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 SANT VICENT DEL RASPEIG DEL AÑO 2020

Situación a 31 de diciembre de 2021

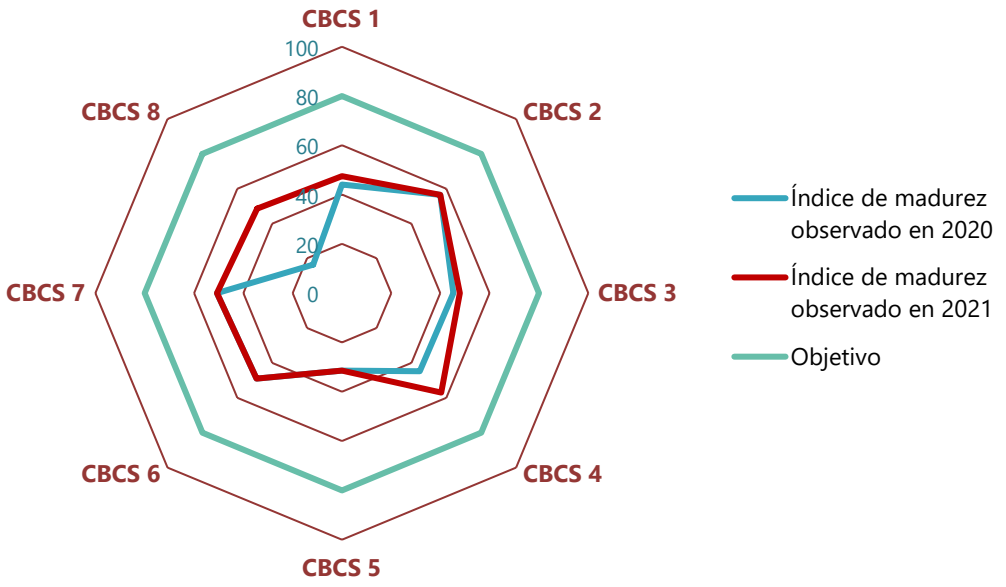
RESUMEN

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

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

Conclusiones

El Ayuntamiento únicamente ha atendido de forma parcial algunas de las recomendaciones de nuestro anterior informe, por lo que el índice de madurez general actual alcanza un 48,5%, y solo ha mejorado levemente desde el 42,3% valorado en la auditoría de 2020. Por lo tanto, el índice de madurez general de los controles básicos de ciberseguridad actual es muy deficiente y refleja un nivel de riesgo inaceptable, lejos del 80% requerido por el ENS.



El Ayuntamiento debe adoptar las medidas necesarias para alcanzar los niveles exigidos por el Esquema Nacional de Seguridad para la protección de los sistemas de información, especialmente en aquellos controles que presentan deficiencias significativas.

El Ayuntamiento de Sant Vicent del Raspeig no tiene establecida una adecuada gobernanza de la ciberseguridad, situación que debe ser subsanada. Los órganos de gobierno deben aprobar normas y procedimientos en relación con la seguridad de la información aplicables a toda la organización por igual y reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

Es preciso que el comité de seguridad de la información, órgano imprescindible para coordinar dicha seguridad en la entidad, se reúna regularmente, con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna. Los roles definidos en la política correspondiente del Ayuntamiento deben definirse correctamente y ejercer sus funciones de manera efectiva. Además, es necesaria la implantación, en todos los niveles del Ayuntamiento, de una cultura en materia de ciberseguridad, impulsada por la dirección en forma de planes estratégicos que definan objetivos y medidas concretas, además de la formación y concienciación de los trabajadores.

