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 SAGUNTO DEL AÑO 2019

Situación a 31 de diciembre de 2021

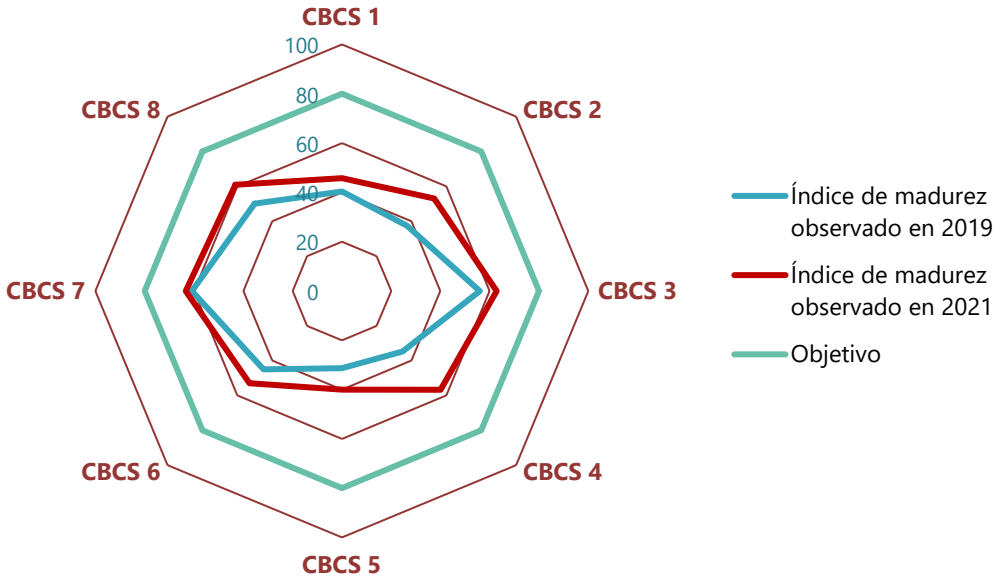
RESUMEN

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 Sagunto respecto a la situación mostrada en la auditoría del año 2019.

Conclusiones

Aunque se han realizado progresos desde nuestra anterior auditoría y se han atendido parcialmente algunas de nuestras recomendaciones, el índice de madurez general de los controles básicos de ciberseguridad, cuyo objetivo sería alcanzar un 80% , muestra un valor del 54,4% (44,5% en 2019), por lo que el nivel de efectividad en los controles analizados sigue 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 de Sagunto no tiene establecida una adecuada gobernanza de la ciberseguridad, situación que debe ser subsanada. Los órganos de gobierno deben aprobar normas y procedimientos en relación con la seguridad de la información aplicables a toda la organización por igual.

La política de seguridad del Ayuntamiento debe ser actualizada y los roles definidos en esta deben ejercer sus funciones de manera efectiva. Es preciso que el comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad, se reúna regularmente, con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna.

Asimismo, nuestra revisión también ha puesto de manifiesto un grado de cumplimiento insuficiente en cuanto a la adecuación a las normas legales relacionadas con la seguridad de la información. El informe señala diversos aspectos sobre los que se debe actuar para su pronta subsanación.

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, además de aprobar formalmente procedimientos que describan las acciones y controles implantados, recomendamos la implantación de soluciones para restringir el acceso de dispositivos físicos no autorizados a la red corporativa, actualizar los sistemas obsoletos, extender el uso de la herramienta de gestión de vulnerabilidades, parches y actualizaciones a todos los equipos de la entidad y aplicar a los administradores de sistemas el criterio de mínima funcionalidad.

NOTA

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

Informe de seguimiento de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Sagunto 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 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 ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes y el 5 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 Sagunto, 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.

La experiencia sufrida por el Ayuntamiento en 2021, que se menciona en el siguiente apartado, es un claro exponente de la necesidad de reforzar los controles de seguridad en todas las instituciones públicas y alcanzar el nivel de madurez exigido por el ENS.

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

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

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

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

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

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.

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.

Para ello, hemos llevado a cabo el trabajo de conformidad con los *Principios fundamentales de fiscalización de las instituciones públicas de control externo* y con las normas técnicas de fiscalización aprobadas por el Consell de la Sindicatura recogidas en el *Manual de fiscalización* de la Sindicatura de Comptes. Dichos principios exigen que cumplamos los requerimientos de ética, así como que planifiquemos y ejecutemos la auditoría con el fin de obtener una seguridad limitada sobre la situación de los CBCS revisados.

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

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

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

4. CONCLUSIONES

Aunque se han realizado progresos desde nuestra anterior auditoría y se han atendido parcialmente nuestras recomendaciones, el índice de madurez general de los controles básicos de ciberseguridad es insuficiente y debe mejorar para alcanzar los niveles exigidos por el ENS

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el **índice de madurez general** en la gestión de los controles básicos de ciberseguridad alcanza un **54,4%**, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente.

Aunque el Ayuntamiento ha atendido de forma parcial nuestras recomendaciones y el índice de madurez general ha mejorado desde el 44,5% de nuestra auditoría de 2019, el índice de madurez actual sigue siendo insuficiente para garantizar un adecuado grado de seguridad y alcanzar el 80% requerido por el ENS. La comparación de los resultados detallados con los obtenidos en el año 2019 muestra una mejora en todos los controles, si bien la mejora ha sido insuficiente y ninguno alcanza el objetivo del 80%, dado el bajo grado de atención a algunas de nuestras recomendaciones (véase apartado 5 siguiente).

