Ayuntamiento deben mantener el actual nivel de compromiso y apoyo a la seguridad de la información, con objeto de garantizar el desarrollo efectivo de los proyectos en curso, mejorar los niveles de madurez de los controles y solventar las deficiencias identificadas.

Asimismo, nuestra revisión también ha puesto de manifiesto que el grado de cumplimiento en cuanto a la adecuación a las normas legales relacionadas con la seguridad de la información ha mejorado, pero siguen existiendo incumplimientos que deben subsanarse. El informe señala diversos aspectos sobre los que se debe actuar para su pronta subsanación. En relación con el Esquema Nacional de Seguridad, el Ayuntamiento debe actualizar y aprobar la política de seguridad para que se adapte a las nuevas circunstancias técnicas y organizativas, incluyendo la regulación de los roles de seguridad y el comité de seguridad.

También hemos realizado una serie de recomendaciones con el propósito de contribuir a subsanar las deficiencias observadas y mejorar los procedimientos de gestión de la ciberseguridad del Ayuntamiento. Entre ellas aconsejamos formalizar un procedimiento unificado para gestión de usuarios con privilegios de administración, finalizar la implantación de las soluciones adquiridas para restringir el acceso de dispositivos físicos no autorizados a la red corporativa y finalizar las actuaciones iniciadas y planificadas para actualizar todos los sistemas que se encuentran fuera del periodo de soporte.

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 leer el 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 València del año 2019

Situación a 31 de diciembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

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

En la guía de auditoría GPF-OCEX 5311, "Ciberseguridad, seguridad de la información y auditoría externa", del *Manual de fiscalización* de la Sindicatura de Comptes, se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las Administraciones públicas, razón por la que los auditores públicos les deben prestar cada vez más atención. En línea con lo anterior, **en el Plan Estratégico de la Sindicatura de Comptes para el periodo 2019-2022 se señala 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 4 de marzo de 2020 el Consell de la Sindicatura de Comptes aprobó el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València, 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 fundamental[1] relacionado con la seguridad de la información y equivale a establecer medidas rutinarias sencillas para minimizar los riesgos de las ciberamenazas. De manera análoga a lo que ocurre con la higiene personal, las buenas prácticas de ciberhigiene pueden impulsar una mayor inmunidad en las entidades que las aplican, lo que reduce el riesgo frente a un ciberataque.

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

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

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

Cambio en los sistemas de información auditados

El conjunto de aplicaciones que proporciona soporte para la gestión contable y presupuestaria del Ayuntamiento, incluido el Sistema de Información Económico Municipal (SIEM), ha sido sustituido en 2022 por un nuevo sistema tecnológicamente más complejo y avanzado denominado SEDA. En la actual auditoría realizada en 2022 se ha omitido la revisión del sistema utilizado hasta el año 2021 dado que ya no estaba siendo utilizado.

La revisión del nuevo sistema SEDA, que incluye al anterior SIEM y a una pluralidad de otras aplicaciones de gestión económica, no ha sido incluida en el presente trabajo y está siendo objeto de una auditoría de seguridad específica con mayor profundidad.

4. CONCLUSIONES

Aunque se han realizado progresos desde nuestra anterior auditoría y nuestras recomendaciones se han atendido parcialmente, el índice de madurez general de los CBCS sigue siendo insuficiente.

El Ayuntamiento tiene en marcha un conjunto de proyectos que, si se ejecutan y gestionan adecuadamente, contribuirán a mejorar sustancialmente los niveles de ciberseguridad de sus sistemas de información, aspecto crítico dado su tamaño y complejidad.

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 58,2%**, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o no formalizados documentalmente.

El Ayuntamiento ha atendido de forma parcial nuestras recomendaciones y el índice de madurez general ha mejorado desde el 47,5% identificado en nuestra auditoría de 2019, pero 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

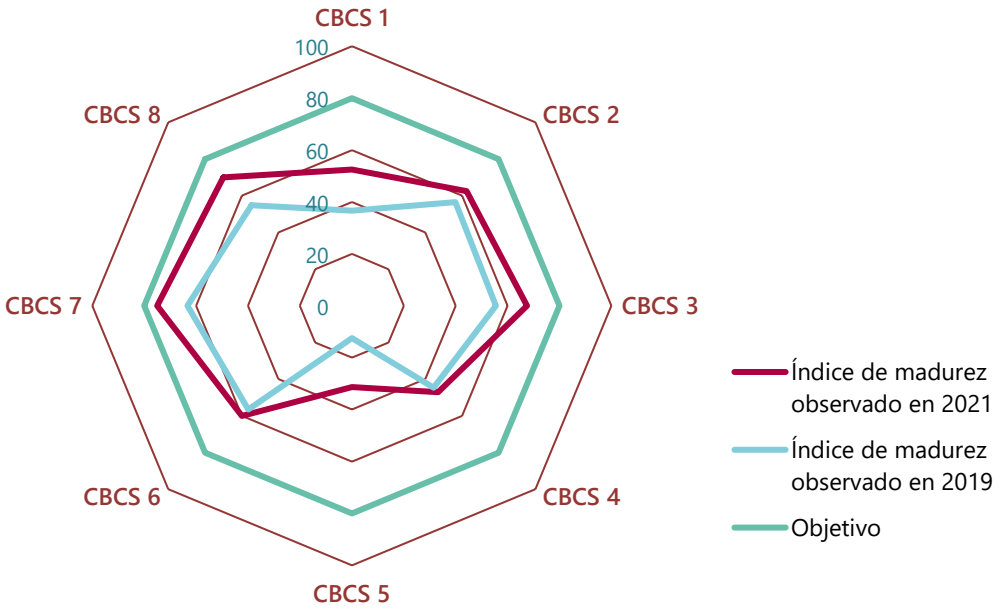
Control	2019			2021		
	Índice de madurez	Nivel de madurez	Índice de cumplimiento	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	*36,6%*	***N1***	*45,8%*	52,5%	N2	65,6%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	*56,5%*	*N2*	*70,6%*	62,5%	N2	78,1%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	*55,5%*	*N2*	*69,4%*	67,5%	N2	84,4%
CBCS 4 Uso controlado de privilegios administrativos	*44,6%*	***N1***	*55,7%*	47,0%	**N1**	58,7%
CBCS 5 Configuraciones seguras del *software* y *hardware*	*12,4%*	***N1***	*15,5%*	31,4%	**N1**	39,2%
CBCS 6 Registro de la actividad de los usuarios	*56,5%*	*N2*	*70,6%*	60,0%	N2	75,0%
CBCS 7 Copias de seguridad de datos y sistemas	*63,3%*	*N2*	*79,2%*	75,0%	N2	93,8%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	*54,8%*	*N2*	*68,4%*	70,0%	N2	87,5%
General	47,5%	***N1***	59,4%	58,2%	*N2*	72,8%

El índice de cumplimiento de los CBCS es del 72,8%, que resulta de comparar el indicador de madurez con el nivel requerido u objetivo que tiene el sistema según el ENS, que es el 80%. Este índice ha mejorado desde el 59,4% de nuestro anterior informe.

La comparación de los resultados detallados del presente trabajo con los obtenidos en el año 2019 muestra una mejora en todos los controles. No obstante, a pesar de la mejora experimentada, el nivel de efectividad en los controles analizados es insuficiente, ya que ninguno alcanza el objetivo y existen claras posibilidades de mejora para alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información, y particularmente sobre los controles que presentan deficiencias significativas y no alcanzan el nivel de madurez N2 (CBCS 4 y 5). 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 València tiene establecida una aceptable gobernanza de la ciberseguridad, pero tiene pendiente de constituir el comité de seguridad de la información. Se debe mantener el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información, y finalizar las acciones iniciadas.

Los órganos superiores del Ayuntamiento (en particular el alcalde y la Junta de Gobierno) son los responsables de que existan unos controles de seguridad adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo

constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad. El compromiso y concienciación con la ciberseguridad también debe extenderse a la dirección[2] (tal como queda definida en el glosario al final de este informe), que son los responsables de articular y facilitar la ejecución de las actividades establecidas por la alta dirección en materia de ciberseguridad.

Hemos podido verificar la existencia de un adecuado nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento, lo que, junto con la existencia de unos adecuados procesos de gestión, nos permite concluir que la gobernanza de ciberseguridad alcanza un nivel aceptable.

No obstante, hemos identificado alguna carencia relevante, como la inexistencia de un comité de seguridad, que debe ser subsanada. También es preciso separar la responsabilidad de la seguridad de los sistemas de información de la responsabilidad sobre la explotación de dichos sistemas.

Existen proyectos e iniciativas que se encuentran en fase de ejecución o de planificación que, en caso de ser finalizados y gestionados de manera efectiva, tendrán un impacto positivo desde el punto de vista operativo y de la seguridad. Además, existe una planificación estratégica de la seguridad de la información que ha sido materializada en el Plan Director de Seguridad de los Sistemas de Información, aprobado por la Junta de Gobierno el 23 de diciembre del año 2021, que orienta de forma coherente las acciones en esta materia.