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

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

NOTA

Este resumen pretende ayudar a la comprensión de los resultados de nuestro informe y facilitar la labor a los lectores y a los medios de comunicación. Recomendamos 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 Sant Vicent del Raspeig del año 2020

Situación a 31 de diciembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

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

En la guía de auditoría GPF-OCEX 5311, "Ciberseguridad, seguridad de la información y auditoría externa", del *Manual de fiscalización* de la Sindicatura de Comptes, se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las Administraciones públicas, razón por la que los auditores públicos les deben prestar cada vez más atención. En línea con lo anterior, **en el Plan Estratégico de la Sindicatura de Comptes para el periodo 2019-2022 se señala 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 18 de junio de 2020 el Consell de la Sindicatura de Comptes aprobó el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Sant Vicent del Raspeig, Ejercicio 2020. Posteriormente, el Consell de la Sindicatura incluyó en los programas anuales de actuación de 2021 y 2022 realizar un trabajo de seguimiento de la situación de los controles básicos de ciberseguridad de ese ayuntamiento y de los otros 14 ayuntamientos analizados.

La necesidad de una adecuada ciberhigiene

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 Sant Vicent del Raspeig, ejercicio 2020.

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

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

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

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

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

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

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

4. CONCLUSIONES

El índice de madurez general de los controles básicos de ciberseguridad es muy deficiente y refleja un nivel de riesgo inaceptable. La entidad debe adoptar medidas para reconducir la situación.

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el **índice de madurez general** en la gestión de los controles básicos de ciberseguridad alcanza un **48,5%**, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada.

El Ayuntamiento únicamente ha atendido de forma parcial algunas de nuestras recomendaciones, por lo que el índice de madurez general solo ha mejorado levemente desde el 42,3% valorado en nuestra auditoría de 2020. Por lo tanto, el índice de madurez actual sigue siendo insuficiente para garantizar un adecuado grado de seguridad y alcanzar el 80% requerido por el ENS.

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

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

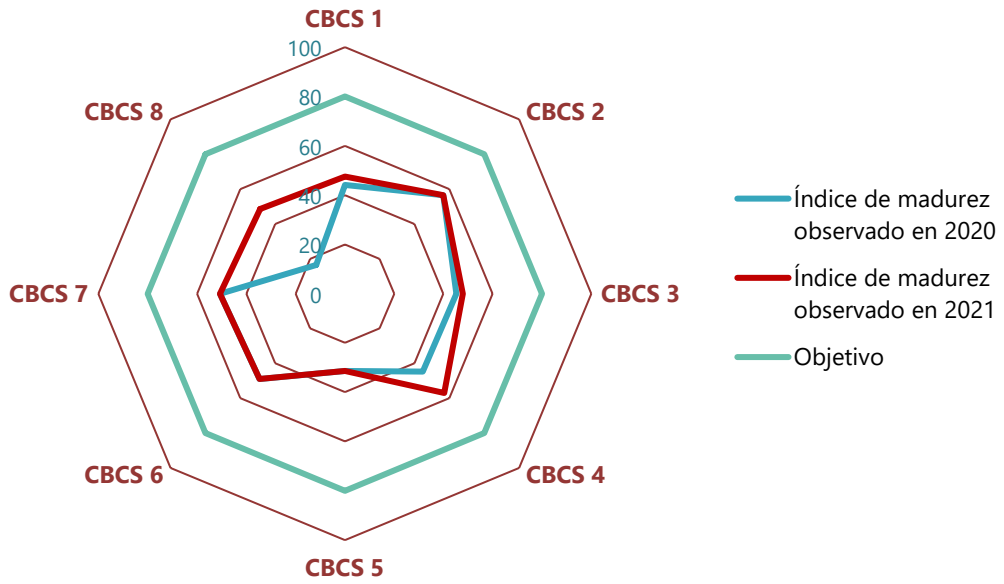
Control	2020			2021		
	Índice de madurez	Nivel de madurez	Índice de cumplimiento	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	*44,1%*	***N1***	*55,1%*	47,5%	**N1**	59,4%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	*56,5%*	***N2***	*70,6%*	56,5%	**N2**	70,6%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	*45,3%*	***N1***	*56,6%*	47,9%	**N1**	59,8%
CBCS 4 Uso controlado de privilegios administrativos	*44,7%*	***N1***	*55,9%*	57,0%	**N2**	71,3%
CBCS 5 Configuraciones seguras del *software* y *hardware*	*31,4%*	***N1***	*39,2%*	31,4%	**N1**	39,2%
CBCS 6 Registro de la actividad de los usuarios	*49,0%*	***N1***	*61,3%*	49,0%	**N1**	61,3%
CBCS 7 Copias de seguridad de datos y sistemas	*50,7%*	***N2***	*63,3%*	50,7%	**N2**	63,3%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	*16,5%*	***N1***	*20,6%*	48,5%	**N1**	60,6%
General	42,3%	***N1***	52,8%	48,5%	**N1**	60,7%