Existen claras posibilidades de mejora para alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información, particularmente sobre aquellos controles que presentan deficiencias significativas y no llegan al nivel de madurez N2 (CBCS 1 y CBCS 5). En el apartado 5 se realizan las recomendaciones pertinentes con esa finalidad.

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

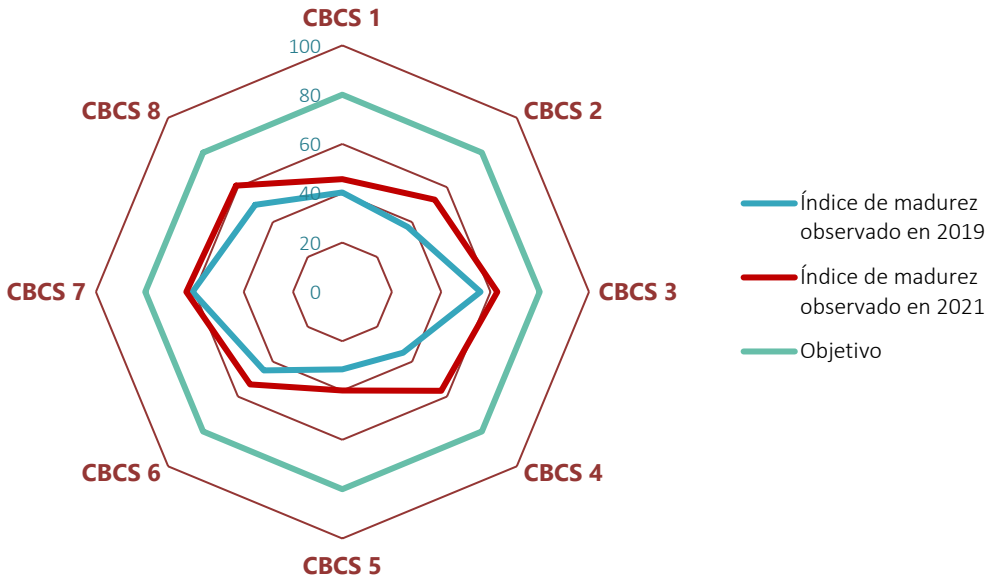
Cuadro 1. Índice de madurez de los controles básicos de ciberseguridad

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	*40,4%*	***N1***	*50,4%*	45,8%	**N1**	57,2%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	*37,4%*	***N1***	*46,8%*	53,0%	**N2**	66,3%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	*56,0%*	***N2***	*70,0%*	62,8%	**N2**	78,5%
CBCS 4 Uso controlado de privilegios administrativos	*34,8%*	***N1***	*43,5%*	56,7%	**N2**	70,9%
CBCS 5 Configuraciones seguras del *software* y *hardware*	*31,4%*	***N1***	*39,2%*	40,0%	**N1**	50,0%
CBCS 6 Registro de la actividad de los usuarios	*45,0%*	***N1***	*56,3%*	53,0%	**N2**	66,3%
CBCS 7 Copias de seguridad de datos y sistemas	*60,8%*	***N2***	*76,0%*	63,3%	**N2**	79,2%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	*50,0%*	***N2***	*62,5%*	61,0%	**N2**	76,3%
General	**44,5%**	***N1***	**55,6%**	**54,4%**	**N2**	**68,1%**

El índice de cumplimiento de los CBCS es del 68,1%, 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 55,6% de nuestro anterior informe y la comparación de los resultados detallados del presente trabajo con los obtenidos en el año 2019 muestra una ligera mejoría en todos los controles.

De una forma más sintética y gráfica, la situación observada de los controles, tanto en la presente auditoría como en la realizada en el año 2019, queda reflejada en el gráfico 1.

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 Sagunto no tiene establecida una adecuada gobernanza de la ciberseguridad, situación que debe ser subsanada. Además, se debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información

Los órganos superiores del Ayuntamiento (en particular el alcalde y la Junta de Gobierno) son los responsables de que existan unos controles 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.

Si bien hemos podido verificar la existencia de cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento y

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

particularmente de los responsables de las áreas implicadas, existen carencias relevantes que impiden que la gobernanza pueda considerarse efectiva:

- La falta de actividad del Comité de Seguridad, órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas del Ayuntamiento y de los roles clave, particularmente el responsable de seguridad, cuyas responsabilidades se encuentran detalladas y asignadas en la política de seguridad, pero no son ejercidas de manera efectiva.

- La falta de recursos suficientes, tanto económicos como de personal, en el departamento TIC para atender la problemática de la seguridad de la información.

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

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

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

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

Para subsanar las deficiencias de control identificadas por la Sindicatura en la presente auditoría y mejorar los niveles de control señalados en el apartado 4 anterior, reformulamos las recomendaciones que se efectuaron en la auditoría de 2019, considerando 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 actualmente implantado, incluyendo las revisiones periódicas de *hardware*, actualización del inventario e incluyendo la periodicidad de dichas revisiones.

2. Mejorar los controles que permiten 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* que contemple las acciones actualmente implantadas.

4. Revisar y actualizar los sistemas que todavía se encuentran fuera del período de soporte, especialmente aquellos ligados a procesos críticos de la entidad.