Los órganos superiores del Ayuntamiento deben mantener el actual nivel de compromiso y apoyo a la seguridad de la información, con objeto de garantizar el desarrollo efectivo de los proyectos en curso, mejorar los niveles de madurez de los controles y solventar las deficiencias identificadas.

El grado de cumplimiento de la normativa relativa a la seguridad de la información ha mejorado, pero siguen existiendo incumplimientos que deben subsanarse.

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

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

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

   Finalizar la implantación de la herramienta adquirida para el inventariado automático de dispositivos de usuario.

2. Finalizar la implantación de las soluciones adquiridas para restringir el acceso de dispositivos físicos no autorizados a la red corporativa.

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

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

   - La elaboración de listas de *software* autorizado (listas blancas), la implantación de las medidas técnicas que impidan la ejecución del no autorizado y la realización de revisiones periódicas del *software* instalado.
   - La definición de un plan de mantenimiento de la totalidad del *software* utilizado en el Ayuntamiento.

4. Finalizar las actuaciones iniciadas y planificadas para actualizar todos los sistemas que se encuentran fuera del periodo de soporte.

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

5. Aprobar o incluir en alguno de los procedimientos de seguridad el proceso de identificación y remediación de vulnerabilidades, incluyendo el análisis previo a la entrada en producción de los sistemas, la priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades, identificando fechas, prioridad, responsable, solución, etc.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

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

   - La eliminación de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos.

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

   - La utilización, por cada administrador de sistemas de la entidad, de diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar (gestión del dominio y servidores, administración de equipos de usuario o tareas ofimáticas no administrativas).

   - La política de autenticación a aplicar a este tipo de cuentas.

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

7. Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el principio de mínimo privilegio. Para ello, se propone el desarrollo de guías de seguridad específicas por sistemas, basadas en las recomendaciones de los fabricantes y de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN[3].

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

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

8. Aprobar formalmente un procedimiento para el tratamiento de registros de 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

[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.

logs. Para dicha revisión es aconsejable la centralización de estos en sistemas dedicados a tal efecto.

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

9. Aprobar formalmente un procedimiento para la gestión de copias de seguridad de datos y sistemas, que defina, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, la matriz de asignación de responsabilidades, el control del proceso mediante la herramienta de gestión de flujos de trabajo, las pruebas de restauración y los requisitos de protección de las copias.

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

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

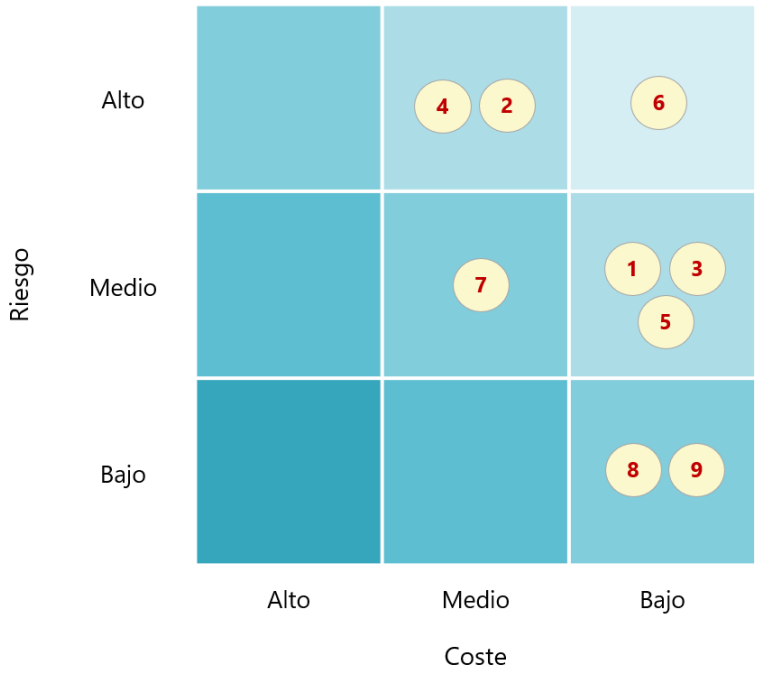
    - Actualizar y aprobar la política de seguridad para que se adapte a las nuevas circunstancias técnicas y organizativas, incluyendo la regulación de los roles de seguridad y el comité de seguridad.

    - Debe actualizarse la auditoría de seguridad y obtener y 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.

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 ha sido actualizado respecto al trabajo realizado en el año 2019, adaptando la relación riesgo/coste de cada recomendación considerando las mejoras realizadas desde la anterior revisión. No se incluye el punto 10 anterior, ya que es una medida 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 trece recomendaciones realizadas en ese informe, dos no se han atendido y ocho 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	Aprobar formalmente un procedimiento para la gestión del inventario y el control de activos físicos que recoja el proceso completo, incluyendo las revisiones periódicas de *hardware*, actualizando debidamente el inventario e incluyendo las fechas de dichas revisiones. A la hora de garantizar un nivel de actualización adecuado del inventario, es aconsejable primar el uso de herramientas para la detección y actualización automática de los elementos del sistema de información frente a procedimientos manuales.	Ha sido adquirida una herramienta que realiza el inventariado automático de todos los equipos que disponen de agente. No obstante, la herramienta no ha sido completamente desplegada y únicamente realiza la gestión de una parte de los equipos de la entidad.	**Aplicada parcialmente**	Se actualiza la redacción anterior
2	Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Se han adquirido dos herramientas, una para la gestión de dispositivos mediante conexiones inalámbricas y otra mediante conexiones cableadas. No obstante, esta última se encuentra en una fase inicial de proyecto.	**Aplicada parcialmente**	Se actualiza la redacción anterior
3	Elaborar y aprobar un procedimiento para la gestión integral del *software* de la entidad que contemple: - La elaboración de listas de *software* autorizado (listas blancas) como complemento del procedimiento existente, la implantación de las medidas técnicas que impidan la ejecución de *software* no autorizado y la realización de revisiones periódicas de *software*. - La definición de un plan de mantenimiento de la totalidad del *software* utilizado, incluyendo tanto el gestionado mediante licitaciones y cláusulas contractuales, como el resto de *software* utilizado en el Ayuntamiento.	La herramienta adquirida para el inventariado automático de equipos realiza el inventariado del *software* instalado en todos los dispositivos con agente. Esta herramienta permite la realización de revisiones periódicas de *software* para identificar la instalación de *software* no autorizado. No obstante, la herramienta no ha sido completamente desplegada y únicamente realiza la gestión de una parte de los equipos de la entidad.	**Aplicada parcialmente**	Se mantiene la redacción, ya que sigue vigente
4	Revisar y actualizar todos los sistemas que se encuentran fuera del periodo de soporte.	El Ayuntamiento ha actualizado parte de los equipos de usuario que tenían los sistemas operativos sin soporte del fabricante.	**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
5	Aprobar o incluir en alguno de los procedimientos de seguridad el proceso de identificación y remediación de vulnerabilidades, incluyendo el análisis previo a la entrada en producción de los sistemas, la priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades, identificando fechas, prioridad, responsable, solución, etc. Para la mejora de los procesos existentes de identificación de vulnerabilidades se propone el uso de herramientas de escaneo y la realización de tests de penetración.	El Ayuntamiento ha realizado el despliegue de la herramienta microCLAUDIA del CCN en los sistemas y equipos de usuario de la entidad. Además, ha adquirido una herramienta que realiza la gestión centralizada de parches y actualizaciones de todo el *software* instalado en los equipos, incluyendo sistemas operativos y aplicaciones. No obstante, la herramienta no ha sido completamente desplegada y únicamente realiza la gestión de una parte de los equipos de la entidad. Se han realizado diversos ejercicios de *hacking* ético con el objeto de evaluar el estado de seguridad de los sistemas de información.	**Aplicada parcialmente**	Se actualiza la redacción anterior
6	Ajustar la instalación de la sonda del CCN de manera que permita la identificación inequívoca del origen de los eventos de seguridad.	El Ayuntamiento ha desplegado las soluciones CARMEN y SAT-INET, que permiten identificar intentos de intrusión y realizan la detección en tiempo real de amenazas e incidentes.	**Total o sustancialmente aplicada**	Se elimina la recomendación
7	Formalizar un único procedimiento unificado de gestión de usuarios con privilegios de administración que establezca las directrices para todos los sistemas de la entidad y que incluya: - La eliminación, siempre que sea posible desde el punto de vista técnico, de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos. - Cuando existan razones de índole técnica que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas.	El Ayuntamiento ha establecido el uso de doble factor de autenticación en la herramienta de virtualización de aplicaciones. Además, existe un proyecto para el uso de doble factor de autenticación en la plataforma de acceso remoto, que se encuentra en fase de pruebas en el momento de la revisión.	**No aplicada**	Se mantiene la redacción