El índice de cumplimiento de los CBCS es del 60,7%, que resulta de comparar el indicador de madurez con el nivel requerido u objetivo que tiene el sistema según el ENS, que es el 80%. La comparación de los resultados detallados con los obtenidos en el año 2020 muestra una leve mejora desde el 52,8% de nuestro anterior informe. Cuatro de los controles han mejorado y cuatro de ellos no han experimentado ningún cambio.

El nivel de efectividad en los controles analizados sigue siendo muy deficiente y refleja un nivel de riesgo inaceptable. La entidad debe aplicar medidas para reconducir la situación y alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información, particularmente sobre los controles que presentan deficiencias significativas y no alcanzan el nivel de madurez N2 (CBCS 1, CBCS 3, CBCS 5, CBCS 6 y CBCS 8). En el apartado 5 se realizan las recomendaciones pertinentes con esa finalidad.

De una forma más sintética y gráfica, la situación observada de los controles, tanto en la presente auditoría como en la realizada en el año 2020, queda reflejada en el gráfico 1.

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



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

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

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

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

Si bien hemos podido verificar la existencia de cierto nivel de compromiso y concienciación con la ciberseguridad, existen carencias relevantes detalladas en el apéndice 2 que impiden que la gobernanza pueda considerarse efectiva.

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

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

El grado de cumplimiento de la normativa relativa a la seguridad de la información es muy deficiente.

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

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

Para subsanar las deficiencias de control identificadas por la Sindicatura en la presente auditoría y mejorar los niveles de control señalados en el apartado 4 anterior, reformulamos las recomendaciones que se efectuaron en la auditoría de 2020, considerando en su caso las mejoras realizadas desde entonces. El Ayuntamiento deberá dedicar los esfuerzos y recursos necesarios para subsanar las deficiencias pendientes.

También se señalan las medidas para el cumplimiento de la legalidad que deben adoptarse.

Sobre el inventario y control de dispositivos físicos (CBCS 1)

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

2. Implantar soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.

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

3. Elaborar y aprobar un procedimiento que describa las acciones llevadas a cabo para la gestión integral del *software* de la entidad y establezca, además de las medidas ya implantadas, aspectos como las autorizaciones, revisiones periódicas, responsables, medidas que impidan la ejecución de aplicaciones no permitidas, etc. También es recomendable que el Ayuntamiento defina un plan de mantenimiento de la totalidad del *software* utilizado.

4. Identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte.

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

5. Documentar los controles actualmente existentes, completarlos y aprobar formalmente unos procedimientos, de manera que incluyan las acciones actualmente implantadas y que considere, como mínimo, los siguientes aspectos:

   - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas, el análisis previo a la entrada en producción de los sistemas y las acciones actualmente establecidas de seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad.

   - La priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

6. Completar y aprobar formalmente el procedimiento existente de gestión unificada de usuarios con privilegios de administración, estableciendo las directrices para todos los sistemas de la entidad y que incluya:

   - La eliminación de los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos. Cuando existan razones de índole técnico que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas.

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

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

7. Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el 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 las guías STIC de las series 400, 500 y 600 del CCN.

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

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

8. Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de la actividad de los usuarios, que especifique, como mínimo, los sistemas afectados, la

información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Para dicha revisión es aconsejable centralizarlos en sistemas dedicados a tal efecto.

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

9. Establecer, por parte de la corporación y en un procedimiento formalmente aprobado, las acciones llevadas a cabo para la gestión de copias de seguridad de datos y sistemas, especificando, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas de restauración y los requisitos de protección de las copias.