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

5. Aprobar formalmente un procedimiento que describa las acciones llevadas a cabo para la gestión de vulnerabilidades, desde la identificación hasta su remediación, y que considere, además de las acciones ya establecidas, el escaneo mediante herramientas específicas, 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 tratadas.

6. Hacer extensivo a toda la organización el uso de la herramienta implantada para la gestión unificada y automatizada de parches de seguridad y actualizaciones.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

7. Aprobar un procedimiento que incluya la gestión de usuarios con privilegios de administración que aplique las mismas directrices para todos los sistemas de la entidad y que establezca, además de las prácticas que ya se llevan a cabo en este control, la utilización, por cada administrador de sistemas de la entidad, de diferentes cuentas con distintos niveles de privilegios dependiendo de las tareas a realizar.

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

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, 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.

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

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

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

10. Actualizar y aprobar formalmente el procedimiento de copias de seguridad, que describa el conjunto de medidas implantadas y detalle los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas planificadas de restauración y los requisitos de protección de las copias.

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

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

    - Cumplimentar la Instrucción Técnica de Seguridad del Informe del Estado de la Seguridad, de la Secretaría de Estado de Administraciones Públicas (Informe INES).
    - Realizar las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010.
    - Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS del 13 de octubre de 2016.

12. En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular debe:

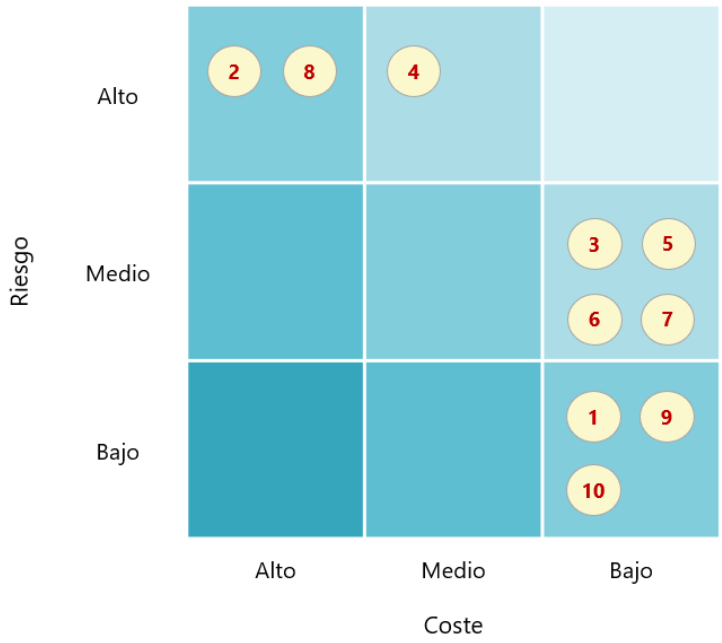
    - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD.
    - Planificar y ejecutar auditorías en materia de protección de datos.

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 y considerando las mejoras realizadas desde la anterior revisión. No se incluyen los puntos 11 y 12 anteriores, ya que son medidas de obligado cumplimiento.

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



Seguimiento de recomendaciones anteriores

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

Tal como se muestra en el cuadro 2, de las trece recomendaciones realizadas en ese informe, una ha sido atendida, ocho lo han sido parcialmente y cuatro no se han atendido.

