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 BENIDORM DEL AÑO 2019

Situación a 31 de diciembre de 2021

RESUMEN

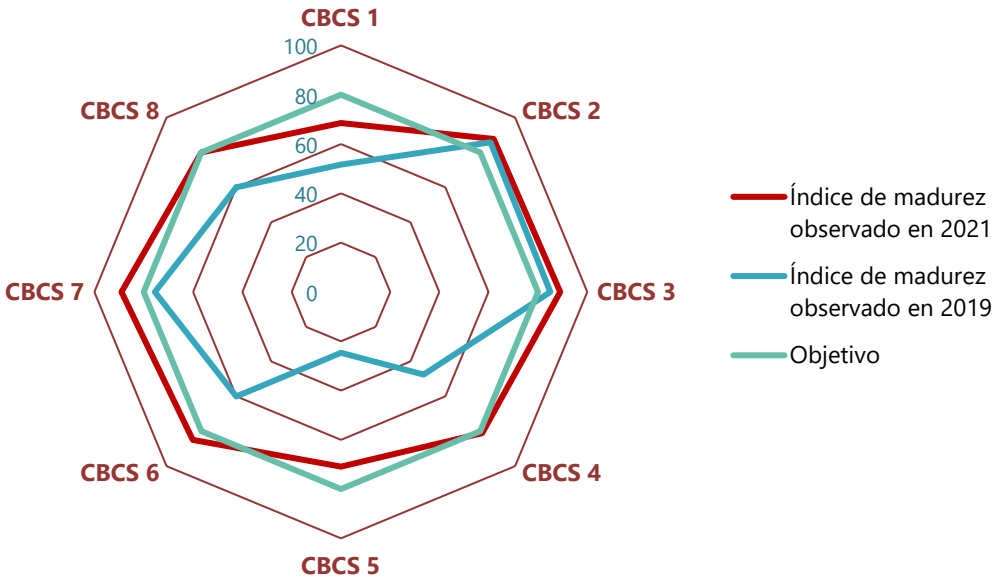
La transformación digital que están experimentando todas las Administraciones públicas y su interconexión a través de complejas redes informáticas las expone de forma cada vez más intensa a amenazas provenientes del ciberespacio. Esto origina un incremento de los riesgos asociados a los sistemas de información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

Conclusiones

El Ayuntamiento ha realizado progresos significativos desde nuestra anterior auditoría y se han atendido la mayoría de nuestras recomendaciones.

El índice de madurez general de los controles básicos de ciberseguridad alcanza el objetivo establecido y muestra un valor del 81,4%, que mejora sustancialmente el 61,3% registrado en nuestra auditoría de 2019.



Hemos constatado que el Ayuntamiento tiene establecida una aceptable gobernanza de la ciberseguridad. Los órganos superiores del Ayuntamiento (alcalde y/o la Junta de Gobierno) son los responsables del sistema de control, 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.

Sin embargo, es necesario que el comité de seguridad, como órgano colegiado, se reúna periódicamente con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones convenientes.

Asimismo, nuestra revisión ha puesto de manifiesto un razonable grado de cumplimiento de las normas legales relacionadas con la seguridad de la información, aunque en el Informe se señalan diversos aspectos pendientes de mejora sobre los que se debe actuar, como la planificación y ejecución de auditorías de cumplimiento del ENS.

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. En particular, aconsejamos mejorar los controles que impiden la conexión de dispositivos no autorizados a la red corporativa y desarrollar un proceso de gestión continuada de la configuración sobre los sistemas críticos de la entidad.

NOTA

Este resumen pretende ayudar a la comprensión de los resultados de nuestro informe y facilitar la labor a los lectores y a los medios de comunicación. Recomendamos 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 Benidorm del año 2019

Situación a 31 de diciembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

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

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

En 2019 y 2020 la Sindicatura de Comptes realizó sendas auditorías sobre la situación de los controles básicos de ciberseguridad (CBCS) de los 15 ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes y el 12 de febrero de 2020 el Consell de la Sindicatura de Comptes aprobó el *Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Benidorm, 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 analizados.

La necesidad de una adecuada ciberhigiene

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

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

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

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

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

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

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

De acuerdo con lo previsto en los programas anuales de actuación de 2021 y 2022 hemos realizado el seguimiento de la situación de los controles básicos de ciberseguridad y de las recomendaciones efectuadas en el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Benidorm. Ejercicio 2019.

La responsabilidad de la Sindicatura de Comptes es concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación sobre su diseño y eficacia operativa, sobre el cumplimiento de la normativa básica relativa a la seguridad de la información y, en su caso, formular recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control.

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

La presente auditoría se ha centrado en el análisis de la situación actualizada 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 del trabajo.

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

El ayuntamiento ha realizado progresos significativos desde nuestra anterior auditoría y se han atendido la mayoría de nuestras recomendaciones. El índice de madurez general de los controles básicos de ciberseguridad alcanza el objetivo establecido.

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el grado de control existente en la gestión de los controles básicos de ciberseguridad alcanza un **índice de madurez general del 81,4%**, que se corresponde con un nivel de madurez *N3, proceso definido,* es decir, los procesos de control implantados están estandarizados y formalmente documentados.

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 Índice de madurez	2019 Nivel de madurez	2019 Índice de cumplimiento	2021 Índice de madurez	2021 Nivel de madurez	2021 Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	*51,6%*	*N2*	*64,5%*	68,5%	N2	85,6%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	*85,8%*	*N3*	*100%*	87,7%	N3	100%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	*85,0%*	*N3*	*100%*	89,0%	N3	100%
CBCS 4 Uso controlado de privilegios administrativos	*47,4%*	*N1*	*59,2%*	81,0%	N3	100%
CBCS 5 Configuraciones seguras del *software* y *hardware*	*24,7%*	*N1*	*30,9%*	70,9%	N2	88,6%
CBCS 6 Registro de la actividad de los usuarios	*60,0%*	*N2*	*75,0%*	85,0%	N3	100%
CBCS 7 Copias de seguridad de datos y sistemas	*75,5%*	*N2*	*94,3%*	89,0%	N3	100%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	*60,0%*	*N2*	*75,0%*	80,0%	N3	100%
General	61,3%	N2	74,9%	81,4%	N3	96,8%