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

10. Implantar las medidas necesarias para dar cumplimiento a las disposiciones del Real Decreto que regula el ENS. Específicamente, el Ayuntamiento debe:

    - Elaborar una declaración de aplicabilidad y adoptar las medidas de seguridad allí descritas.

    - Realizar las auditorías previstas en el artículo 34 del Real Decreto 3/2010.

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

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

    - Realizar un análisis de riesgos sobre sus tratamientos de datos personales y, en su caso, las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD.

    - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD.

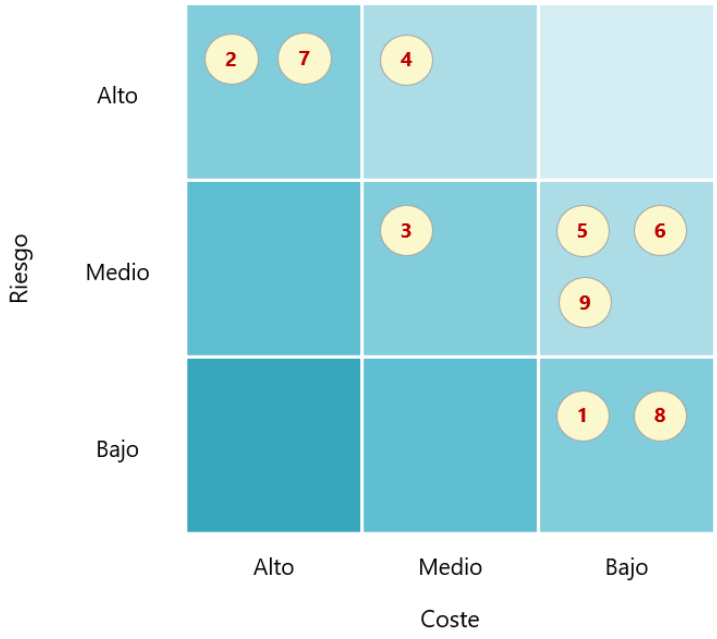
    - Planificar y ejecutar auditorías en materia de protección de datos.

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 2020, adaptando la relación riesgo/coste de cada recomendación y considerando las mejoras realizadas desde

la anterior revisión. No se incluyen los puntos 10 y 11 anteriores, ya que son medidas de obligado cumplimiento.

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



Actuaciones en curso

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

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

- El Ayuntamiento está elaborando un pliego de condiciones para la instalación de algunas de las herramientas del CCN, como la sonda SAT-INET para la detección temprana de incidencias de seguridad. Dicha implantación se incluirá en el plan de subvenciones destinadas a la transformación digital y modernización de las entidades locales en el marco del Plan de Recuperación, Transformación y Resiliencia.

- El departamento TIC ha iniciado una reorganización de las copias de seguridad, para lo que se ha incluido una cabina de cintas (copia desconectada).