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 actualmente implantado, incluyendo las revisiones periódicas de *hardware*, actualizando debidamente el inventario e incluyendo la periodicidad de dichas revisiones.	El Ayuntamiento no ha aprobado un procedimiento a tal efecto. Aunque se han realizado algunas acciones relacionadas con este control, como la actualización del *software* que gestiona el inventario de dispositivos físicos y la incorporación de algunos edificios a la red corporativa, dichas acciones no atienden lo esencial de nuestra recomendación.	**No aplicada**	Se mantiene la redacción dada en 2019.
2	Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	El departamento de informática ha trabajado en la desconexión de tomas de red de las zonas públicas o comunes; sin embargo, no existe un mecanismo robusto de control en este aspecto. También se ha implantado una solución para el bastionado de los equipos de usuario atendiendo a criterios de seguridad de los *endpoints*. Las medidas implantadas para este control no han sido formalizadas en un procedimiento aprobado.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
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) y la realización de revisiones periódicas de *software*. - La implantación de las medidas técnicas que impidan la instalación y ejecución del software no autorizado. - 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.	El Ayuntamiento ha implantado determinadas medidas para subsanar las deficiencias detectadas, como la eliminación de los usuarios administradores de los equipos cliente o el bloqueo de aplicaciones en el perímetro de la red. No obstante, las medidas implantadas no han sido recogidas en un procedimiento aprobado formalmente.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
4	Revisar y actualizar todos los sistemas que se encuentran fuera del período de soporte.	Aunque se han actualizado gran parte de los sistemas que se encontraban fuera del periodo de soporte, siguen existiendo sistemas críticos obsoletos. Esto supone una deficiencia grave que afecta a todo el sistema de información.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el Informe
5	Aprobar un procedimiento de identificación y remediación de vulnerabilidades que formalice y amplíe el proceso actual, que aplique de forma integral a la totalidad de sistemas del Ayuntamiento y que considere, como mínimo, los siguientes aspectos: - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas, el análisis previo a la entrada en producción de los sistemas y las acciones actualmente establecidas de seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad. - La priorización actualmente implantada basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.	El Ayuntamiento ha desplegado el sistema microCLAUDIA para la provisión de vacunas frente a código dañino de tipo *ransomware*, y la herramienta CARMEN, que monitoriza los flujos de datos para la identificación de amenazas persistentes avanzadas. El departamento TIC ha desplegado un sistema EDR que identifica vulnerabilidades en los equipos con agente de red instalado, aunque en el momento de la revisión únicamente se dispone de 100 licencias de prueba. Se ha implantado una herramienta de cibervigilancia que proporciona múltiples servicios, entre los que se encuentra la gestión de vulnerabilidades y parches o la monitorización de filtraciones de datos.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
6	Utilizar herramientas que permitan la gestión unificada y automatizada de parches de seguridad y otras actualizaciones.	Aunque se ha implantado un sistema EDR que realiza la gestión de parches y actualizaciones, en el momento de la revisión únicamente disponía de 100 licencias de prueba.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
7	Aprobar 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. - 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.	El departamento ha eliminado los permisos de administración para los usuarios que no requieren dichos privilegios, han solucionado la incidencia detectada en la aplicación de gestión tributaria y fortalecido la política de contraseñas. No obstante, existen posibilidades de mejora para alcanzar el nivel exigido por el ENS, como la utilización de distintos niveles de privilegios por parte de los administradores, que las acciones llevadas a cabo sean extendidas a todos los sistemas o la aprobación de una política de gestión de usuarios administradores que detalle dichas acciones.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el Informe
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 y que sea aplicado a la totalidad de los sistemas del Ayuntamiento. 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 (como ya se está haciendo para un subconjunto de los activos de la entidad). 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.	Aunque se han realizado acciones relacionadas con la configuración segura de sistemas –como el control de acceso de equipos en el *firewall* o la exigencia de las certificaciones del ENS en las soluciones y empresas contratadas–, el Ayuntamiento no dispone de un procedimiento aprobado por la corporación que describa la gestión de configuraciones y cambios en los sistemas críticos de la entidad.	**Aplicada parcialmente**	Se mantiene la redacción.
9	Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de la actividad de los usuarios, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, la gestión de derechos de acceso al registro 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 servicio de directorio de usuarios en la nube cuenta con un sistema de registro de acciones de los usuarios. El Ayuntamiento ha implantado herramientas ofrecidas por el CSIRT-CV y CCN-CERT que alertan de las anomalías detectadas en la red corporativa. Además, está en fase de integración con el vSOC del CSIRT-CV. No obstante, no se dispone de un procedimiento que describa el tratamiento de *logs* de auditoría que incluya los aspectos necesarios.	**No aplicada**	Se mantiene la redacción.
10	Actualizar y aprobar formalmente el procedimiento existente para la gestión de las copias de seguridad de datos y sistemas, que defina, como mínimo, los datos y los sistemas afectados, la periodicidad de las copias, las ubicaciones, los responsables, las pruebas de restauración y los requisitos de protección de las copias.	El departamento ha mejorado el sistema de copias mediante la adquisición de un nuevo *hardware* y la contratación de servicios en la nube. Sin embargo, no se realizan pruebas de restauración planificadas de los sistemas críticos ni el procedimiento está aprobado por la dirección.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el Informe
11	Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe: - Cumplimentar la Instrucción Técnica de Seguridad del Informe del Estado de la Seguridad, de la Secretaría de Estado de Administraciones Públicas (Informe INES). - Realizar las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010. - Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS del 13 de octubre de 2016.	Sin variación en 2021.	**No aplicada**	Se mantiene la redacción.
12	En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular debe: - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD. - Planificar y ejecutar auditorías de cumplimiento en materia de protección de datos.	Sin variación en 2021.	**No aplicada**	Se mantiene la redacción.
13	Llevar a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.	Se ha realizado la auditoría del registro de facturas del ejercicio 2021.	**Aplicada**	Se elimina la recomendación dada en 2019.

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. La implantación efectiva de estas actuaciones tendrá un impacto positivo en el nivel de ciberseguridad de la entidad.

Enumeramos a continuación aquellas actuaciones que se encuentran planificadas o en ejecución y que por su relevancia deben ser destacadas:

- La herramienta EDR utilizada para la gestión de parches y actualizaciones está en fase de licitación. Durante el trabajo de revisión únicamente se disponía de 100 licencias de prueba. Esta herramienta mejorará varios de los controles de seguridad analizados.

- El Ayuntamiento está en fase de licitación de un proyecto para la adecuación y cumplimiento del nuevo ENS, proyecto subvencionado con los fondos Next Generation EU, en el que se incluirá la elaboración y aprobación de procedimientos de control sobre los distintos sistemas de información.

- Despliegue de servicios y herramientas proporcionados por el CSIRT-CV, como parte del Plan de Choque de Ciberseguridad para las entidades locales de la Comunitat Valenciana. Tiene previsto el despliegue de:

    - CARMEN, solución desarrollada con el objetivo de identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas (APT).

    - LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas), herramienta para la gestión de ciberincidentes.

    - SAT-INET (Sistema de Alerta Temprana de Internet), servicio desarrollado e implantado por el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes.

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[3] 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.

[3] 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 Sagunto. Ejercicio 2019, así como obtener una seguridad limitada y concluir sobre la situación de los controles básicos de ciberseguridad revisados. Para ello hemos evaluado tanto su diseño[4] como su eficacia operativa[5] para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte. También hemos revisado el cumplimiento de la normativa básica relativa a la seguridad de la información.