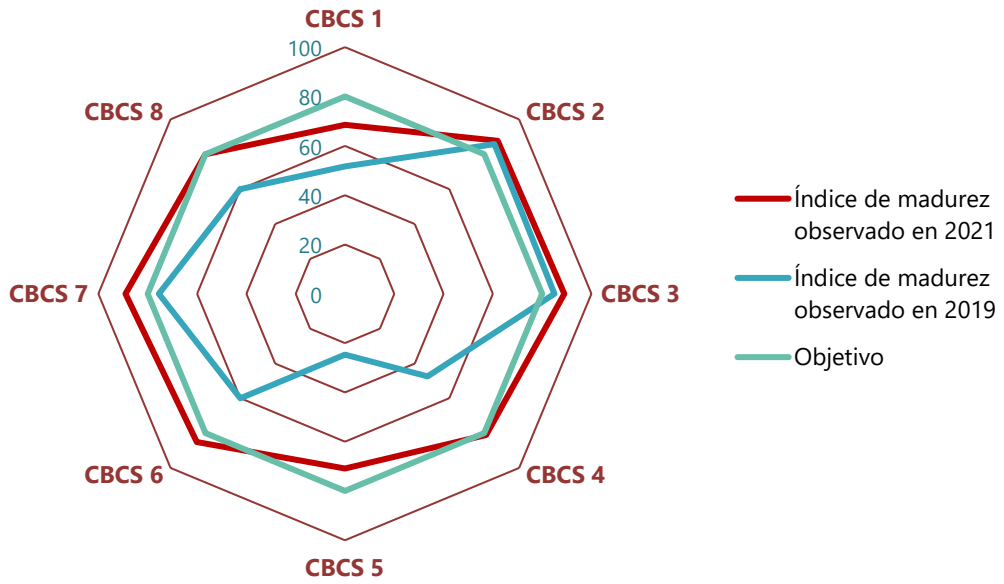
El índice de cumplimiento de los CBCS resulta de comparar el indicador de madurez con el nivel requerido u objetivo que tiene el sistema según el ENS, que es el 80% o *N3, proceso definido*.

El índice de cumplimiento general es la media de los índices individuales (con tope individual en el 100%) y alcanza el 96,8%, que ha mejorado desde el 74,9% de nuestro anterior informe. La comparación de los resultados detallados del presente trabajo con los obtenidos en el año 2019 muestra una mejora en todos los controles.

A pesar de la mejora experimentada, existen controles que no alcanzan los niveles exigidos por el ENS para la protección de los sistemas de información (CBCS 1, CBCS 5). En el apartado 5 se realizan las recomendaciones pertinentes con esa finalidad.

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

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



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

El Ayuntamiento de Benidorm tiene establecida una aceptable gobernanza de la ciberseguridad y debe mantener 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.

Hemos podido verificar la existencia de un adecuado nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento, junto con unos adecuados procesos de gestión. No obstante, es necesario que el comité de seguridad, como órgano colegiado, se reúna periódicamente con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones convenientes. Todo ello nos permite afirmar que la gobernanza de ciberseguridad alcanza un nivel aceptable.

Existe un razonable grado de adecuación a la normativa relativa a la seguridad de la información

La revisión del cumplimiento de legalidad en materia relacionada con la seguridad de la información ha puesto de manifiesto un razonable nivel de cumplimiento de la normativa.

No obstante, en el apartado 5 se señalan varios aspectos pendientes de mejora 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. Mejorar las soluciones actualmente implantadas para impedir la conexión de dispositivos no autorizados a la red corporativa y establecer dichas medidas en un procedimiento aprobado formalmente.

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

2. La recomendación del informe de 2019 ha sido implementada.

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

3. La recomendación del informe de 2019 ha sido implementada.

4. La recomendación del informe de 2019 ha sido implementada.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

5. La recomendación del informe de 2019 ha sido implementada.

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

6. 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)

7. La recomendación del informe de 2019 ha sido implementada.

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

8. La recomendación del informe de 2019 ha sido implementada.

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

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

   - Adoptar las medidas de seguridad descritas en la declaración de aplicabilidad.
   - Realizar las auditorías de seguridad previstas en el Real Decreto 3/2010.
   - Publicar en la sede electrónica la certificación 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.

10. La recomendación del informe de 2019 ha sido implementada.

Seguimiento de recomendaciones anteriores

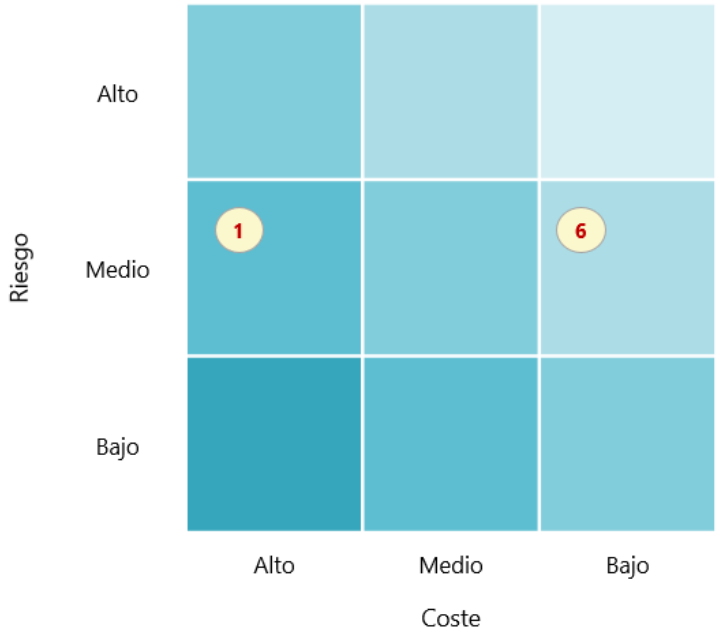
Hemos realizado un seguimiento de las recomendaciones efectuadas en el informe de auditoría del año 2019.

Tal como se muestra en el cuadro 2, de las diez recomendaciones realizadas en ese informe, siete han sido atendidas, dos lo han sido solo parcialmente y una no ha sido atendida.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el gráfico 2 se muestra la clasificación de las recomendaciones según los criterios combinados de **riesgo potencial a mitigar** y **coste estimado de su implantación**. Este gráfico ha sido actualizado respecto al trabajo realizado en el año 2019, adaptando la relación riesgo/coste de cada recomendación considerando las mejoras realizadas desde la anterior revisión. No se incluye el punto 9 anterior, ya que es una medida de obligado cumplimiento.