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
	- La utilización, para cada administrador de sistemas de la entidad, de diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar (gestión del dominio y servidores, administración de equipos de usuario o tareas ofimáticas no administrativas). - La política de autenticación a aplicar a este tipo de cuentas.			
8	Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN. Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la revisión periódica de los cambios realizados, bien mediante procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.	El Ayuntamiento ha realizado mejoras en la arquitectura de la red de datos, implementando cambios en su configuración que proporcionan significativas mejoras de rendimiento y de seguridad en las comunicaciones. Se han desarrollado nuevas guías de instalación de equipos de usuario que contemplan la aplicación de determinadas configuraciones de seguridad. El Ayuntamiento ha iniciado un proyecto para la licitación de un sistema EDR para protección de dispositivos *endpoint,* pero este proyecto se encuentra temporalmente suspendido. Se ha adquirido una herramienta para supervisar y garantizar de manera permanente la conformidad de las configuraciones de elementos críticos de la electrónica de red.	**Aplicada parcialmente**	Se mantiene la redacción
9	Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de actividad de usuario, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Para la revisión de *logs* es aconsejable la centralización de estos en sistemas dedicados a tal efecto.	El Ayuntamiento ha iniciado un proyecto, que se encuentra en fase de prueba, para la implantación de un SIEM y un centro de operaciones de seguridad.	**No aplicada**	Se mantiene la redacción

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
10	Mejorar el sistema de auditoría de los *logs* del *software* de contabilidad.	El sistema contable ha sido sustituido en el año 2022 por el nuevo sistema SEDA, de manera que la recomendación del informe anterior no es de aplicación en este informe. La Sindicatura está realizando una auditoría de seguridad específica del nuevo sistema.	Sin validez en el marco actual	Se elimina la recomendación
11	Aprobar formalmente un procedimiento para la gestión de copias de seguridad de datos y sistemas, que defina, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas de restauración y los requisitos de protección de las copias.	El Ayuntamiento ha implementado mejoras respecto a la gestión y control de las copias realizadas mediante la elaboración de una matriz de asignación de responsabilidades, y la incorporación a la herramienta corporativa para la gestión de flujos de trabajo de los distintos subprocesos y tareas del control que componen el proceso de copia. Se han automatizado, mediante la herramienta para la gestión de flujos de trabajo, las tareas de revisión y pruebas de recuperación de copias, tareas que son asignadas automáticamente a los miembros del equipo y realizadas sobre todos los tipos de copia existentes.	**Aplicada parcialmente**	Se actualiza la redacción anterior
12	Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe: - 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.	Se publicó en la sede electrónica, en el año 2019, la certificación de conformidad con el ENS para el "Sistema de información que soporta la Sede Electrónica del Ayuntamiento de València y los servicios y trámites vinculados a la misma". No obstante, la auditoría de seguridad y la certificación caducó antes del 31 de diciembre del 2021, por lo que no es considerada como válida para la valoración de control.	**Aplicada parcialmente**	Se actualiza la redacción anterior
13	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: - Finalizar la aplicación de las medidas organizativas y técnicas necesarias apropiadas para garantizar un nivel de seguridad adecuado al riesgo. - Planificar y ejecutar auditorías en materia de protección de datos.	Se ha mejorado de manera general la madurez de los procesos gestionados por la Oficina de la Delegación de Protección de Datos Personales.	**Total o sustancialmente aplicada**	Se elimina la recomendación

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.

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

- El Ayuntamiento se encuentra en trámites para la creación de una sección específica para la gestión de la seguridad integrada en el Servicio TIC. La propuesta de cambio se encuentra pendiente de aprobación por parte de la Junta de Gobierno Local y, una vez aprobada, dispondrá de dotación presupuestaria propia para el personal y proyectos específicos.

- El Ayuntamiento dispone de un Plan Director de Seguridad de los Sistemas de Información como instrumento para planificar las actuaciones en materia de seguridad TIC y contiene una relación de 26 proyectos, que han sido adecuadamente diseñados y priorizados. Algunos de los proyectos ya han sido ejecutados y el resto se encuentran pendientes de finalización o en planificación. La ejecución de la totalidad de proyectos, que ha sido acordada por la Junta de Gobierno Local, mejorará sustancialmente el nivel de seguridad del Ayuntamiento.

- El Ayuntamiento está tramitando la licitación para contratar los servicios de una oficina de ciberseguridad. Las funciones de la oficina incluyen la coordinación de la implantación de las medidas contempladas en el Plan Director, el desarrollo y cumplimiento normativo, la formación y concienciación en ciberseguridad, la constitución de un centro de operaciones de seguridad y la monitorización de sistemas, entre otros.

- El Ayuntamiento ha solicitado la adhesión a la Red Nacional de Centros de Operaciones de Ciberseguridad, iniciativa impulsada por el Centro Criptológico Nacional para integrar y coordinar los centros de operaciones de ciberseguridad del sector público y articular la colaboración y el intercambio de información ágil y efectivo entre las distintas Administraciones públicas.

- El Ayuntamiento ha adquirido, y se encuentran en fase de despliegue, dos módulos adicionales para el sistema que proporciona el servicio de directorio que realizan las siguientes funciones:

    - Gestión de inventario *software* y *hardware*, solución integrada de inventariado que permite relacionar ambos inventarios y facilita la aplicación de controles de seguridad posteriores.

- Gestión de parches y actualizaciones del *software* instalado, incluyendo sistemas operativos y aplicaciones.

- El Ayuntamiento ha adquirido dos herramientas para limitar la conexión de dispositivos no autorizados, una para la gestión de dispositivos mediante conexiones inalámbricas, que se encuentra en fase de despliegue, y otra mediante conexiones cableadas, que se encuentra en una fase inicial de proyecto.

- El Ayuntamiento ha iniciado un proyecto, que se encuentra en fase de pruebas, para la implantación de un sistema de gestión de información y eventos de seguridad (SIEM). Han sido definidos los procesos internos para la gestión de incidencias detectadas y están siendo evaluados para su implementación definitiva.

- El Ayuntamiento ha iniciado un proyecto para la licitación de un sistema EDR para protección de dispositivos *endpoint*, pero este proyecto se encuentra temporalmente suspendido por retrasos en la tramitación administrativa. Consideramos que es conveniente que se reactive lo antes posible.

El conjunto de actuaciones en marcha en materia de seguridad de los sistemas de información en el momento de finalizar el trabajo de campo de la auditoría permitirá que, una vez implantadas y debidamente gestionadas, mejore sustancialmente el nivel de ciberseguridad del Ayuntamiento de València.

APÉNDICE 1
Metodología aplicada

Introducción

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

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

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

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

Aun cuando la adopción de medidas de seguridad adecuadas hace más resilientes a las organizaciones frente a los ciberataques, el análisis de los incidentes ocurridos que se realiza en los informes INES[4] 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 València. 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 diseño[5] como sobre su eficacia operativa[6] 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, <https://www.cisecurity.org/>.

Cuadro 3. Los CBCS y el ENS

Control		Medida de seguridad del ENS*
CBCS 1	Inventario y control de dispositivos físicos	op.exp.1
CBCS 2	Inventario y control de *software* autorizado y no autorizado	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	op.acc.4 op.acc.5
CBCS 5	Configuraciones seguras del *software* y *hardware*	op.exp.2 op.exp.3
CBCS 6	Registro de la actividad de los usuarios	op.exp.8 op.exp.10
CBCS 7	Copias de seguridad de datos y sistemas	mp.info.9
CBCS 8	Cumplimiento normativo y gobernanza de la ciberseguridad	

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

Los CBCS como medidas de ciberhigiene

La European Union Agency for Cybersecurity (ENISA) señala[8] que "la ciberhigiene es un principio fundamental relativo a la seguridad de la información y, como analogía con la higiene personal, es el equivalente a establecer simples medidas rutinarias para minimizar los riesgos de las ciberamenazas. La suposición subyacente es que las buenas prácticas de ciberhigiene pueden proporcionar inmunidad en las entidades que las aplican", reduciendo los ciberriesgos[9].

Sintetizando, la ciberhigiene se refiere al conjunto de prácticas y acciones básicas que una organización debe implantar para hacer frente a los riesgos de ciberseguridad más comunes y generalizados a los que se enfrenta hoy en día[10].

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

[8] *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.

Cuadro 4. Puntos de acción de ENISA

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

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

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

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

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

Cuadro 5. Los CBCS y sus subcontroles

Control	Objetivo del control	Subcontrol	
CBCS 1 Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos *hardware* en la red, de forma que solo los dispositivos autorizados tengan acceso a la red.	CBCS 1-1: Inventario de activos físicos autorizados	La entidad dispone de un inventario de activos físicos autorizados completo, actualizado y detallado.
		CBCS 1-2: Control de activos físicos no autorizados	La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el acceso de dispositivos físicos no autorizados.
CBCS 2 Inventario y control de *software* autorizado	Gestionar activamente todo el *software* en los sistemas, de forma que solo se pueda instalar y ejecutar *software* autorizado.	CBCS 2-1: Inventario de SW autorizado	La entidad dispone de un inventario de SW completo, actualizado y detallado.
		CBCS 2-2: SW soportado por el fabricante	El SW utilizado por la entidad tiene soporte del fabricante. En caso contrario, se marca en el inventario como fuera de soporte.
		CBCS 2-3: Control de SW no autorizado	La entidad dispone de mecanismos que impiden la instalación y ejecución de SW no autorizado.
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	CBCS 3-1: Identificación de vulnerabilidades	Existe un proceso para identificar las vulnerabilidades de los componentes del sistema que asegura que estas son identificadas en tiempo oportuno.
		CBCS 3-2: Priorización	Las vulnerabilidades identificadas son analizadas y priorizadas para su resolución atendiendo al riesgo que suponen para la seguridad del sistema.
		CBCS 3-3: Resolución de vulnerabilidades	Se realiza un seguimiento de la corrección de las vulnerabilidades identificadas, de forma que se garantiza que estas son resueltas en el tiempo previsto en el procedimiento.
		CBCS 3-4: Parcheo	La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.
CBCS 4 Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	CBCS 4-1: Inventario y control de cuentas de administración	Los privilegios de administración están limitados adecuadamente y la entidad dispone de un inventario de cuentas de administración que facilita su correcto control.
		CBCS 4-2: Cambio de contraseñas por defecto	Las contraseñas por defecto de las cuentas que no se utilizan o bien son estándares se cambian antes de la entrada en producción del sistema.
		CBCS 4-3: Uso dedicado de cuentas de administración	Las cuentas de administración solo se realizan para las tareas que son estrictamente necesarias.
		CBCS 4-4: Mecanismos de autenticación	Las cuentas de administración están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.
		CBCS 4-5: Auditoría y control	El uso de las cuentas de administración está sujeto a auditoría y control de las actividades realizadas.