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

La presente auditoría se ha centrado en el análisis de la situación actualizada de los ocho CBCS revisados en la auditoría del año 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

[4] 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.

[5] 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)[6], 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:

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

Cuadro 3. Los CBCS y el ENS

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

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

Los CBCS como medidas de ciberhigiene

La European Union Agency for Cybersecurity (ENISA) señala[7] 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[8].

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[9].

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.

[8] 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.

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

Controles

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

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

Cuadro 7. Niveles de madurez

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

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

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

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

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

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

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

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

Confidencialidad	Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Integridad	Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.
Disponibilidad	Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.

Autenticidad	Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Trazabilidad	Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

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

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

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

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

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

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

De acuerdo con la categoría de cada sistema, los niveles mínimos de exigencia o de madurez requeridos son[10]:

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%.

[10] *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.[11]

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**[12].

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

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

[12] 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[13]. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información[14] 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[15], 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.

[13] *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.

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

[15] *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 Sagunto. Ejercicio 2019.

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

Cuadro 8. Situación de las recomendaciones

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

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

Comunicación y confidencialidad

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

Dado que la información utilizada en la auditoría tiene un carácter sensible y puede afectar a la seguridad de los sistemas de información, los resultados con el máximo detalle de cada uno de los controles revisados solo se comunican con carácter confidencial a los responsables del Ayuntamiento para que puedan adoptar las medidas correctoras que consideren precisas. En el presente informe los resultados se muestran de forma sintética.

APÉNDICE 2
Situación de los controles básicos de ciberseguridad

CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

Objetivo del control

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

Situación del control

El Ayuntamiento no dispone de un procedimiento formalmente aprobado para el mantenimiento y la gestión del inventario de dispositivos físicos.

La herramienta para la gestión del inventario *hardware* ha sido actualizada, permitiendo nuevas funcionalidades sobre los dispositivos con agente de red instalado, como la gestión de licencias, además de ser la herramienta de *ticketing* del departamento TIC.

Una de las mejoras más significativas ha sido la implantación de un *software* de EDR para la gestión centralizada de puestos de trabajo, permitiendo, entre otros, control de aplicaciones, actualizaciones y parches, etc. Sin embargo, durante nuestra revisión, el Ayuntamiento únicamente contaba con 100 licencias de prueba, aunque se tenía prevista la ampliación de dichas licencias y la incorporación de un sistema (MDM) para la gestión de dispositivos móviles.

Respecto al control de acceso de dispositivos físicos a la red corporativa, el departamento de informática ha realizado determinadas acciones encaminadas a mejorar, aunque de manera limitada, la situación señalada en nuestra anterior auditoría:

- Revisión de todas las tomas de red en zonas comunes o de acceso público, deshabilitando las tomas sin uso o innecesarias.

- Implantación de medidas que impiden el acceso de dispositivos a la red basadas en los requisitos de seguridad de los *endpoint*, aunque únicamente afecta a equipos que se conectan a la red desde el exterior.

- Integración a la red corporativa de distintos edificios, lo que permite ampliar las dependencias sobre las que se aplican controles.

Aunque el Ayuntamiento ha realizado determinadas acciones para corregir las deficiencias detectadas en nuestra anterior auditoría, no se han aplicado medidas efectivas que garanticen un control robusto sobre los dispositivos *hardware*, como la implantación de un servidor de validación para el acceso de dispositivos a la red o controles para otro tipo de dispositivos (móviles, dispositivos extraíbles, etc.).

Existe un insuficiente nivel de control sobre el inventario y el control de activos físicos, y su valoración global alcanza un **índice de madurez del 45,8%**, que se corresponde con un **nivel de madurez *N1, inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su

gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 1 del 57,2%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 40,4%, por tanto, se ha producido una leve mejora de 5,4 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* en la red, de forma que solo se pueda instalar y ejecutar *software* autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

Situación del control

El Ayuntamiento mantiene correctamente actualizado el inventario *software* mediante la misma herramienta utilizada para el inventario de activos *hardware*. Dicha herramienta EDR detecta y realiza un inventario automático del *software* de los dispositivos con agente de red y permite la gestión centralizada de parches y actualizaciones. Sin embargo, esta nueva herramienta únicamente se encuentra desplegada en 100 equipos de prueba, aunque han licitado más licencias con objeto de ampliar su uso a toda la organización.

Durante nuestro trabajo de auditoría realizado en 2019 se observó un determinado número de equipos con *software* fuera del periodo de soporte del fabricante, cosa que suponía un grave riesgo para todo el sistema de información. Durante el presente trabajo hemos observado que el departamento TIC ha realizado un esfuerzo en subsanar dicha deficiencia actualizando y homogeneizando el parque de equipos de usuario. También se ha revisado el *firmware* de la electrónica de red y del *firewall,* y se ha verificado que está correctamente actualizado. No obstante, sigue habiendo sistemas obsoletos (sin soporte del fabricante, actualizaciones o parches) que albergan algunos de los procesos críticos de la entidad, tal y como se describe en el siguiente control.

El Ayuntamiento no dispone de un plan de mantenimiento para la gestión integral de *software*. Las necesidades para la actualización de licencias, contrataciones y la adquisición de soluciones se van cubriendo mediante informes de necesidad emitidos por el departamento TIC que son aprobados por la dirección.