Seguimiento de recomendaciones anteriores

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

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

Cuadro 2. Seguimiento de recomendaciones

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
1	Aprobar formalmente un procedimiento para la gestión del inventario y el control de activos físicos que recoja el proceso completo, incluyendo las revisiones periódicas de *hardware*, actualizando debidamente el inventario e incluyendo las fechas de dichas revisiones.	Sin variación.	**No aplicada**	Se mantiene la redacción.
2	Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Sin variación.	**No aplicada**	Se mantiene la redacción.
3	Elaborar y aprobar formalmente e implantar un procedimiento de gestión integral del *software* de la entidad que incluya: - La autorización de las instalaciones, la elaboración de listas de *software* autorizado (listas blancas), la implantación de las medidas técnicas que impidan la ejecución del no autorizado y la realización de revisiones periódicas del *software* instalado. - La definición de un plan de mantenimiento de la totalidad del *software* utilizado en el Ayuntamiento.	El Ayuntamiento ha aprobado una lista blanca de aplicaciones permitidas, sin embargo, la aprobación ha sido durante el ejercicio de 2022. Las acciones no han sido formalmente establecidas en un procedimiento aprobado por la corporación.	**Aplicada parcialmente**	Se modifica la redacción dada en 2020.
4	Identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte.	Sin variación.	**No aplicada**	Se mantiene la redacción.
5	Documentar los controles actualmente existentes, completarlos y aprobar formalmente unos procedimientos, de manera que incluyan las acciones actualmente implantadas y considere, como mínimo, los siguientes aspectos: - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas, el análisis previo a la entrada en producción de los sistemas y las acciones actualmente establecidas de seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad. - La priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.	El Ayuntamiento no ha realizado cambios significativos que mejoren la gestión de vulnerabilidades que se realizaba en la revisión anterior. Sin embargo, se han realizado determinadas acciones relacionadas con el control, como el despliegue de microCLAUDIA para la protección de equipos contra código dañino de tipo *ransomware*.	**Aplicada parcialmente**	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
6	Completar y aprobar formalmente el procedimiento existente de gestión unificada de usuarios con privilegios de administración, estableciendo 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.	El departamento de informática ha creado, para cada administrador de sistemas de la entidad, 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). Se han eliminado la mayoría de usuarios no nominativos de los sistemas. En los sistemas donde los usuarios son genéricos, su uso está controlado.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2020.
7	Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN. Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la revisión periódica de los cambios realizados, bien mediante procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.	Sin variación.	**No aplicada**	Se mantiene la redacción.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
8	Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de la actividad de los usuarios, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Para la revisión de *logs* es aconsejable la centralización de estos en sistemas dedicados a tal efecto.	Sin variación.	**No aplicada**	Se mantiene la redacción.
9	Completar y aprobar formalmente el procedimiento para la gestión de copias de seguridad de datos y sistemas, especificando, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, pruebas de restauración y los requisitos de protección de las copias.	La entidad no dispone de normativa aprobada que describa el proceso de realización de copias de seguridad implantado. No obstante, aunque se han realizado algunos cambios, estos están siendo implantados en fecha posterior al periodo revisado.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2020.
10	Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe: - Aprobar por parte del órgano superior competente la política de seguridad (PS) desarrollada. - Realizar la designación de las personas para los roles definidos en la política de seguridad y constitución de los órganos allí descritos. - Elaborar una declaración de aplicabilidad y adoptar las medidas de seguridad allí descritas. - Realizar las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010. - Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes.	Se ha desarrollado y aprobado la política de seguridad de la información. Se han designado los roles y se ha creado el comité de seguridad. Sin embargo, sigue sin existir una declaración de aplicabilidad que describa las medidas a implantar para el cumplimiento del ENS. Tampoco se han realizado las auditorías pertinentes ni se ha obtenido el distintivo correspondiente.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2020.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
11	En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular debe: - Comunicar a la Agencia de Protección de Datos el nombramiento del DPD. - Publicar y hacer accesible por medios electrónicos el registro de actividades del tratamiento. - Realizar un análisis de riesgos sobre sus tratamientos de datos personales y, en su caso, las evaluaciones de impacto de los tratamientos, conforme a los artículos 32.2 y 35 del RGPD. - Aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del RGPD. - Planificar y ejecutar auditorías en materia de protección de datos.	Se ha realizado la designación del DPD y se ha comunicado a la AEPD. Se ha elaborado, aprobado y publicado el registro de actividades del tratamiento de datos de carácter personal. Sin embargo, no se ha aportado el análisis de riesgos ni se realizan auditorías periódicas en materia de protección de datos.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2020.
12	Llevar a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.	Se ha llevado a cabo el informe de auditoría exigido por la normativa.	**Aplicada**	Se elimina la recomendación dada en 2020.

APÉNDICE 1
Metodología aplicada

Introducción

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

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

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

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

Aun cuando la adopción de medidas de seguridad adecuadas hace más resilientes a las organizaciones frente a los ciberataques, el análisis de los incidentes ocurridos que se realiza en los informes INES[3] del CCN revela que las organizaciones no siempre implementan ni tan siquiera las medidas más básicas que podrían haber evitado o mitigado el daño causado. Por otro lado, el hecho de que los ciberataques permanezcan en muchos casos sin ser detectados durante mucho tiempo puede ser evidencia de que las medidas básicas no están correctamente implementadas.