Control	Objetivo del control	Subcontrol	
CBCS 5 Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Establecer, implantar y gestionar la configuración de seguridad, mediante un proceso de control de cambios y gestión de la configuración riguroso, con el objetivo de prevenir ataques mediante la explotación de servicios y configuraciones vulnerables.	CBCS 5-1: Configuración segura	La entidad ha definido, documentado e implantado estándares de configuración segura para todos los sistemas operativos y SW.
		CBCS 5-2: Gestión de la configuración	La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.
CBCS 6 Registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría)	Recoger, gestionar y analizar *logs* de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	CBCS 6-1: Activación de *logs* de auditoría	El *log* de auditoría está activado en todos los sistemas y dispositivos de red y contiene el detalle suficiente para la detección, análisis, investigación y prevención de ciberataques.
		CBCS 6-2: Almacenamiento de *logs*: Retención y protección	Los *logs* se conservan durante el tiempo indicado en la política de retención, de forma que se encuentran disponibles para su consulta y análisis. Durante dicho periodo, el control de acceso garantiza que no se producen accesos no autorizados.
		CBCS 6-3: Centralización y revisión de *logs*	Los *logs* de todos los sistemas son revisados periódicamente para detectar anomalías y posibles riesgos de seguridad del sistema. Se dispone de mecanismos para la centralización de los *logs* de auditoría, de forma que se facilite su revisión.
		CBCS 6-4: Monitorización y correlación	La entidad dispone de un SIEM (*security information and event management*) o una herramienta de analítica de *logs* para realizar correlación y análisis de *logs*.
CBCS 7 Copia de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	CBCS 7-1: Realización de copias de seguridad	La entidad realiza copias de seguridad automáticas y periódicamente de todos los datos y configuraciones del sistema.
		CBCS 7-2: Realización de pruebas de recuperación	Se verifica la integridad de las copias de seguridad realizadas de forma periódica, realizando un proceso de recuperación de datos que permita comprobar que el proceso de copia de seguridad funciona adecuadamente.
		CBCS 7-3: Protección de las copias de seguridad	Las copias de seguridad se protegen adecuadamente, mediante controles de seguridad física o cifrado, mientras están almacenadas o bien son transmitidas a través de la red.
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación y tiene establecida una adecuada gobernanza de ciberseguridad.	CBCS 8-1: Cumplimiento del ENS	La entidad cumple con los requerimientos establecidos en el ENS.
		CBCS 8-2: Cumplimiento de la LOPD/RGPD	La entidad cumple con los requerimientos establecidos en la LOPD/RGPD.
		CBCS 8-3: Cumplimiento de la Ley 25/2013	La entidad cumple con los requerimientos establecidos en la Ley 25/2013, de 27 de diciembre.

Evaluación de los resultados del trabajo

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

Subcontroles

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

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

Cuadro 6. Evaluación de los subcontroles

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

Controles

Para determinar la situación global de cada control de ciberseguridad hemos utilizado el **modelo de nivel de madurez** de los procesos de control de acuerdo con lo establecido

en la GPF-OCEX 5313, que a su vez está basada en la *Guía de seguridad CCN-STIC 804* del CCN, usando una escala que se resume en el siguiente cuadro.

Cuadro 7. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El control no está siendo aplicado en este momento.
N1 Inicial / ad hoc	10	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. *La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.*
N2 Repetible, pero intuitivo	50	Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas. No hay procedimientos escritos ni actividades formativas. *La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.*
N3 Proceso definido	80	Los procesos están estandarizados, documentados y comunicados con acciones formativas. *Se dispone de un catálogo de procesos que se mantiene actualizado. Estos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).* *El éxito es algo más que buena suerte: se merece.* *Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2 y que sí se gestiona en el nivel 3.*
N4 Gestionado y medible	90	La dirección controla y mide el cumplimiento de los procedimientos y adopta medidas correctoras cuando se requiere. *Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La dirección es capaz de establecer objetivos cualitativos y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.* *En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.*
N5 Optimizado	100	Se siguen buenas prácticas en un ciclo de mejora continua. *El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras.* *Se establecen objetivos cuantitativos de mejora, y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.* *En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.*

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

Para evaluar el nivel de madurez de cada control se 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 son[11]:

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 ciberseguridad[14]. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información[15] que debe materializarse en aspectos tales como:

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

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

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

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

  La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[16], 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 València. 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 realiza actividades de control como parte de un proceso que está implantado de manera general para todos los sistemas de la entidad, aunque dicho proceso no se encuentra establecido en un procedimiento formalmente aprobado.

Hemos verificado que se han realizado determinados cambios respecto a la situación del inventario y control de dispositivos físicos que observamos en la auditoría anterior, pero parte de estos cambios estaban en implantación y no pueden considerarse totalmente efectivos para la valoración del control.

Ha sido adquirido, para el sistema que proporciona el servicio de directorio, un módulo adicional que realiza el inventariado automático de todos los elementos que disponen de agente. Esta solución integrada de inventariado permite relacionar los inventarios *software* y *hardware* de la entidad y facilita la aplicación de controles de seguridad posteriores, mejorando las capacidades de la herramienta de inventariado actualmente en uso. La instalación del agente y el inventariado de nuevos elementos se encuentran adecuadamente recogidos en las guías de instalación de nuevo equipamiento.

No obstante, nos han indicado que la nueva herramienta de inventariado, que se encuentra operativa y en producción desde el año 2021, no ha sido completamente desplegada y en el momento de la revisión únicamente realiza la gestión de una parte de los equipos de la entidad.

Además, ha sido adquirida y desplegada una herramienta para el *ticketing* y la gestión de flujos de trabajo, incluyendo la gestión de dispositivos de la entidad, y en el momento de la revisión se estaba realizando la migración de tareas desde la herramienta anterior.

En cuanto al control de dispositivos no autorizados, el Ayuntamiento dispone de una herramienta que permite la autenticación de usuarios que se conectan a la red corporativa de manera inalámbrica.

Sobre el control de dispositivos que se conectan a la red corporativa mediante conexiones cableadas, ha sido recientemente adquirida una herramienta que permitirá restringir el acceso únicamente a aquellos dispositivos que se encuentran registrados en esta. Hemos verificado que el proyecto para implantarla se encontraba en la fase inicial de ejecución.

Existe cierto nivel de control sobre el inventario y el control de activos físicos, y su valoración global alcanza un **índice de madurez del 52,5%**, 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 1 del 65,6%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 36,6%. Por tanto, se ha producido una mejora de 15,9 puntos en el índice de madurez del control.

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 determinados cambios en este control desde la revisión anterior, pero las acciones realizadas como parte del proceso de gestión del *software* no han sido establecidas en un procedimiento aprobado.

El módulo adquirido para el inventariado automático de todos los elementos gestionados por el servicio de directorio realiza el inventariado *software* de todos los dispositivos con agente, tal y como se ha indicado en el control anterior. Esta herramienta permite, adicionalmente la gestión de licencias, actualizaciones y parches, y la realización de revisiones periódicas de *software* para identificar la instalación de *software* no autorizado. No obstante, la nueva herramienta de inventariado no ha sido completamente desplegada.

Hemos verificado que se han actualizado dos terceras partes de los equipos que en la anterior auditoría estaban fuera del periodo de soporte, quedando pendiente el resto.

Además se ha planificado, como parte de las actuaciones incluidas en el Plan Director de Seguridad, la contratación del suministro de un sistema EDR para protección de dispositivos *endpoint* que limita la ejecución de *software* no autorizado. No obstante, esta iniciativa no ha sido considerada para la valoración del control, por las razones señaladas en el CBCS 5.

Existe un cierto nivel de control sobre el inventario y control de *software* autorizado, que alcanza un **índice de madurez del 62,5%**, 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 78,1%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 56,5%. Por tanto, se ha producido una leve mejora de 6 puntos en el índice de madurez del control.

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

Hemos analizado la gestión de las vulnerabilidades de los sistemas y hemos observado que han sido implantadas medidas adicionales para su identificación y resolución, pero no ha sido desarrollado, y formalmente aprobado, un procedimiento a tal efecto.