El Departamento TIC ha elaborado una lista blanca de aplicaciones autorizadas, pero dicha lista no ha sido formalmente aprobada.

La organización no tiene establecido un sistema de bloqueo de aplicaciones no permitidas, sin embargo, el control ha sido mejorado desde nuestro anterior trabajo de auditoría. Se han aplicado medidas compensatorias que proporcionan cierta efectividad al control, como la eliminación de privilegios de administración de los usuarios sobre sus máquinas y la

aplicación de reglas de *firewall* para impedir las conexiones de las aplicaciones fuera de la red.

Aunque el Ayuntamiento ha realizado acciones encaminadas a la mejora del control sobre el *software*, estas no están establecidas en un procedimiento aprobado formalmente.

El nivel de control sobre el inventario y control de *software* autorizado alcanza un **índice de madurez del 53,0%**, 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 2 del 66,3%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 37,4%, por tanto, se ha producido una mejora de 15,6 puntos en este índice.

CBCS 3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

Objetivo del control

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

Situación del control

Hemos verificado que, aunque el Ayuntamiento no ha aprobado un procedimiento que describa las acciones llevadas a cabo para la gestión de vulnerabilidades, sí se han realizado diversas acciones para mejorar dicha gestión.

Una de las mejoras en este control ha sido la implantación de una aplicación EDR, que permite la identificación de vulnerabilidades, además de la gestión centralizada de actualizaciones y parches en los sistemas con agente de red instalado. No obstante, como ya hemos señalado, únicamente disponen de 100 licencias de prueba a fecha del trabajo de revisión. El departamento ha licitado un contrato para extender las licencias a todos los equipos de la organización.

Las actualizaciones y parches de la electrónica de red o el *firewall* se aplican de manera manual y hemos comprobado que se realiza de manera periódica. Además, una de las buenas prácticas llevadas a cabo por el departamento de informática es la creación de *tickets* con alertas periódicas en la herramienta de *ticketing* para la revisión y actualización del *firmware* de la electrónica de red.

El departamento ha llevado a cabo el despliegue de la solución del CCN-CERT microCLAUDIA en todos los equipos de la red. También han desplegado la solución CARMEN, ofrecida por el CCN-CERT y gestionada por el CSIRT-CV, que alerta mediante informes periódicos de anomalías en la red. Los técnicos del departamento de informática aplican medidas acordes con los resultados de dichos informes.

Por último, el Ayuntamiento ha implantado una herramienta de vigilancia digital que rastrea la red en busca de filtraciones de datos de la organización. El departamento TIC monitoriza y realiza las notificaciones o correcciones pertinentes de los incidentes de seguridad detectados.

Aunque el control ha mejorado, sigue habiendo posibilidades de mejora que le garantizarían mayor efectividad, como el uso de herramientas de escaneo de vulnerabilidades, auditorías de *hacking* ético, la actualización de sistemas sin soporte o la documentación de todas las acciones llevadas a cabo desde la identificación hasta la resolución de vulnerabilidades críticas en un procedimiento aprobado por la corporación.

Además, la deficiencia más significativa ha sido la existencia, tal y como se ha descrito en el control de *software*, de determinados sistemas ligados a procesos críticos del Ayuntamiento que están fuera de su periodo de soporte con el fabricante (*software* de virtualización, aplicación de gestión de la información económico-financiera, sistemas del CPD), hecho que ha sido notificado por el departamento TIC a la dirección, pero no ha sido subsanado. No tener soporte del fabricante implica no recibir actualizaciones funcionales, ni parches de seguridad sobre las vulnerabilidades detectadas, lo que supone un riesgo grave que pone en peligro a todo el sistema de información.

Existe cierto nivel de control sobre la gestión de vulnerabilidades, siendo la valoración global del control de un **índice de madurez del 62,8%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 3 del 78,5%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 56,0%, por tanto, se ha producido una mejora de 6,8 puntos en este indicador.

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 tiene aprobado un procedimiento que describa la gestión de usuarios con privilegios de administración sobre los distintos sistemas y aplicaciones. Sin embargo, han llevado a cabo determinadas acciones para corregir las deficiencias detectadas en este control.

Una de las deficiencias graves detectada durante nuestra anterior auditoría fue la asignación a todos los usuarios de privilegios de administración sobre sus equipos. Hemos verificado que se han deshabilitado estos permisos a todos los usuarios que no los

necesitan. Además, se han creado cuentas de administración sobre los equipos de usuario que únicamente son utilizadas por el personal del departamento TIC para tareas de mantenimiento.

Otra de las incidencias graves reportadas fue la existencia de usuarios con perfiles de administración en la aplicación de gestión tributaria. Hemos podido verificar que la situación fue notificada a la empresa contratada y subsanada.

Además de las correcciones anteriores, el departamento ha realizado una revisión de los usuarios con privilegios de administración sobre el dominio, eliminando los usuarios genéricos y creando usuarios nominativos que identifican de manera inequívoca al personal que está realizando tareas de administración. Sin embargo, los miembros del departamento no disponen de usuarios con distintos niveles de privilegios en función del tipo de tarea a realizar.

Aunque la política de autenticación o de contraseñas no está formalmente aprobada, se han fortalecido los mecanismos de autenticación aumentando su complejidad. Además, el Ayuntamiento ha forzado a cambiar las contraseñas a todos los usuarios en determinadas ocasiones en las que han sido detectadas posibles vulneraciones de seguridad en el Ayuntamiento.