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



Actuaciones en curso

Aunque no se han tenido en cuenta en el cálculo de los indicadores mostrados en el apartado 4, hemos verificado que en el momento de finalización del trabajo de campo de la auditoría han sido iniciadas o planificadas actuaciones en materia de ciberseguridad en diversos ámbitos que atenderían algunas de las recomendaciones anteriores. Estas actuaciones se encuentran alineadas con los objetivos del Ayuntamiento para la adecuación al ENS y algunas se han iniciado como consecuencia de las recomendaciones realizadas en la auditoría del año 2019. La implantación efectiva de estas actuaciones tendrá un impacto positivo en el nivel de ciberseguridad de la entidad.

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

- Despliegue de una solución MDM (m*obile device management*). El Ayuntamiento se encuentra en fase de implantación de un sistema de control de dispositivos móviles.

- Contratación de servicios especializados en ciberseguridad. El Ayuntamiento se dispone a incluir entre sus acciones una auditoría de *hacking* desde dentro de su propia red, estableciendo como objetivos sus propios servicios y sistemas críticos.

- Despliegue de servicios y herramientas proporcionados por el CCN y el CSIRT-CV que se suman a los servicios ya implantados en la organización (LUCIA, GLORIA):

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

Herramienta en fase de implantación a fecha 31 de diciembre de 2021 pero implantada en su totalidad a fecha de este informe.

- CLAUDIA, solución de *endpoint*[2] integrada con la herramienta CARMEN que permite tener una visión más completa de lo que ocurre dentro de una red.

- microCLAUDIA, que proporciona protección contra código dañino de tipo *ransomware*[3]. Herramienta en fase de implantación a fecha 31 de diciembre de 2021 pero implantada en su totalidad a fecha de este informe.

- REYES, que permite realizar investigación y análisis sobre ciberincidentes de forma ágil y rápida. Consiste en un metabuscador de información de diversas fuentes especializadas en ciberamenazas, que está integrado con herramientas de análisis del CCN-CERT. El Ayuntamiento recibe informes periódicos del CSIRT-CV con incidentes de seguridad relacionados con los dominios y correos corporativos (vigilancia digital).

[2] Un punto final o *endpoint* es un dispositivo informático remoto que se comunica a través de una red a la que está conectado. Se refiere típicamente a dispositivos utilizados como ordenadores de escritorio, portátiles, teléfonos inteligentes, tabletas o dispositivos de Internet de las cosas.

[3] Un *ransomware* es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Cuadro 2. Seguimiento de recomendaciones

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior.	Estado de la recomendación	Consecuencia en el informe
1	Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Aunque se han implantado medidas para restringir el acceso de dispositivos no autorizados a la red corporativa, el control puede ser mejorado. Adicionalmente, todas las medidas implantadas a tal efecto deben recogerse en un procedimiento formalmente aprobado.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
2	Actualizar el procedimiento para la gestión integral del *software* de la entidad, considerando: - La elaboración de listas de *software* autorizado (listas blancas) y la realización de revisiones periódicas del *software* instalado. - La definición de un plan de mantenimiento del *software* que considere de manera integral la totalidad del *software* utilizado, incluyendo tanto el gestionado mediante licitaciones y cláusulas contractuales, como el resto de *software* utilizado en el Ayuntamiento.	Ha sido elaborado un procedimiento, que se encuentra aprobado, en funcionamiento y se ha destinado personal a tal efecto.	**Aplicada**	Se elimina la recomendación dada en 2019.
3	Implantar una herramienta de escaneo de vulnerabilidades en la red, como medida adicional a las pruebas de penetración. Se deberán llevar a cabo y documentar revisiones periódicas de vulnerabilidades. Este proceso deberá ser añadido al procedimiento de seguridad perimetral.	Se ha implantado una herramienta SIEM de análisis en tiempo real que es gestionada por una empresa experta. Se emiten informes diarios que son revisados y se realizan acciones atendiendo a las vulnerabilidades detectadas.	**Aplicada**	Se elimina la recomendación 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
4	Completar el documento de seguridad perimetral ampliando la documentación referente al proceso de remediación de vulnerabilidades, considerando: - Análisis previo a la entrada en producción de sistemas. - Priorización basada en el análisis de riesgos. - La resolución y la documentación de las vulnerabilidades, identificando fechas, prioridad, responsable, solución, etc.	Todas las acciones relacionadas con la gestión de vulnerabilidades se han establecido en el procedimiento aprobado a tal efecto. Se establecen responsabilidades atendiendo al tipo de vulnerabilidad detectada.	**Aplicada**	Se elimina la recomendación dada en 2019.
5	Formalizar un único procedimiento unificado de gestión de usuarios con privilegios de administración que establezca las directrices para todos los sistemas de la entidad y que incluya: - La eliminación, siempre que sea posible desde el punto de vista técnico, de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos. - Cuando existan razones de índole técnico que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas. - 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.	Han sido revisados los usuarios con privilegios de administración de todos los sistemas de la entidad y se han eliminado aquellos usuarios cuya existencia no se encontraba justificada. Los administradores tienen distintos perfiles de administración, dependiendo del tipo de tareas a realizar. Todas las medidas implantadas han sido establecidas en el procedimiento aprobado a tal efecto.	**Aplicada**	Se elimina la recomendación 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
6	Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN. Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la revisión periódica de los cambios realizados, bien mediante procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.	Se ha elaborado y aprobado un procedimiento a tal efecto que describe la configuración de plantillas, el uso de guías de seguridad, etc. El departamento ha implantado una herramienta que monitoriza y detecta cambios en equipos, sin embargo, no se ha definido un grupo de sistemas críticos sobre los que realizar revisiones periódicas de cambios de configuración.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
7	Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de actividad de usuario, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*.	Se ha elaborado y aprobado un procedimiento que describe todos los aspectos recomendados. Adicionalmente, los registros y la correlación de los mismos son revisados regularmente y se realizan acciones con las incidencias detectadas.	**Aplicada**	Se elimina la recomendación dada en 2019.
8	Complementar el proceso de gestión de copias de seguridad mediante el establecimiento de un nivel adicional de protección, de manera que existan copias de seguridad en soporte desconectado o no accesibles de forma directa a nivel de red.	El departamento ha implementado el funcionamiento de copias inmutables. Adicionalmente, se ha auditado esta característica para verificar su efectividad y se han separado las copias de los usuarios del dominio.	**Aplicada**	Se elimina la recomendación dada en 2019.
9	Implantar las medidas necesarias para dar cumplimiento a los requisitos del RD 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe: - Adoptar las medidas de seguridad de la declaración de aplicabilidad. - Realizar las auditorías de seguridad previstas en el artículo 34.	Sin variación.	**No aplicada**	Se mantiene la redacción.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior.	Estado de la recomendación	Consecuencia en el informe
	- 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.			
10	En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la LO 3/2018, de 5 de diciembre. En particular debe: - Hacer público por medios electrónicos el inventario de sus actividades de tratamiento, dando cumplimiento al artículo 31.2 de la Ley Orgánica 3/2018. - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD. - Planificar y ejecutar de auditorías de cumplimiento en materia de protección de datos.	Se realizan auditorías anuales por áreas y se realizan trabajos regulares en este campo. Se emite un informe anual con las actuaciones en esta materia.	**Aplicada**	Se elimina la recomendación dada en 2019.