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

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

Objetivo de la auditoría

De acuerdo con lo previsto en los programas anuales de actuación de 2021 y 2022, nuestro objetivo ha sido realizar el seguimiento de la situación de los controles básicos de ciberseguridad y de las recomendaciones efectuadas en el *Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Sant Vicent del Raspeig, ejercicio 2020*, y obtener una seguridad limitada y concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación tanto sobre su diseño[4] como sobre su eficacia operativa[5] para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte, así como sobre el cumplimiento de la normativa básica relativa a la seguridad de la información.

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

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

Alcance

La auditoría se ha centrado en el análisis de la situación de los ocho CBCS:

CBCS 1	Inventario y control de dispositivos físicos
CBCS 2	Inventario y control de *software* autorizado y no autorizado
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades
CBCS 4	Uso controlado de privilegios administrativos
CBCS 5	Configuraciones seguras del *software* y *hardware*
CBCS 6	Registro de la actividad de los usuarios
CBCS 7	Copias de seguridad de datos y sistemas
CBCS 8	Cumplimiento normativo y gobernanza de ciberseguridad

Dada la naturaleza del objeto material a revisar –la gran amplitud, complejidad y diversidad de los sistemas de información de un ente local de tamaño grande– ha sido necesario

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

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

delimitar y concretar qué sistemas se iban a analizar. En este sentido, hemos analizado las aplicaciones que soportan los procesos de gestión contable y presupuestaria y la gestión tributaria y recaudatoria, así como los controles que tienen implantados.

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

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

Ámbito temporal

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

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

Metodología

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

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

Esta auditoría de los controles básicos de ciberseguridad ha sido realizada por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI), siguiendo la

metodología establecida en la guía práctica de fiscalización GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad (CBCS)".

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

La guía práctica de fiscalización de los OCEX 5313

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

El contenido de la GPF-OCEX 5313, fundamentalmente relacionado con la auditoría de la seguridad de los sistemas de información, es coherente con los postulados del ENS. No obstante, dada la amplitud del ENS, que está formado por 75 medidas de seguridad, para su inclusión en los CBCS se seleccionó una serie limitada de controles. Para escoger los más relevantes se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security (CIS)[6], que define, prioriza y clasifica veinte controles de ciberseguridad según su importancia para hacer frente a las ciberamenazas. Su ventaja principal es que están orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. Según el CIS, con carácter general, las organizaciones que apliquen solo los cinco primeros controles pueden reducir su riesgo ante ciberataques alrededor del 85%. Si se implementan los veinte controles el riesgo se puede reducir un 94%.

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

Alineación de los CBCS con el Esquema Nacional de Seguridad

Dado que el ENS es de obligado cumplimiento para todos los entes públicos, se ha tenido especial cuidado en que la metodología de auditoría de los controles básicos de ciberseguridad estuviera plenamente alineada con el ENS. Esa alineación facilita la realización de las auditorías de ciberseguridad por parte de la Sindicatura y coadyuva a la implantación del ENS en los entes auditados, ya que prácticamente todos los subcontroles o controles detallados que verifica la Sindicatura son requeridos por el ENS. De este modo,

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

los ocho controles básicos de ciberseguridad presentan una correspondencia (no exacta) con las siguientes referencias del ENS:

Cuadro 3. Los CBCS y el ENS

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

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

Los CBCS como medidas de ciberhigiene

La European Union Agency for Cybersecurity (ENISA) señala[7] que "la ciberhigiene es un principio fundamental relativo a la seguridad de la información y, como analogía con la higiene personal, es el equivalente a establecer simples medidas rutinarias para minimizar los riesgos de las ciberamenazas. La suposición subyacente es que las buenas prácticas de ciberhigiene pueden proporcionar inmunidad en las entidades que las aplican", reduciendo los ciberriesgos[8].