El Ayuntamiento ha realizado el despliegue de la herramienta microCLAUDIA del CCN en los sistemas y equipos de usuario de la entidad, lo que proporciona protección contra código dañino de tipo *ransomware*. Hemos verificado que la instalación se ha realizado de manera masiva y se encuentra desplegada en todos los dispositivos de usuario.

También ha desplegado las soluciones CARMEN y SAT-INET, proporcionadas por el CCN-CERT y gestionadas por el CSIRT-CV, que permiten identificar la existencia de usos indebidos o intentos de intrusión y realizan la detección en tiempo real de amenazas e incidentes existentes en el tráfico que fluye entre la red interna. Estas herramientas se encuentran plenamente operativas y se realiza la gestión de alertas suministradas por ambas sondas.

El Ayuntamiento ha adquirido, para el sistema que proporciona el servicio de directorio, un módulo adicional que realiza la gestión centralizada de parches y actualizaciones de todo el *software* instalado en los equipos gestionados, incluyendo sistemas operativos y todas las aplicaciones instaladas. No obstante, la herramienta no ha sido completamente desplegada y únicamente realiza la gestión de una parte de los equipos de la entidad.

Adicionalmente, el Ayuntamiento ha realizado diversos ejercicios de *hacking* ético con el objeto de evaluar el estado de seguridad de los sistemas de información. Además, se ha contratado y planificado la realización de diversos ejercicios de caja negra para su ejecución a lo largo de 2022.

La valoración global del control da un **índice de madurez del 67,5%**, 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 3 del 84,4%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 55,5%. Por tanto, se ha producido una mejora de 12 puntos en el índice de madurez del control.

CBCS 4. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

Objetivo del control

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

Situación del control

El Ayuntamiento no ha realizado cambios significativos en el uso controlado de privilegios administrativos respecto de la situación observada en la revisión anterior. Se realizan acciones para el control de las cuentas de administración, y si bien existen determinadas medidas adecuadas para el control de cuentas, estas no se encuentran implantadas de manera homogénea en todos los sistemas y no han sido formalmente establecidas en un procedimiento aprobado.

Únicamente se han realizado mejoras relativas a la utilización de doble factor de autenticación en determinados sistemas críticos de la entidad. Además, existe un proyecto para el uso de doble factor de autenticación en otros sistemas, que se encuentra en fase de pruebas y no está operativo en el momento de la revisión.

Hemos verificado que el Ayuntamiento no ha creado, para los usuarios administradores de los sistemas críticos de la entidad, cuentas sin privilegios de administración destinados a su uso en la operativa ordinaria, de manera que se limite el uso de las cuentas con privilegios de administración únicamente a las tareas que lo requieran. Esta carencia supone un riesgo para la entidad e incumple el principio de mínimo privilegio.

Existe un insuficiente nivel de control sobre las cuentas con privilegios administrativos y la valoración global del control supone un **índice de madurez del 47,0%**, 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 de este CBCS 4 del 58,7%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 44,6%. Por tanto, se ha producido una leve mejora de 2,4 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 exploten servicios y configuraciones vulnerables.

Situación del control

El Ayuntamiento ha realizado diversas mejoras respecto a las configuraciones seguras de *software* y *hardware* que observamos en la auditoría anterior, pero dichos cambios no han sido aplicados a todos los sistemas como parte de un proceso definido y no ha sido aprobado un procedimiento que detalle el control aplicado.

Hemos verificado que se han realizado mejoras significativas en la arquitectura de la red de datos de la entidad, manteniendo el equipamiento físico disponible, pero implementando cambios en la configuración de la red que proporcionan mejoras de rendimiento, de seguridad en las comunicaciones y posibilitan la aplicación de futuros controles adicionales.

Se han desarrollado nuevas guías de instalación de equipos de usuario que se encuentran adecuadamente detalladas y contemplan la aplicación de determinadas configuraciones de seguridad, incluyendo la gestión de actualizaciones, parches y vulnerabilidades.

Hemos verificado que el Ayuntamiento ha iniciado un proyecto para la licitación de un sistema EDR para protección de dispositivos *endpoint*. No obstante, debido a retrasos en la gestión administrativa, este proyecto se encuentra temporalmente suspendido, a la espera de la renovación del Acuerdo Marco del Sistema Estatal de Contratación Centralizada del Ministerio de Hacienda y Función Pública para formalizar la adquisición.

No se han aplicado mejoras en la configuración del resto de sistemas de la entidad, como servidores y otros sistemas críticos, que debería formar parte de un proceso sistemático formalmente aprobado.

El Ayuntamiento ha adquirido, como parte de un proyecto de renovación de elementos críticos de la electrónica de red, una herramienta que dispone, entre otras funciones, de la capacidad para supervisar y garantizar la conformidad de manera permanente de acuerdo con las políticas corporativas o la normativa de los equipos de red, pero no hemos verificado que el Ayuntamiento explote adecuadamente dicha funcionalidad.

Para el resto de los activos, el Ayuntamiento no ha implantado un proceso de gestión continua de la configuración de los sistemas, no realiza la gestión de manera manual ni dispone de las herramientas necesarias para la gestión automática de configuraciones.

La valoración global del control alcanza un **índice de madurez del 31,4%**, que se corresponde con un **nivel de madurez *N1*, *inicial/ad hoc***; es decir, existe un insuficiente nivel de control en la aplicación de configuraciones seguras en dispositivos y *software*, por lo que se deberán dedicar esfuerzos y recursos para mejorarla. Esto representa un **índice de cumplimiento del CBCS 5 del 39,2%**.

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 19 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 ha realizado determinadas mejoras respecto a la situación observada en la anterior auditoría, pero los cambios no se encuentran completamente operativos en el momento de la revisión y no ha sido aprobado un procedimiento que detalle las acciones aplicadas en el control.

El Ayuntamiento ha habilitado la recolección de *logs* en todos los sistemas críticos de la entidad y dispone de diversas herramientas, específicas para cada sistema o grupos de dispositivos, para la centralización y tratamiento de estos. Estas herramientas son adecuadamente gestionadas y explotadas por los administradores y operadores de los sistemas.

Además, desde la anterior auditoría, el Ayuntamiento ha iniciado un proyecto para la implantación de un SIEM y un centro de operaciones de seguridad. El proyecto se encontraba en fase de pruebas en el momento de realizar la auditoría y hemos verificado que el sistema SIEM recolecta registros de 4 de los sistemas críticos de la entidad. Han sido definidos los procesos internos de gestión de incidencias y eventos detectados por el sistema, que están siendo evaluados para la implementación definitiva.

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 56,5%. Por tanto, se ha producido una leve mejora de 3,5 puntos en el índice de madurez del control.

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 implementado mejoras respecto a la situación observada en la auditoría anterior sobre la gestión y control de los procesos de copia.

El Ayuntamiento dispone de dos sistemas distintos para la realización y gestión de copias de seguridad, utilizando cada uno de ellos según el sistema y tipo de copia a implementar. Las políticas de copia se encuentran definidas por el departamento TIC o por los responsables de los servicios, dependiendo del sistema a salvaguardar.

Las copias se encuentran almacenadas en ubicaciones redundantes y adicionalmente se dispone de copias en cinta para determinados sistemas, proporcionando distintos niveles de protección dependiendo del tipo de copia.

Hemos verificado que desde nuestra anterior auditoría se han implementado mejoras respecto a la gestión y control de las copias realizadas. Ha sido definida una matriz de asignación de responsabilidades, que define los responsables para la realización de copias y la revisión de estas e independiza el proceso de copia de perfiles concretos.

Además, hemos verificado que los distintos subprocesos y tareas del control han sido incluidos en la herramienta corporativa para la gestión de flujos de trabajo, lo que proporciona un nivel de madurez adicional al control y permite una gestión más eficaz por parte de los responsables de las copias.

Se han automatizado distintas tareas de revisión, incluyendo recuperaciones y comprobaciones de integridad, que son asignadas automáticamente a los miembros del equipo de trabajo y realizadas sobre todos los tipos de copia existentes, máquinas virtuales, bases de datos y almacenamiento de ficheros.

La valoración global del control existente sobre las copias de seguridad es que el Ayuntamiento alcanza un **índice de madurez del 75,0%**, 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 7 del 93,8%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 63,3%. Por tanto, se ha producido una mejora de 11,7 puntos en 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

Desde la revisión realizada en el año 2019, el Ayuntamiento ha realizado las siguientes acciones relativas al cumplimiento exigido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica:

- Se ha actualizado la categorización del sistema, según las últimas directrices de las guías del CCN.

- El Ayuntamiento realizó en 2019, tras la publicación de nuestro informe, la auditoría de seguridad prevista en el artículo 34 del Real Decreto 3/2010. No obstante, han transcurrido más de dos años desde su realización, por lo que debe realizarse nuevamente para verificar el cumplimiento de los requerimientos del ENS.

- Se publicó en la sede electrónica, en el año 2019, la certificación de conformidad y los distintivos correspondientes previstos en el ENS para el "Sistema de información que soporta la Sede Electrónica del Ayuntamiento de València y los servicios y trámites vinculados a la misma". No obstante, dicha certificación caducó antes del 31 de diciembre del 2021, por lo que no es considerada para la valoración de control.