APÉNDICE 1
Metodología aplicada

Introducción

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

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

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

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

Aun cuando la adopción de medidas de seguridad adecuadas hace más resilientes a las organizaciones frente a los ciberataques, el análisis de los incidentes ocurridos que se realiza en los informes INES[4] del CCN revela que las organizaciones no siempre implementan ni tan siquiera las medidas más básicas que podrían haber evitado o mitigado el daño causado. Por otro lado, el hecho de que los ciberataques permanezcan en muchos casos sin ser detectados durante mucho tiempo puede ser evidencia de que las medidas básicas no están correctamente implementadas.

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

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

Objetivo de la auditoría

De acuerdo con lo previsto en los programas anuales de actuación de 2021 y 2022, nuestro objetivo ha sido realizar el seguimiento de la situación de los controles básicos de ciberseguridad y de las recomendaciones efectuadas en el *Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Benidorm, 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[5] como su eficacia operativa[6] para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte. 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 aplicaciones que

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

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

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

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

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

Ámbito temporal

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

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

Metodología

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

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

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

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

La guía práctica de fiscalización de los OCEX 5313

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

El contenido de la GPF-OCEX 5313, fundamentalmente relacionado con la auditoría de la seguridad de los sistemas de información, es coherente con los postulados del ENS. No obstante, dada la amplitud del ENS, que está formado por 75 medidas de seguridad, para su inclusión en los CBCS se seleccionó una serie limitada de controles. Para escoger los más relevantes se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security (CIS)[7], que define, prioriza y clasifica veinte controles de ciberseguridad según su importancia para hacer frente a las ciberamenazas. Su ventaja principal es que están orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. Según el CIS, con carácter general, las organizaciones que apliquen solo los cinco primeros controles pueden reducir su riesgo ante ciberataques alrededor del 85%. Si se implementan los veinte controles el riesgo se puede reducir un 94%.

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

Alineación de los CBCS con el Esquema Nacional de Seguridad

Dado que el ENS es de obligado cumplimiento para todos los entes públicos, se ha tenido especial cuidado en que la metodología de auditoría de los controles básicos de ciberseguridad estuviera plenamente alineada con el ENS. Esa alineación facilita la realización de las auditorías de ciberseguridad por parte de la Sindicatura y coadyuva a la implantación del ENS en los entes auditados, ya que prácticamente todos los subcontroles o controles detallados que verifica la Sindicatura son requeridos por el ENS. De este modo, los ocho controles básicos de ciberseguridad presentan una correspondencia (no exacta) con las siguientes referencias del ENS:

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

Cuadro 3. Los CBCS y el ENS

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

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

Los CBCS como medidas de ciberhigiene

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

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

En esa dirección, ENISA establece diez puntos de acción para una adecuada ciberhigiene. Como se observa en el cuadro 4, de los siete CBCS, sin contar el de cumplimiento normativo, cinco son coincidentes con los puntos de acción prioritarios recomendados por ENISA como buenas prácticas de ciberhigiene.

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

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

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

Cuadro 4. Puntos de acción de ENISA

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

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

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

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

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

Cuadro 5. Los CBCS y sus subcontroles

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

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

Evaluación de los resultados del trabajo

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

Subcontroles

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

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

Cuadro 6. Evaluación de los subcontroles

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

Controles

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

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

Cuadro 7. Niveles de madurez

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

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

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

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

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

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

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

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

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

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

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

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

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

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

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

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

De acuerdo con la categoría de cada sistema, los niveles mínimos de exigencia o de madurez requeridos son[11]:

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

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

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

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

Indicadores globales

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

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

- El **índice de cumplimiento** analiza igualmente el nivel de madurez alcanzado, pero en relación con la exigencia aplicable en cada caso, teniendo en cuenta la categoría del sistema.

Gobernanza de ciberseguridad

A los efectos del presente trabajo, se entenderá por gobernanza de la seguridad de la información y las comunicaciones o de ciberseguridad (términos que utilizamos de forma indistinta en este informe) el conjunto de responsabilidades y actividades realizadas por la alta dirección con el objetivo de proporcionar una dirección estratégica en esta materia, garantizar que se logren los objetivos, verificar que el riesgo se gestione adecuadamente y comprobar que se utilicen los recursos de la entidad de una forma responsable.[12]

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

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

Es más que una mera cuestión técnica, por lo que **exige un liderazgo efectivo, procesos sólidos y estrategias en consonancia con los objetivos de la organización**[13].

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

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

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

La implicación de los órganos superiores es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información o de ciberseguridad[14]. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información[15], que debe materializarse en aspectos tales como:

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

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

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

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

  La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[16], que se constituye como un órgano colegiado, algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad, y es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio. Su composición debe constar en la PSI.

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

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

- Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.

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

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

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

- 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 Benidorm. 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 complementa la herramienta de inventario analizada en la auditoría anterior, OCS Inventory, con una nueva herramienta, Microsoft Endpoint Configuration Manager 2019, con la que se ha mejorado la gestión del inventario de activos *hardware*.