El departamento TIC mantiene un inventario de las aplicaciones que requieren usuarios con privilegios de administración, pero afirma que son los responsables de los departamentos quienes gestionan los usuarios y permisos.

Existe un cierto nivel de control sobre las cuentas con privilegios administrativos, siendo la valoración global del control de un **índice de madurez del 56,7%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 4 del 70,9%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 34,8%, por tanto, se ha producido una mejora de 21,9 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

Hemos analizado las acciones realizadas en el Ayuntamiento para el control de configuraciones seguras de los distintos dispositivos y aplicaciones y hemos verificado que, aunque existen ciertas acciones en este control, las mejoras son limitadas y no existe un procedimiento formalmente aprobado que describa los pasos a seguir para aplicar configuraciones seguras a los sistemas de la entidad.

Una de las mejoras llevadas a cabo es el uso de la opción *GlobalProtect* del *firewall* que impide la conexión de los equipos que no han sido configurados de acuerdo con unos criterios de seguridad definidos por el departamento TIC. Esta opción ha sido mejorada durante el periodo de teletrabajo ocasionado por la pandemia.

Además, hemos verificado que el departamento de informática incorpora en sus licitaciones la obligatoriedad, para las empresas o soluciones que van a ser contratadas, de incorporar las correspondientes certificaciones de seguridad del ENS. Para la contratación de aplicaciones se exigen configuraciones basadas en las guías de seguridad de las TIC del CCN-CERT.

Aunque algunas de las acciones descritas están relacionadas con la configuración segura de sistemas y aplicaciones, el control es únicamente efectivo de manera parcial, dado que no se dispone de un sistema para la monitorización de cambios no autorizados en las configuraciones o repositorios para gestión de versiones de las configuraciones de los sistemas críticos.

La valoración global del control existente sobre las configuraciones seguras es que la organización alcanza un insuficiente **índice de madurez del 40,0%**, que se corresponde con un **nivel de madurez *N1*, *inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 5 del 50,0%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 31,4%, por tanto, se ha producido una mejora de 8,6 puntos en el índice de madurez del control.

CBCS 6. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

Objetivo del control

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

Situación del control

El Ayuntamiento no ha aprobado un procedimiento que describa el tratamiento de los *logs* de auditoría que incluya aspectos como los sistemas afectados, la información que se

retiene, el periodo de retención, las copias de seguridad, la gestión de derechos de acceso a los registros o las revisiones y responsables de dichos registros.

El Ayuntamiento tiene el servicio de directorio de usuarios desplegado en la nube, solución que incorpora un completo sistema de registros de auditoría.

Las herramientas vistas en controles anteriores (vigilancia digital, gestor de actualizaciones, inventario) y las herramientas desplegadas del CSIRT-CV y CCN-CERT incluyen aspectos relacionados con este control, dado que incorporan registros que, aunque no son registros de auditoría sino eventos en tiempo real, son analizados y revisados por terceros. Además, el Ayuntamiento se encuentra en fase de integración con el vSOC del CSIRT-CV.

El Ayuntamiento no dispone de un recolector de eventos que permita la revisión centralizada e incluya los sistemas más críticos de la entidad.

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 53,0%**, 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 66,3%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 45,0%, por tanto, se ha producido una mejora de 8 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 la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.

Situación del control

El Ayuntamiento ha mejorado el sistema de copias visto en nuestra anterior auditoría. Sin embargo, no ha aprobado un procedimiento destinado a tal efecto, aspecto especialmente relevante en este control.

El departamento TIC ha realizado dos mejoras que han permitido evolucionar desde su sistema anterior de copias. Por una parte, han integrado una nueva solución para albergar los datos de la copia de seguridad de manera cifrada e inmutable, impidiendo la alteración de la información por parte de cualquier proceso de sistema o usuario. Por otro lado, han contratado un nivel adicional de copias de seguridad en la nube.

Una de las buenas prácticas llevadas a cabo por el departamento de informática es la creación de *tickets* que funcionan como recordatorios periódicos para la revisión de *backups*.

Aunque el departamento afirma realizar pruebas de restauración de las copias de distintos sistemas, dichas restauraciones no son planificadas ni documentadas, ni están establecidas en un documento formalmente aprobado.

La valoración global del control existente sobre las copias de seguridad es que el Ayuntamiento alcanza un **índice de madurez del 63,3%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 7 del 79,2%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,8%, por tanto, se ha producido una leve mejora de 2,5 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

El Ayuntamiento no ha realizado las acciones recomendadas durante nuestra revisión de 2019, realizadas con objeto de cumplir con 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. En consecuencia, siguen vigentes las carencias identificadas y las recomendaciones realizadas en el informe precedente.

Cumplimiento del RGPD

En cuanto al cumplimiento en materia de protección de datos personales, desde la revisión realizada en el año 2019 el Ayuntamiento afirma haber aplicado determinadas medidas para proteger los datos de carácter personal, habiendo adaptado el DPD de algunos sistemas a la normativa vigente. No obstante, no se ha aportado documentación al respecto.

Cumplimiento de la legalidad del registro de facturas

Se ha aportado la auditoría de sistemas exigida por la Ley 25/2013, de 27 de diciembre.