Por otra parte, la política de seguridad de la información y la normativa relacionada se encuentran desactualizadas. El Ayuntamiento está trabajando en la licitación de un servicio de oficina de ciberseguridad, servicio que hemos verificado incluye, entre otras funciones, el desarrollo normativo requerido para alcanzar el cumplimiento de la legislación vigente.

Además, no ha sido constituido formalmente el comité de seguridad de la información, no han sido nombrados los responsables de la información y del servicio y existe una incompatibilidad en el nombramiento del responsable de seguridad, rol que es actualmente ejercido por el jefe del Servicio TIC.

Cumplimiento del RGPD

En cuanto al cumplimiento en materia de protección de datos personales, desde la revisión realizada en el año 2019 el Ayuntamiento ha realizado acciones que han mejorado el nivel de cumplimiento.

Las mejoras identificadas se basan en la aplicación de medidas organizativas y técnicas por parte de la Oficina de la Delegación de Protección de Datos Personales. Algunas de las medidas aplicadas son:

- Realización de cursos de formación obligatorios para el personal del Ayuntamiento.

- El asesoramiento a los servicios municipales y elaboración de informes se ha incrementado de manera importante en los últimos 3 años.

- Colaboración con el servicio municipal de contratación mediante la elaboración de informes cuando puede haber tratamiento de datos por terceros y estableciendo, en caso necesario, los detalles del encargo del tratamiento.

- Se ha establecido un proceso para mantener debidamente actualizado el inventario de actividades de tratamiento de datos personales, mediante el cruce de información municipal de manera continuada.

- Se ha realizado una auditoría interna por parte de la propia Oficina de la Delegación de Protección de Datos Personales.

La Oficina de la Delegación de Protección de Datos Personales del Ayuntamiento ha organizado en los años 2019 y 2022 un encuentro nacional de DPD de la Administración local, con el fin de compartir conocimiento y difundir la cultura de la protección de datos personales. Además, ha colaborado con el Comité Técnico de la Sociedad de la Información, Innovación Tecnológica y Agenda Digital de la Federación Española de Municipios y Provincias con el objeto de fomentar un modelo de autoevaluación del cumplimiento normativo.

En consecuencia, dado el grado de madurez de los procesos gestionados por la Oficina de la Delegación de Protección de Datos Personales, se dan por cumplidas las recomendaciones efectuadas en el anterior informe.

Cumplimiento de legalidad del registro de facturas

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

Indicadores

En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad incluidos en la revisión ha mejorado con respecto al informe emitido en el año 2019, alcanzando el Ayuntamiento un **índice de madurez del 70,0%**, que se corresponde con un **nivel de madurez N2**, que indica que existe un nivel razonable de adecuación a la normativa, pero hay aspectos pendientes de mejora sobre los que se debe actuar para su subsanación.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 54,8%. Por tanto, se ha producido una mejora de 15,2 puntos en el índice de madurez del control.

Gobernanza de ciberseguridad

Hemos podido verificar la existencia de un adecuado nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento, lo que, junto con la existencia de unos adecuados procesos de gestión, nos permite concluir que la gobernanza de ciberseguridad alcanza un nivel aceptable. Los aspectos fundamentales que sustentan esta afirmación son:

- La existencia de una política de seguridad de la información aprobada, que constituye el conjunto de directrices y principios que representan el compromiso de la entidad con respecto a la protección de los activos de información del Ayuntamiento. No obstante, como hemos indicado antes, debe ser actualizada.

- La existencia de un Plan Director de Ciberseguridad, que establece el conjunto de actuaciones a medio plazo, considerando prioridades en la implantación, el coste de las medidas y los indicadores para la medición del avance en la implementación. El Plan ha sido aprobado por la Junta de Gobierno Local en el año 2021.

- La existencia de una iniciativa, todavía pendiente de aprobación por la Junta de Gobierno Local, para la creación de una sección específica en el Servicio TIC para la gestión de la seguridad, dotándola de los recursos necesarios.

- La participación activa de la alta dirección, particularmente el concejal delegado, en la gestión de la seguridad de la información y en la elaboración y aprobación del Plan Director de Ciberseguridad.

- La existencia de roles clave, particularmente el responsable de seguridad y el DPD. Hemos verificado que existen y ejercen de manera efectiva y continuada las funciones establecidas.

- La existencia de una oficina de la Delegación de Protección de Datos Personales que, adicionalmente a sus atribuciones ordinarias, realiza acciones para la difusión y concienciación de la protección de datos personales en el ámbito de la Administración local.

- La realización de inversiones que permiten dar cumplimiento a los objetivos estratégicos en materia de seguridad, incluyendo el desarrollo de proyectos y la implantación de sistemas que han contribuido al establecimiento de controles técnicos, sin perjuicio de las mejoras todavía necesarias.

- La articulación de proyectos, en el contexto de utilización de los fondos Next Generation EU, que tienen como objeto promover la seguridad de la información, eliminar las carencias más relevantes identificadas y alcanzar el cumplimiento normativo.

No obstante, se han identificado carencias significativas que merman o limitan la capacidad de la organización para gestionar la seguridad, que deben subsanarse:

- La inexistencia de determinados roles clave en la organización para la gestión de la seguridad, como los responsables de la información y del servicio, y **particularmente la inexistencia de un comité de seguridad**. Hemos verificado la existencia de grupos de trabajo para la gestión de la seguridad, pero estos no estaban formalmente constituidos como comité de seguridad y además no han tenido actividad efectiva desde nuestra anterior auditoría.

- Hemos identificado una falta de agilidad administrativa en la gestión de las contrataciones que merma la capacidad de reacción y limita las oportunidades de mejora.

- Existe una incompatibilidad en el nombramiento del responsable de seguridad, dado que su figura recae sobre el jefe del Servicio TIC. El responsable de seguridad debe determinar las medidas a aplicar y el jefe del Servicio TIC debe implementarlas.

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.

Planificación estratégica de la seguridad

El Ayuntamiento ha elaborado un Plan Director de Seguridad de los Sistemas de Información como instrumento de planificación de las actuaciones horizontales en materia de seguridad TIC.

Este Plan dispone del contenido necesario, materializado en una relación de 26 proyectos. Así mismo, para cada uno de los proyectos detalla una estimación de la prioridad en la implementación, el esfuerzo humano requerido, los costes económicos, el impacto del proyecto en nivel de seguridad y su duración.

El Plan ha sido desarrollado por especialistas independientes tras la realización de un análisis diferencial, para conocer las diferencias entre el modelo de seguridad actual de la organización y el propuesto por el ENS, y un análisis de riesgos, para identificar las amenazas que pueden afectar a los activos de la entidad y la frecuencia de ocurrencia de esas amenazas.

Además, el Plan ha sido articulado de manera adecuada, elaborado por el Servicio TIC y aprobado por la Junta de Gobierno Local. Esta aprobación implica el compromiso por parte de los órganos de gobierno en la dotación de crédito adecuado y suficiente en las aplicaciones presupuestarias del Servicio de Tecnologías de la Información y Comunicación, así como la ampliación de su plantilla, para hacer posible la ejecución de todas las medidas contempladas.

Esta planificación estratégica de las actuaciones proporciona un marco de actuación a medio plazo que asegura la atención a las necesidades prioritarias con respecto a la seguridad y evita una gestión basada principalmente en la consideración de necesidades sobrevenidas.

Creación de una oficina de seguridad

El Ayuntamiento ha dispuesto la creación de una oficina de seguridad, mediante la contratación de un servicio que asumirá responsabilidades de supervisión y brindará orientación al Servicio TIC y al resto de servicios y unidades del Ayuntamiento, garantizando que los procesos de ciberseguridad estén implementados y sean operativos.

Este servicio se encuentra organizado en tres ámbitos: gobierno, centro de operaciones de seguridad y respuesta a incidentes.

Sobre el gobierno, se realizarán tareas relativas al cumplimiento normativo, gestión de riesgos, desarrollo normativo y formación en ciberseguridad.

En cuanto al centro de operaciones de seguridad, se asumirá la monitorización de sistemas y redes, el escaneo de vulnerabilidades, la gestión de parches y la realización de auditorías técnicas.

Sobre la respuesta a incidentes de ciberseguridad, la oficina identificará e informará sobre amenazas, proporcionará herramientas de análisis forense y realizará la gestión de ciberintrusiones.

En relación con el Plan Director de Seguridad de los Sistemas de Información, la oficina de seguridad coordinará la implantación de las medidas contempladas y realizará la medición

del grado de avance en la implantación del Plan, del que se dará cuanta semestralmente a la Junta de Gobierno Local.

Automatización de los procesos de gestión de copias de seguridad

El Ayuntamiento ha establecido un proceso de gestión de copias de seguridad que incluye la automatización de determinadas medidas de control, que son periódicamente asignadas de manera aleatoria a los miembros del equipo.

La creación de las tareas es realizada mediante un *script* de la herramienta de gestión de flujos de trabajo, que realiza consultas a los sistemas de la entidad para identificar las copias existentes y genera tareas para la realización de distintas tareas de revisión sobre copias seleccionadas de manera aleatoria.