La nueva herramienta incluye los elementos sin agente de red, permite ver cambios significativos en los distintos dispositivos, permite gestión centralizada de *software*, gestión de parches y actualizaciones, control de acceso a recursos en red, aplicación de políticas, generación de informes, etc.

Respecto al control de dispositivos físicos no autorizados, el departamento gestiona las tomas de red deshabilitando los puertos en los *switches*, que además son controlados por *mac*. Además, el departamento ha deshabilitado el servicio DHCP y restringido el acceso a los recursos compartidos únicamente a elementos del dominio del Ayuntamiento.

Dado que existen usuarios que se conectan al sistema de información a través de escritorios virtualizados, el departamento ha implantado medidas adicionales de protección para estos sistemas, como el acceso con doble factor de autenticación o la prohibición de compartir discos duros locales o dispositivos USB con los sistemas remotos.

Aunque se ha mejorado el control sobre los dispositivos físicos no autorizados, las medidas descritas no están implantadas en todos los dispositivos de la entidad, no se recogen en los procedimientos aprobados y existen mejoras que garantizarían mayor efectividad al control.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 68,5%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 1 del 85,6%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 51,6%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*. Por tanto, se ha producido una mejora de 16,9 puntos en el índice de madurez del control.

CBCS 2. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) todo el *software* 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 ha mejorado el control establecido sobre el *software* con la implantación de la herramienta descrita en el control anterior, Microsoft Endpoint Configuration Manager 2019, que inventaría todo el software e incluye mejoras respecto a la aplicación OCS Inventory revisada durante la anterior auditoría, como la visualización del software fuera o cerca del periodo de finalización de soporte o aspectos como la gestión centralizada de aplicaciones y parches.

El Ayuntamiento ha aprobado en 2021 un plan de mantenimiento de *software* que define las acciones que se realizan en este aspecto y ha destinado personal a tal efecto.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 87,7%**, que se corresponde con un **nivel de madurez *N3*, *proceso definido***; es decir, los procesos de control implantados están estandarizados y formalmente documentados. Esto representa un **índice de cumplimiento del CBCS 2 del 100%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 85,8%, que se corresponde con un nivel de madurez *N3, proceso definido*. Por tanto, se ha producido una mejora de 1,9 puntos en el índice de madurez del control.

CBCS 3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

Objetivo del control

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

Situación del control

El Ayuntamiento ha dado un paso importante en el proceso de identificación y remediación de vulnerabilidades, pues ha implantado una herramienta de SIEM (*security information and event management*) para el análisis y correlación de eventos en tiempo real, que además se nutre de bases de datos de dos plataformas, una pública colaborativa y otra privada. Esta herramienta ha sido externalizada y es gestionada por una empresa especialista en la materia.

Todas las acciones encaminadas a la gestión de vulnerabilidades -la identificación, priorización y resolución- han sido detalladas en un procedimiento aprobado que establece la priorización atendiendo a la criticidad de las vulnerabilidades, e incluye la actualización de sistemas y dispositivos previa su entrada en producción.

El departamento también ha mejorado el sistema utilizado para aplicar parches y actualizaciones, dado que la nueva herramienta implantada, Microsoft Endpoint Configuration Manager 2019, permite la gestión centralizada de parches y actualizaciones.

Por último, se ha mejorado la situación del control mediante acciones como:

- Dividir resultados de los test de *hacking* ético por áreas y establecer responsables en cada área.

- Implantación de herramientas del CCN como CARMEN y microCLAUDIA, en fase de implantación a fecha de 31 de diciembre de 2021, pero totalmente implantadas durante la redacción del presente informe.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 89,0%**, que se corresponde con un **nivel de madurez *N3*, *proceso definido***; es decir, los procesos de control implantados están estandarizados y formalmente documentados. Esto representa un **índice de cumplimiento del CBCS 3 del 100%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 85,0%, que se corresponde con un nivel de madurez *N3, proceso definido*. Por tanto, se ha producido una mejora de 4 puntos en el índice de madurez del control.

CBCS 4. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

Objetivo del control

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

Situación del control

Para subsanar las deficiencias detectadas durante el anterior trabajo de auditoría, el Ayuntamiento ha realizado las correcciones y mejoras que se proponían.

Se han eliminado, cuando ha sido posible desde el punto de vista técnico, todos los usuarios no nominativos de todos los sistemas. Únicamente se utilizan usuarios no nominativos para procesos del sistema que requieren de privilegios, casos en los que el nombre de usuario identifica inequívocamente el proceso que realiza.

Se han eliminado los usuarios por defecto de todos los sistemas y se ha establecido en el procedimiento aprobado que se deben evitar nombres de usuario que sugieran que los usuarios tienen privilegios de administración.

Para cada administrador de sistemas de la entidad, el departamento utiliza diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar. Además, existe en un nivel adicional, consistente en la creación de usuarios administradores por servicios o grupos de servidores que se administran. Este nivel adicional consigue segmentar las máquinas sobre las que un administrador tiene privilegios, disminuyendo la zona de exposición en caso de infecciones por *ransomware*.

Se han establecido en los procedimientos buenas prácticas en la creación y gestión de usuarios y contraseñas, como son, entre otras:

- Cambiar los nombres de usuario y las contraseñas que por defecto vienen en los dispositivos y sistemas.
- Evitar nombres de usuario que sugieran que un usuario tiene privilegios de administración.
- Establecer, siempre que sea posible y proporcione ventajas de seguridad, una política de usuario único, de manera que se utilicen los usuarios del dominio en los servicios y aplicaciones que lo permitan.
- No utilizar el usuario administrador del dominio, cuyas credenciales son conocidas únicamente por los responsables y custodiadas por la dirección, cosa que se ha establecido en el procedimiento.

Todas las acciones llevadas a cabo por el departamento para la gestión de usuarios con privilegios administrativos y cambios de contraseñas han sido añadidas al procedimiento aprobado.

Aunque se ha verificado que existen controles efectivos en cada uno de los puntos detallados, el Ayuntamiento puede seguir mejorando en algunos aspectos:

- El uso de políticas de contraseñas en los sistemas que no permiten la integración de los usuarios con las políticas del dominio.
- Auditoría de acciones de usuarios administradores extensiva a todos los sistemas.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 81,0%**, que se corresponde con un **nivel de madurez *N3*, *proceso definido***; es decir, los procesos de control implantados están estandarizados y formalmente documentados. Esto representa un **índice de cumplimiento del CBCS 4 del 100%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 47,4%, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*. Por tanto, se ha producido una notable mejora de 33,6 puntos en el índice de madurez del control.