Indicadores

En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad ha puesto de manifiesto que existe un insuficiente grado de cumplimiento de la normativa, siendo el **índice de madurez del 61,0%**, que se corresponde con un **nivel de madurez N2,** que indica que existen incumplimientos significativos de la normativa y hay aspectos que se deben mejorar.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 50,0%, que se corresponde con un nivel de madurez *N2*. Por tanto, se ha producido una mejora de 11 puntos en el índice de madurez del control.

Gobernanza de ciberseguridad

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

Si bien en la auditoría hemos observado cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento y particularmente de los responsables de las áreas implicadas, existen carencias relevantes que indican que la gobernanza no puede considerarse efectiva.

Las carencias más relevantes identificadas y que dificultan el establecimiento de un adecuado sistema de gestión de la seguridad de la información (SGSI) son las siguientes:

- La política de seguridad de la información (PSI) está formalmente aprobada pero está desactualizada y no refleja la realidad de la institución.

- La inexistencia de procedimientos de seguridad formalmente asumidos por la organización y que se apliquen de manera homogénea a todas sus áreas.

- La falta de actividad del Comité de Seguridad, órgano imprescindible para coordinar la seguridad de la información en la entidad, que debe reunirse periódicamente y asumir un carácter proactivo en la toma de todas las decisiones que afecten a la seguridad de la información.

- La falta de actividad de los roles clave en la organización, particularmente el responsable de seguridad, cuyas responsabilidades se encuentran detalladas y asignadas en la política de seguridad, pero no son ejercidas de manera efectiva.

- Existe insuficiencia de recursos económicos y humanos reportada desde el departamento TIC para atender:

    - La necesidad de actualización de ciertos sistemas en el CPD o la situación del sistema económico-financiero.

- La necesidad de cubrir las vacantes existentes de personal en el departamento TIC.

No obstante, se han identificado determinados aspectos positivos en la gestión de la ciberseguridad:

- Las actividades formativas y de concienciación al personal de la corporación, que están siendo adecuadamente organizadas y gestionadas y que están reportando resultados positivos, con un alto grado de aceptación por parte del personal del Ayuntamiento.

- La investigación proactiva y el uso de soluciones innovadoras para la gestión o implantación de determinados controles de seguridad.

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

- El esfuerzo, por parte de los responsables de las áreas relacionadas, en la identificación de necesidades, requisitos y su adecuada comunicación a la corporación mediante informes de necesidad.

- La existencia de una planificación estratégica de actuaciones en el marco de la ciberseguridad.

Es urgente solventar, por tanto, las carencias identificadas, ya que afectan de manera negativa al nivel de seguridad de la información, y explotar las fortalezas existentes, que facilitarán la aplicación de medidas necesarias y recomendaciones efectuadas en el presente informe para articular de forma efectiva el SGSI del Ayuntamiento.

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.

Plataforma para la gestión y dinamización de la concienciación en la ciberseguridad

Uno de los aspectos en los que el departamento TIC está realizando un esfuerzo notable ha sido en la concienciación de los trabajadores de toda la organización. Para ello, el Ayuntamiento utiliza una plataforma desde la que son programadas distintas campañas de concienciación y acciones de duración corta que son lanzadas a los usuarios. Dichas campañas incluyen la difusión de noticias, exámenes, pruebas de *phishing*, etc.

Los resultados obtenidos son analizados y permiten evaluar el estado de concienciación de la entidad, emitiendo informes con indicadores sobre el nivel de riesgo. La herramienta tiene la capacidad de filtrar los resultados por áreas o incluso por usuarios.

El uso de este tipo de herramientas en el Ayuntamiento permite, de acuerdo con los resultados obtenidos, aumentar de manera considerable la cultura de ciberseguridad de todos los miembros de la organización. Además, no se trata de un proyecto ejecutado en un momento puntual, sino que está enfocado como un proceso de mejora continua.

Vigilancia digital/Cibervigilancia

El Ayuntamiento ha implantado una herramienta de vigilancia digital, un servicio basado en robots que rastrean la red en busca de filtraciones de información de la organización, emitiendo alertas de las incidencias detectadas. Dichas alertas son recibidas por los miembros del departamento TIC, quienes supervisan los informes generados y realizan las acciones pertinentes.

Esta herramienta proporciona un indicador del estado de la ciberseguridad de la entidad basado en el análisis de diferentes aspectos, como la fuga de datos o credenciales, seguridad en el correo electrónico, análisis web o reputación IP, entre otros.

Este sistema de vigilancia digital, junto con las alertas de las aplicaciones implantadas del CCN-CERT y CSIRT-CV, completan el sistema de detección de anomalías e incidencias dentro y fuera de la red.

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[16]: 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

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

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

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

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

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

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, un borrador previo del Informe de auditoría se discutió con el concejal de Nuevas Tecnologías del Ayuntamiento y con el coordinador técnico del Servicio Municipal de Informática 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 auditoría correspondiente a 2021, el mismo se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Transcurrido dicho plazo no se han recibido alegaciones.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y del artículo 55.1.h) de su Reglamento de Régimen Interior y de los programas anuales de actuación de 2021 y 2022 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 18 de octubre de 2022, aprobó este informe de auditoría.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe seguimiento recomendaciones CBCS Ayuntamiento Sagunto 2019 - SEFYCU 3562427

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 ZANK D7Q3 UXTC 3CRC

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 - 18/10/2022 11:48 VICENT CUCARELLA TORMO