Las tareas de revisión incluyen distintos tipos de comprobaciones, incluyendo recuperaciones y comprobaciones de integridad, y son realizadas sobre todos los tipos de copia existentes, máquinas virtuales, bases de datos y almacenamiento de ficheros.

Esta gestión, controlada mediante la herramienta de gestión de flujos de trabajo y automatizada mediante *scripts*, proporciona un nivel de madurez adicional, independizando las tareas de miembros concretos del equipo, estandarizando los trabajos a realizar y estableciendo indicadores que permiten la medición del desempeño del control.

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.

EDR[17]: Un sistema EDR, acrónimo en inglés de *endpoint and 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

[17] *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 Comunitat 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 concejal delegado de Agenda Digital y Administración Electrónica, el secretario municipal del Área II y el jefe del Servicio de Tecnologías de la Información y Comunicaciones, 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 fiscalización correspondiente a 2021, este se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Dentro del plazo concedido, el Ayuntamiento ha formulado las alegaciones que ha considerado pertinentes.

En relación con el contenido de las alegaciones y su tratamiento, es preciso señalar lo siguiente:

1. Todas las alegaciones han sido analizadas detenidamente.

2. Las alegaciones admitidas se han incorporado al contenido del Informe.

El texto de las alegaciones formuladas, así como el informe motivado que se ha emitido sobre estas que ha servido de antecedente para su estimación o desestimación por esta Sindicatura se incorporan en los anexos I y II.

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 15 de diciembre de 2022, aprobó este informe de auditoría.

ANEXO I

Alegaciones presentadas

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

C/ Sant Vicent, 4 - 46002
Tel. +34 96 386 93 00
Fax +34 96 386 96 53
sindicom@gva.es
www.sindicom.gva.es

JUSTIFICANTE DE PRESENTACIÓN EN REGISTRO ELECTRÓNICO

NÚMERO DE REGISTRO 202205371	FECHA DE ENTRADA 07/12/2022 9:12
ÁREA Fiscalización - Alegaciones	PROCEDIMIENTO PAA2020/35 Seguimiento de las 11 auditorías de los controles básicos de ciberseguridad cuyo trabajo de campo se ha realizado en 2019 (una vez transcurrido un año desde su finalización)
DATOS DEL PRESENTADOR Nombre: VICENTE RODRIGO INGRESA NIF / CIF: E-mail: Entidad: VALÈNCIA	
FIRMA DIGITAL 61DEA66A52010738C81DE44998E05480BF04525B	
DOCUMENTOS ENVIADOS Fichero1: 79140179P_2022127_20221207 Informe alegaciones.pdf	

SINDICATURA DE COMPTES

Al·legacions que es formulen a l'esborrany de l'Informe de seguiment de les recomanacions realitzades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019. Situació a 31 de desembre de 2021.

Primera al·legació.

Apartat "CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS" de l'esborrany de l'Informe, pàgina 37.

Contingut de l'al·legació:

De la lectura de este apartado se puede dar a entender que el ayuntamiento no dispone de una herramienta de control de inventario de equipos cuando esto no es realmente cierto. El ayuntamiento dispone de una herramienta de control de inventario de equipos que lleva varios años en producción y que llamamos SGI, y es la misma herramienta con la que gestionamos el *ticketing*. Recientemente, se ha adquirido un nuevo software, que debe sustituir al anterior y que tiene mejores prestaciones, pero este nuevo software todavía no se ha terminado de implantar.

Documentació justificativa de l'al·legació:

Se adjuntan algunas capturas de pantalla de la herramienta actual en la que se puede ver el resultado de la búsqueda y consulta de los datos inventariados de un PC:

Las imágenes han sido eliminadas por razones de seguridad

[redacted]

[redacted]

Segona al·legació.

Apartat "CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS" de l'esborrany de l'Informe, pàgina 37, paràgraf penúltim.

Contingut de l'al·legació:

El párrafo siguiente: "*En cuanto al control de dispositivos no autorizados, el Ayuntamiento dispone de una herramienta que permite la autenticación de usuarios que se conectan a la red corporativa de manera inalámbrica, pero no ha sido desplegada completamente y no se encontraba en operación en el momento de la revisión.*" alegar que sí que está desplegada completamente, de forma que todos los usuarios que se conectan a la wifi corporativa lo hacen con usuario y contraseña. Es decir, no es posible que un usuario se conecte a la wifi corporativa sin introducir ni usuario ni contraseña.

Documentació justificativa de l'al·legació:

Se adjuntan capturas de pantalla con el procedimiento de registro que cada usuario debe hacer, en la intranet municipal, antes de que pueda conectarse a la wifi corporativa:

[redacted]

[redacted]

Tercera al·legació

Apartat "Sobre el inventario y control de software autorizado (CBCS 2)" de l'esborrany de l'Informe, pàgina 9

Contingut de l'al·legació:

Los usuarios de los pc's del ayuntamiento no disponen de privilegios de administración, y por lo tanto, no pueden instalarse una aplicación sin intervención de un técnico del Servicio de Tecnologías de la Información y la Comunicación (SerTIC).

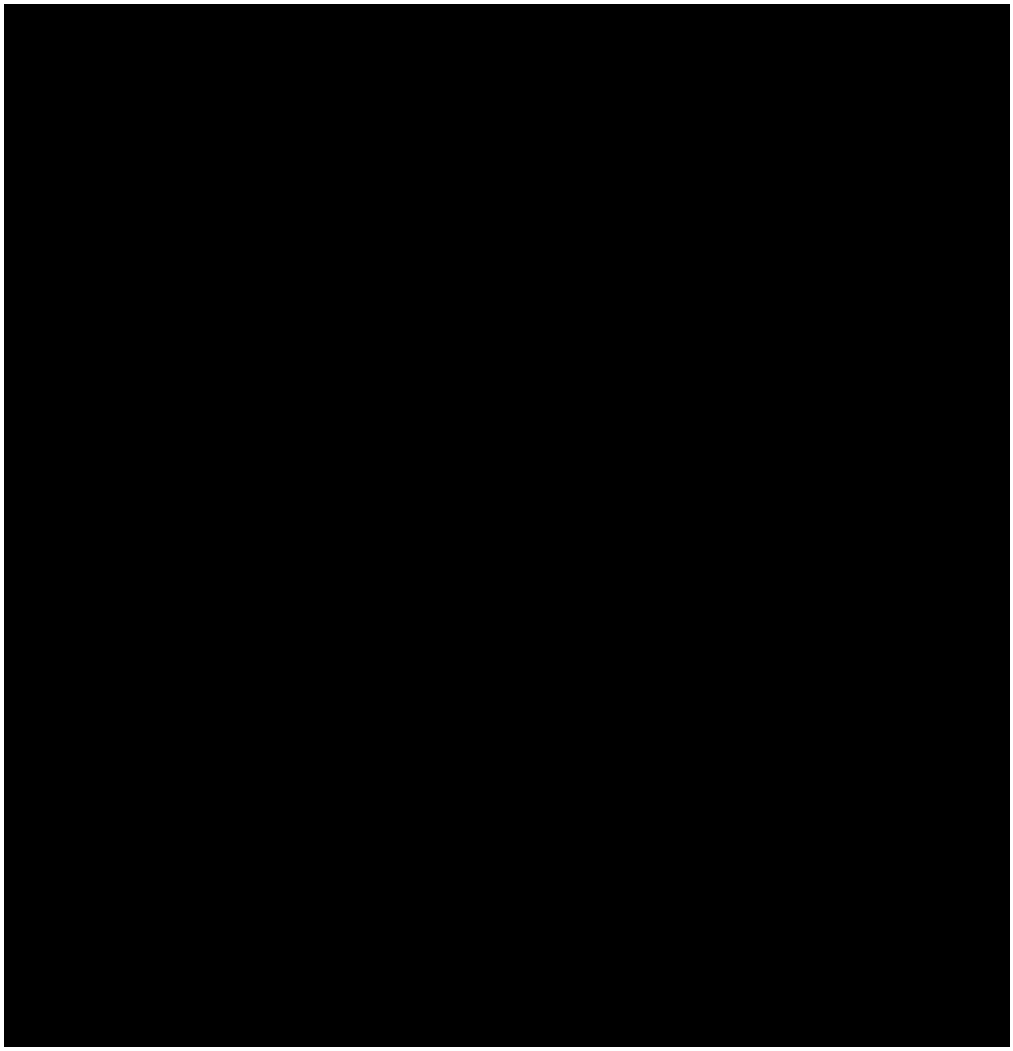
Además, existe un sistema automatizado para la distribución de aplicaciones (ZENworks) y también de actualizaciones y parches en los equipos de usuario.

Documentació justificativa de l'al·legació:

Se adjunta captura de pantalla de un ejemplo de usuario con la lista de aplicaciones autorizadas y que se distribuyen automáticamente en el primer inicio:

Aquí se distinguen entre las aplicaciones que se distribuyen para todos los usuarios del ayuntamiento (“Aplic. Ayuntamiento”), las que solo se distribuyen a usuarios concretos (“Aplic. Específicas”) o las que se distribuyen a los usuarios de un servicio del ayuntamiento (“Aplic. Servicio”). El grupo de aplicaciones “Soporte” está restringido a usuarios del SerTIC.