CBCS 5. CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE

Objetivo del control

Establecer una configuración base segura del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente, utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.

Situación del control

El departamento ha completado el procedimiento existente con todas las tareas que llevan a cabo: protocolo de instalación de estaciones de trabajo, actualización de *firmware* de equipos, revisiones periódicas, configuraciones basadas en plantillas, etc.

La configuración de dispositivos y sistemas se realiza a partir de plantillas preconfiguradas que además son revisadas y actualizadas periódicamente. Para la elaboración de estas plantillas, existen responsables y se establece en el procedimiento que deben seguir las recomendaciones de seguridad de las principales entidades en materia de seguridad (CCN, CIS, etc.).

El procedimiento aprobado a tal efecto incluye un apartado de "Mediciones y métricas" que describe la recogida de indicadores con objeto de garantizar la mejora continua sobre el control. Sin embargo, no se recogen identificadores con la finalidad de establecer objetivos cuantitativos, lo que impide alcanzar niveles de madurez superiores.

Mediante la herramienta comentada en puntos anteriores, Microsoft Endpoint Configuration Manager 2019, el departamento monitoriza y detecta cambios en equipos, sin embargo, no se ha definido un grupo de sistemas críticos sobre los que realizar revisiones periódicas de cambios de configuración.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 70,9%**, 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 5 del 88,6%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 24,7%, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*. Por tanto, se ha producido una notable mejora de 46,2 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, consciente de la oportunidad de mejora en este punto, ha elaborado y aprobado un procedimiento de gestión de registros de auditoría que define el alcance de los sistemas a auditar, las acciones, responsabilidades, permisos de acceso a los registros, periodos de retención, utilización del SIEM, directivas que se aplican, política de *backup* de los registros, etc.

El departamento utiliza la herramienta AlienVault para la recopilación de los registros de los diversos sistemas, permitiendo así homogeneizar el tratamiento de los distintos registros. La herramienta anterior, además, actúa como correlador de eventos.

Tal y como indica el responsable del departamento, AlienVault integra varios sistemas y genera un volumen grande de registros. Por este motivo, el departamento ha redefinido el proceso de revisión y ha externalizado el proceso en una empresa especializada, garantizando así la revisión de anomalías 24/7.

Adicionalmente, el responsable del departamento recibe diariamente un informe de anomalías detectadas y genera *tickets* con los incidentes detectados para su resolución.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 85,0%**, que se corresponde con un **nivel de madurez *N3*, *proceso definido***; es decir, los procesos de control implantados están estandarizados y formalmente documentados. Esto representa un **índice de cumplimiento del CBCS 6 del 100%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,0%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*. Por tanto, se ha producido una mejora de 25 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, consciente de la necesidad de establecer un control robusto que garantice la recuperación de los datos y sistemas en caso de desastre, ha elaborado un plan de recuperación de desastres y ha trabajado en mejorar las copias de seguridad.

Para ello, ha sustituido la herramienta revisada en la anterior auditoría, Symantec Backup Exec, por Veeam Backup. En la nueva herramienta se incluyen todos los sistemas críticos de la entidad e informa a los responsables del estado diario de las copias.

El Ayuntamiento ha decidido focalizar esfuerzos en mejorar las pruebas de restauración, consciente de que este tipo de pruebas son claves para garantizar la recuperación de los sistemas en caso de incidentes. Para ello, se ha anexado al procedimiento un *log* de sistemas restaurados, que incluye el sistema a restaurar, los datos, la fecha, la duración de la restauración, los motivos y los responsables de cada prueba planificada de restauración.

Adicionalmente, se ha elaborado un plan de recuperación de desastres que describe la restauración total en el caso de incidentes graves.

El único punto que se recomendó mejorar durante el trabajo de revisión anterior fue mantener una copia de los datos críticos desconectada o aislada de la red corporativa. El Ayuntamiento ha dado solución a esta recomendación implantando dos medidas: por una parte, el *software* de copias permite la inmutabilidad de estas, es decir, garantizan la integridad de los datos impidiendo que ningún usuario o proceso modifique los datos originales; por otra, se han separado los usuarios del dominio de todo el sistema de copias. Adicionalmente, la inmutabilidad de las copias de seguridad ha sido auditada por un tercero para corroborar su funcionamiento.

Además de lo anterior, se ha completado el sistema de copias de seguridad con un sistema deduplicador de copias, que mejora las copias gestionando de manera eficiente aspectos como el espacio de almacenamiento (evita datos duplicados, comprime los datos) o la reducción de la carga de la red.

La valoración global del control es que el Ayuntamiento alcanza un **índice de madurez del 89,0%**, que se corresponde con un **nivel de madurez *N3*, *proceso definido***; es decir, los procesos de control implantados están estandarizados y formalmente documentados. Esto representa un **índice de cumplimiento del CBCS 7 del 100%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 75,5%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*. Por tanto, se ha producido una mejora de 13,5 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

Durante la revisión de la normativa realizada en el trabajo de auditoría anterior, el Ayuntamiento se encontraba realizando diversas acciones encaminadas al cumplimiento del ENS y a lo establecido por la normativa en materia de protección de datos de carácter personal.

En el informe anterior se recomendó al Ayuntamiento realizar las auditorías que el propio ENS prevé y publicar en sede la documentación y distintivos correspondientes. Sin embargo, previamente a la realización de una auditoría del ENS, el Ayuntamiento ha priorizado la implantación de las medidas de seguridad necesarias.

Aunque la mejora en los distintos controles de ciberseguridad es de notable consideración, los trabajos deben continuar hasta realizar las auditorías de cumplimiento previstas en el ENS para obtener el certificado de conformidad.

Cumplimiento del RGPD

Respecto a la protección de datos de carácter personal, el Ayuntamiento ha dado continuidad a los trabajos que venía cursando durante el periodo de revisión.

Se han realizado revisiones de adecuación en distintas áreas y se realiza un seguimiento de sugerencias e incidencias por parte del DPD.