Se adjunta también captura de pantalla de la herramienta donde se configuran los parches y actualizaciones que deben distribuirse:



Cuarta al·legació

Apartat "Sobre el uso controlado de privilegios administrativos (CBCS 4)" de l'esborrany de l'Informe, pàgina 10

Contingut de l'al·legació:

Los usuarios de los pc's del ayuntamiento no disponen de privilegios de administración, y por lo tanto, no pueden instalarse una aplicación sin intervención de un técnico del SerTIC. Esto se configura de manera centralizada mediante ZENworks y las políticas de Windows.

Documentació justificativa de l'al·legació:

Se adjunta captura de pantalla de las políticas de Windows de un usuario ejemplo gestionadas desde ZENworks:

Quinta al·legació

Apartat "Actuaciones en curso" de l'esborrany de l'Informe, pàgina 17

Contingut de l'al·legació:

Dado que el informe se ha elaborado con datos a 31 de diciembre de 2021, destacar que la Junta de Gobierno Local aprobó el 23/12/2021 el Plan Director de Ciberseguridad.

Aunque las medidas de dicho plan han comenzado a aplicarse durante el 2022, sí que nos gustaría que figurase de manera más destacada en el apartado "4. CONCLUSIONES", que el ayuntamiento aprobó el 23/12/2021 dicho plan.

Documentació justificativa de l'al·legació:

Ya se aportó acta de la Junta de Gobierno Local de 23/12/2021, pero puede localizarse la misma en la web municipal https://www.valencia.es en la siguiente ruta:

"*Ayuntamiento*", "*Actividad Órganos de Gobierno*", "*Junta de Gobierno Local*", "*2021*", "*23 de Diciembre de 2021 (Ordinaria)*"

(no se puede adjuntar enlace directo porque es dinámico)

ANEXO II

Informe sobre las alegaciones presentadas

ANÁLISIS DE LAS ALEGACIONES EFECTUADAS POR EL AYUNTAMIENTO DE VALÈNCIA AL BORRADOR DEL INFORME DE SEGUIMIENTO DE LAS RECOMENDACIONES REALIZADAS EN EL INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE VALÈNCIA DEL AÑO 2019

Mediante el escrito de esta Sindicatura de 25 de noviembre de 2022 se remitió al Ayuntamiento de València el borrador del Informe de auditoría, para que efectuase las alegaciones que considerase oportunas. Con fecha 7 de diciembre de 2022 se recibieron por el registro electrónico las alegaciones formuladas y respecto a estas se señala lo siguiente:

Primera alegación

Apartado "CBCS 1. Inventario y control de dispositivos físicos" del borrador del Informe, apéndice 2

Comentaris

La alegación indica que de la lectura del Informe se puede entender que el Ayuntamiento no dispone de una herramienta de control de inventario de equipos, pero en realidad sí existe una herramienta que se encuentra en producción.

El apartado detalla principalmente las novedades identificadas en los controles, por lo que no se ha incluido referencia expresa a la herramienta existente, pero sí a la adquisición de un nuevo *software* que mejora las prestaciones de la herramienta actual.

No obstante, se acepta la alegación y se matiza la redacción del apartado incluyendo una referencia a la herramienta actualmente en uso.

Consecuencias en el Informe

Modificar el párrafo 4 del apartado "CBCS 1. Inventario y control de dispositivos físicos" del apéndice 2 y dejarlo redactado como sigue:

> "Ha sido adquirido, para el sistema que proporciona el servicio de directorio, un módulo adicional que realiza el inventariado automático de todos los elementos que disponen de agente. Esta solución integrada de inventariado permite relacionar los inventarios *software* y *hardware* de la entidad y facilita la aplicación de controles de seguridad posteriores, mejorando las capacidades de la herramienta de inventariado actualmente en uso. La instalación del agente y el inventariado de nuevos elementos se encuentran adecuadamente recogidos en las guías de instalación de nuevo equipamiento."

Segunda alegación

Apartado "CBCS 1. Inventario y control de dispositivos físicos" del borrador del Informe, apéndice 2

Comentarios

La alegación indica que la herramienta para autenticación de usuarios que se conectan a la red corporativa de manera inalámbrica sí está desplegada completamente.

Durante la visita para la revisión de controles, se nos indicó que la solución de autenticación para dispositivos inalámbricos, basada en el uso de protocolo 802.1x, no se encontraba operativa, aunque la adquisición de las licencias necesarias se había producido dentro del periodo de revisión. En la alegación no se incluye el detalle suficiente como para confirmar que la solución se encontraba plenamente funcional a fecha de 31 de diciembre de 2021.

Verificada la información recibida, se acepta parcialmente la alegación, se matiza la redacción del apartado, pero se mantiene la valoración del control.

Consecuencias en el Informe

Modificar el párrafo 6 del apartado "CBCS 1. Inventario y control de dispositivos físicos" del apéndice 2 y dejarlo redactado como sigue:

> "En cuanto al control de dispositivos no autorizados, el Ayuntamiento dispone de una herramienta que permite la autenticación de usuarios que se conectan a la red corporativa de manera inalámbrica."

Modificar el "Cuadro 2. Seguimiento de recomendaciones", segunda recomendación, "Situación a 31 de diciembre de 2021 respecto al informe anterior" y dejarlo redactado como sigue:

> "Se han adquirido dos herramientas, una para la gestión de dispositivos mediante conexiones inalámbricas y otra mediante conexiones cableadas. No obstante, esta última se encuentra en una fase inicial de proyecto."

Tercera alegación

Apartado 5, "Recomendaciones y medidas necesarias para el cumplimiento de la legalidad", subapartado "Sobre el inventario y control de software autorizado (CBCS 2)" del borrador del Informe

Comentarios

La alegación indica que los usuarios del Ayuntamiento no pueden instalar aplicaciones sin intervención de un técnico del SerTIC, dado que no disponen de privilegios de administración.

Durante la realización del trabajo pudimos verificar la existencia de las medidas de control que se detallan en la alegación. No obstante, la recomendación expresa la necesidad de elaborar y aprobar un procedimiento que detalle y formalice, entre otros aspectos, la explotación de estas medidas que ya se encuentran implantadas.

Además, la alegación indica que existe un sistema automatizado para la distribución de aplicaciones y también de actualizaciones y parches en los equipos de usuario.

La existencia de estas herramientas se encuentra recogida en el apartado correspondiente del apéndice 2. No obstante y como hemos indicado, la recomendación expresa la necesidad de que el procedimiento, que debe ser elaborado y aprobado, detalle la explotación de estas medidas existentes.

No afecta a nuestra conclusión.

Consecuencias en el Informe

Mantener la redacción del Informe.

Cuarta alegación

Apartado 5, "Recomendaciones y medidas necesarias para el cumplimiento de la legalidad", subapartado "Sobre el uso controlado de privilegios administrativos (CBCS 4)" del borrador del Informe,

Comentarios

La alegación indica que los usuarios del Ayuntamiento no pueden instalar aplicaciones sin intervención de un técnico del SerTIC, dado que no disponen de privilegios de administración.

Tal y como se indica en el punto anterior, durante la realización del trabajo pudimos verificar la existencia de las medidas de control relativas a la gestión de privilegios. No obstante, las recomendaciones expresan la necesidad de elaborar y aprobar procedimientos que detallen y formalicen la explotación de medidas que ya se encuentran implantadas.

No afecta a nuestra conclusión.

Consecuencias en el Informe

Mantener la redacción del Informe.

Quinta alegación

Apartado 5, "Recomendaciones y medidas necesarias para el cumplimiento de la legalidad", subapartado "Actuaciones en curso" del borrador del Informe

Comentarios

La alegación indica que el Plan Director de Ciberseguridad fue aprobado por la Junta de Gobierno Local el 23 de diciembre de 2021, dentro del periodo de revisión del informe. Y se solicita que figure de manera más destacada en el apartado 4, "Conclusiones", la fecha de aprobación de dicho plan.

El informe detalla el año de aprobación del Plan Director de Ciberseguridad en el párrafo 3 del subapartado "Gobernanza de la ciberseguridad" del apéndice 2.

No obstante, se acepta la alegación y se modifica la redacción de las conclusiones del Informe para que refleje ese dato.

Consecuencias en el Informe

Modificar la redacción del párrafo quinto de la conclusión sobre la gobernanza del Apartado "4. Conclusiones":

> "Existen proyectos e iniciativas que se encuentran en fase de ejecución o de planificación que, en caso de ser finalizados y gestionados de manera efectiva, tendrán un impacto positivo desde el punto de vista operativo y de la seguridad. Además, existe una planificación estratégica de la seguridad de la información que ha sido materializada en el Plan Director de Seguridad de los Sistemas de Información, aprobado por la Junta de Gobierno el 23 de diciembre del año 2021, que orienta de forma coherente las acciones en esta materia."

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe seguimiento recomanendaciones CBCS Ayuntamiento València 2019_cas - SEFYCU 3745176

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 3CV3 RUC4 FE7C D4JE

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 - 29/12/2022 8:08 VICENT CUCARELLA TORMO