Adicionalmente, se ha evidenciado una responsabilidad proactiva en esta materia, dado que se realizan auditorías anuales por áreas priorizando aquellas en las que los datos son más sensibles. Al finalizar cada ejercicio, se emite un informe con todas las actuaciones realizadas.

Cumplimiento legalidad del registro de facturas

Se han realizado las correspondientes auditorías.

Indicadores

En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad incluidos en la revisión alcanza un **índice de madurez del 80,0%**, que se corresponde con un **nivel de madurez N3**, que indica que existe un razonable grado de adecuación a la

normativa. La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,0%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*. Por tanto, se ha producido una mejora de 20,0 puntos en este índice, aunque existen varios aspectos antes señalados relativos al cumplimiento de legalidad que deben ser subsanados.

Gobernanza de ciberseguridad

El Ayuntamiento de Benidorm tiene establecida una aceptable gobernanza de la seguridad de la información.

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

Si bien en la auditoría hemos observado la existencia de un aceptable nivel de compromiso y concienciación con la ciberseguridad por parte de los gestores y responsables de las áreas implicadas, es importante que exista un buen nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento.

Hemos observado la adecuada gobernanza en el Ayuntamiento en aspectos que permiten el establecimiento de un sistema de gestión de la seguridad de la información (SGSI) efectivo, como son los siguientes:

- **Existencia de un marco normativo y procedimental formalmente aprobado**, incluida la existencia de políticas de seguridad de la información formalmente asumidas por la organización.

- **La existencia de determinados roles clave en la organización, como el responsable de seguridad**.

No obstante, aunque existe un **comité de seguridad**, órgano imprescindible para coordinar la seguridad de la información en la entidad y que incluye representación de las áreas de la organización afectadas, este no se reúne periódicamente. Es necesario que se retomen las reuniones del comité de seguridad, dado que son los órganos de gobierno los que ostentan la responsabilidad de liderar y ser ejemplarizantes en sus acciones y decisiones, como parte de un proceso de concienciación de la entidad.

Como control compensatorio, hemos constatado la implicación proactiva del responsable del departamento TIC, manteniendo semanalmente reuniones con el responsable de seguridad, con objeto de mantenerse mutuamente al corriente del estado de las tareas pendientes, incidentes, próximas actuaciones, etc.

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.

Protección de interfaces para restringir el acceso de dispositivos físicos no autorizados

La entidad ha establecido un control basado en la aplicación de determinadas configuraciones básicas de seguridad en los interfaces de los dispositivos de red, en la gestión escrita de tomas y servicios de red y en la realización de revisiones periódicas.

Si bien la solución no proporciona protección frente a amenazas avanzadas, sí permite impedir la conexión de dispositivos no autorizados por error o por ataques básicos, proporcionando un cierto nivel de seguridad a un reducido coste de implementación y gestión.

Además de la protección de interfaces de red, el departamento restringe el acceso a los discos locales y a los dispositivos USB en todas las conexiones de escritorios virtualizados. También se restringe el acceso a dispositivos USB desde algunos dispositivos de la policía.

Los procedimientos representan con fidelidad la realidad de los procesos de control implantados

La entidad cuenta con un conjunto de procedimientos de seguridad que disponen del nivel de detalle y completitud requerido y además representan con fidelidad la realidad de los controles implantados.

La elaboración, por parte de los propios responsables y técnicos del departamento de informática, de documentos que describen los procesos de control establecidos facilita en gran medida la repetitividad de las acciones, con independencia de los técnicos que las ejecuten, y garantiza la consistencia de las actuaciones, tal y como se define para los controles que disponen de un nivel *N3, proceso definido*.

Dichos procedimientos no incluyen información genérica de utilidad limitada, y se ha evitado utilizar modelos estandarizados no adaptados a la entidad.

Auditorías externas

El departamento de informática realiza auditorías a determinados sistemas o características para garantizar su funcionamiento.

Ejemplo de ello ha sido una auditoría aportada sobre la inmutabilidad de las copias de seguridad, característica que ha sido implantada y de la que se ha auditado su correcto funcionamiento.

Adicionalmente, el Ayuntamiento contrata auditorías técnicas como las realizadas en *hacking* ético.

Seguridad perimetral mejorada

Un *sandbox* (o caja de arena) es un entorno de pruebas aislado que permite ejecutar aplicaciones peligrosas o dudosas sin riesgo de poner en peligro otros sistemas de la organización.

El departamento ha implantado dos herramientas de distintos fabricantes con objeto de analizar el correo electrónico y la navegación, con lo que se garantiza un doble análisis de cualquier fichero sospechoso.

Además, el perímetro de la red del Ayuntamiento cuenta con dos *firewalls* de distintos fabricantes, permitiendo alta disponibilidad y garantizando un nivel adicional de seguridad en la entrada y salida de conexiones.

SIEM mejorado

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

El SIEM ha sido mejorado integrando los eventos publicados en Open Threat Exchange (OTX), base de datos de amenazas pública alimentada por varias fuentes. Esta integración permite la detección temprana y prevención de incidentes de ciberseguridad.

Adicionalmente, el SIEM es revisado 24/7 por la empresa adjudicataria a tal efecto, se completa con el listado de amenazas de la propia empresa, emite informes que se revisan diariamente y se realiza copia de seguridad de sus eventos.

Vigilancia digital

La vigilancia digital es un servicio de rastreo de información y detección de amenazas basada en inteligencia artificial, proporcionando alertas a quienes analizan dicha información. Dada su importancia, el Ayuntamiento ha decidido implantar Trillion, que junto con los reportes del CSIRT-CV alertan al Ayuntamiento de incidencias como la vulneración de credenciales de sus cuentas o el registro de dominios semejantes.

Prevención de ransomware

Además de la herramienta microCLAUDIA del CCN, el Ayuntamiento completa la prevención contra el *ransomware* con otra herramienta, InterceptX de Sophos, instalada en los equipos y que es capaz de detectar encriptación de ficheros por *ransomware* y parar los servicios del sistema infectado, evitando que la infección se propague.

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

ENS: Esquema Nacional de Seguridad

INES: Informe Nacional del Estado de la Seguridad

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

PSI: Política de seguridad de la información

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de gestión de seguridad de la información

SIC: Sistemas de información y comunicaciones

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

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

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

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

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

Correlador de eventos: Correlar es el proceso de comparar diferentes fuentes de información de eventos, dando de esta manera sentido a eventos que, analizados por separado, no lo tendrían o pasarían desapercibidos. Un SIEM *(security information and event management)* o sistema de gestión de información y eventos de seguridad, va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes mediante técnicas de correlación compleja de eventos.

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

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

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

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

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

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

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, el borrador previo del informe de fiscalización se discutió con la concejala delegada de Innovación y con el responsable del departamento de informática para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

Posteriormente, en cumplimiento del artículo 16 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y del artículo 55.1.c) del Reglamento de Régimen Interior de la Sindicatura de Comptes, así como del acuerdo del Consell de esta institución por el que tuvo conocimiento del borrador del informe de fiscalización correspondiente al ejercicio 2021, este se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

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

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

1. Todas las alegaciones han sido analizadas detenidamente.

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

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

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y del artículo 55.1.h) de su Reglamento de Régimen Interior y de los programas anuales de actuación de 2021 y 2022 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 15 de junio de 2022, aprobó este informe de fiscalización.

ANEXO I

Alegaciones presentadas

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

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

JUSTIFICANTE DE PRESENTACIÓN EN REGISTRO ELECTRÓNICO

NÚMERO DE REGISTRO 202203189	FECHA DE ENTRADA 07/06/2022 12:46
ÁREA Fiscalización - Alegaciones	PROCEDIMIENTO PAA2020/35 Seguimiento de las 11 auditorías de los controles básicos de ciberseguridad cuyo trabajo de campo se ha realizado en 2019 (una vez transcurrido un año desde su finalización)
DATOS DEL PRESENTADOR Nombre: E-mail: Entidad: BENIDORM	
FIRMA DIGITAL B3228E5D45A055F7AA435091AD73B2F972495718	
DOCUMENTOS ENVIADOS Fichero1: 25119496T_202267_Informe para alegaciones.pdf Fichero2: 25119496T_202267_Informe auditoria facturas Ayuntamiento de Benidorm 2019_compressed.pdf Fichero3: 25119496T_202267_Informe auditoria facturas Ayuntamiento de Benidorm 2020_compressed.pdf	

INFORME DE ALEGACIONES AL BORRADOR DEL INFORME DE SEGUIMIENTO DE LAS RECOMENDACIONES REALIZADAS EN EL INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE BENIDORM DEL AÑO 2019. SITUACIÓN A 31 DE DICIEMBRE DE 2021

Sr. Interventor

En relación con el borrador del informe de seguimiento de la auditoría de Ciberseguridad que llevó a cabo la Sindicatura de Comptes en el Ayuntamiento de Benidorm (PAA2020/35), he de manifestarle que en él quedan reflejadas fielmente las circunstancias de la seguridad de nuestra instalación informática.

No obstante, observo que en el apartado del CBCS. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD, respecto al cumplimiento de la legalidad del registro de facturas, se apunta que no se han aportado las auditorías correspondientes.

Durante el desarrollo de los trabajos de auditoría no fuimos conscientes de la necesidad de entregarlas, dado que -tratándose de una revisión- ya en la primera ya se había aportado la del año correspondiente.

Por esta razón, debemos remitirles los informes anuales de 2019 y 2020 de la “Evaluación del Cumplimiento de la Normativa de Morosidad y del Registro Contable de Facturas”. Con ello, espero quede subsanada esta carencia y se pueda reflejar en el informe definitivo, modificándose las referencias que aparecen en las páginas 9, 15 y 41, así como, en su caso, en las puntuaciones calculadas.

Benidorm,

Jefe del Departamento de Informática

ANEXO II

Informe sobre las alegaciones presentadas

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

Mediante el escrito de esta Sindicatura de 25 de mayo de 2022 se remitió al Ayuntamiento de Benidorm el borrador del Informe de seguimiento de recomendaciones para que efectuase las alegaciones que considerase oportunas. Con fecha 9 de junio se recibieron por el registro electrónico las alegaciones formuladas y respecto a estas se señala lo siguiente:

Alegación única

Apartado "Cumplimiento normativo y gobernanza de ciberseguridad", del borrador del Informe, en el que se señala que no se han aportado las auditorías del registro de facturas

Comentarios

En la alegación realizada por el Ayuntamiento se incluyen los informes de auditoría del registro de facturas de los ejercicios 2019 y 2020, por lo que se modifica el contenido del Informe.

Consecuencias en el Informe

Se modifican los índices de madurez y cumplimiento del CBCS 8, cuadro 1, que pasan a ser 80,0% y 100,0% respectivamente.

Se modifican los índices de madurez y cumplimiento generales, en el segundo párrafo del apartado 4 (pasa a ser 81,4%), y cuadro 1, que pasan a ser 81,4% y 96,8% respectivamente.

El índice de cumplimiento general del segundo párrafo tras el cuadro 1 pasa a ser 96,8%.

Se modifica el gráfico 1 y se adapta a la nueva puntuación del CBCS 8.

Se elimina la recomendación 11 (era nueva de este informe), del apartado 5.

Se modifica el texto "No se incluyen los puntos 9 y 11 anteriores, ya que son medidas de obligado cumplimiento" del párrafo anterior al gráfico 2, que queda así:

> "No se incluye el punto 9 anterior, ya que es una medida de obligado cumplimiento".

En el apéndice 2, los siguientes apartados del CBCS 8, "Cumplimiento normativo y gobernanza de ciberseguridad", quedan redactados así:

> **"Cumplimiento legalidad del registro de facturas**
>
> Se han realizado las correspondientes auditorías.
>
> **Indicadores**
>
> En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad incluidos en la revisión alcanza un **índice de madurez del 80,0%**, que se corresponde con un **nivel de madurez N3**, que indica que existe un razonable grado de adecuación a la normativa. La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,0%, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*. Por tanto, se ha producido una mejora de 20,0 puntos en este índice, aunque existen varios aspectos antes señalados relativos al cumplimiento de legalidad que deben ser subsanados."

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 ciberseguridad Ayuntamiento Benidorm en 2019 - SEFYCU 3346814

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 WMR2 3C2V MJAQ PT4L

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 - 28/06/2022 7:46 VICENT CUCARELLA TORMO