Sintetizando, la ciberhigiene se refiere al conjunto de prácticas y acciones básicas que una organización debe implantar para hacer frente a los riesgos de ciberseguridad más comunes y generalizados a los que se enfrenta hoy en día[9].

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

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

[9] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices*, 2017.

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.

Cuadro 4. Puntos de acción de ENISA

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

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

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

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

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

Cuadro 5. Los CBCS y sus subcontroles

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

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

Evaluación de los resultados del trabajo

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

Subcontroles

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

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

Cuadro 6. Evaluación de los subcontroles

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

Controles

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

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

Cuadro 7. Niveles de madurez

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

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

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

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

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

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

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indicadores globales

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

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

- El **índice de cumplimiento** analiza igualmente el nivel de madurez alcanzado, pero en relación con la exigencia aplicable en cada caso, teniendo en cuenta la categoría del sistema. Es decir, compara el índice de madurez con el nivel mínimo exigido para dicha categoría en el ENS, que en la presente auditoría es N3 (80%) para todos los casos.

Gobernanza de ciberseguridad

A los efectos del presente trabajo, se entenderá por gobernanza de la seguridad de la información y las comunicaciones o de ciberseguridad (términos que utilizamos de forma indistinta en este informe) el conjunto de responsabilidades y actividades realizadas por la alta dirección con el objetivo de proporcionar una dirección estratégica en esta materia, garantizar que se logren los objetivos, verificar que el riesgo se gestione adecuadamente y comprobar que se utilicen los recursos de la entidad de una forma responsable.[11]

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

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

Es más que una mera cuestión técnica, por lo que **exige un liderazgo efectivo, procesos sólidos y estrategias en consonancia con los objetivos de la organización**[12].

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

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

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

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

La implicación de los órganos superiores es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información o de ciberseguridad[13]. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información[14] que debe materializarse en aspectos tales como:

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

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

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

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

  La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[15], que se constituye como un órgano colegiado, algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad, y es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio. Su composición debe constar en la PSI.

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

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

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

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

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

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

Seguimiento de las recomendaciones

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

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

Cuadro 8. Situación de las recomendaciones

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

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

Comunicación y confidencialidad

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

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

APÉNDICE 2
Situación de los controles básicos de ciberseguridad

CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

Objetivo del control

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

Situación del control

El Ayuntamiento no ha realizado cambios significativos desde nuestra anterior auditoría para mejorar el inventario y control de dispositivos físicos y sigue sin disponer de un procedimiento aprobado que regule la gestión de activos físicos.

A raíz de nuestra auditoría, se revisaron las tomas de red, inutilizando aquellas que no debían estar operativas. De esta forma se proporciona cierto control sobre los dispositivos físicos que tienen acceso a la red, si bien dicha revisión no garantiza un control óptimo, existiendo soluciones más efectivas.

La valoración global del control existente sobre el inventario y control de dispositivos físicos es que la organización alcanza un **índice de madurez del 47,5%**, que se corresponde con un **nivel de madurez *N1, inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 1 del 59,4%**.

La situación del control en nuestra auditoría de 2020 mostraba un índice de madurez del 44,1%. Por tanto, se ha producido una leve mejora de 3,4 puntos en su índice de madurez.

CBCS 2. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO

Objetivo del control

Gestionar activamente (inventariar, revisar y corregir) todo el *software* en la red, de forma que solo se pueda instalar y ejecutar *software* autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

Situación del control

El Ayuntamiento no ha realizado cambios significativos para mejorar la gestión de *software* autorizado desde nuestra anterior auditoría.

El Ayuntamiento ha aprobado en 2022 una lista blanca de aplicaciones autorizadas, por lo que no se ha tenido en cuenta en el cálculo del índice de madurez.

No hay un procedimiento que describa la gestión integral de *software*, que establezca, además, aspectos como revisiones periódicas, responsables, medidas que impidan la ejecución de aplicaciones no permitidas, etc.

Existen servidores cuyos sistemas operativos se encuentran fuera del periodo de soporte del fabricante y se justifica su existencia porque albergan aplicaciones antiguas dependientes de dichos sistemas operativos. Se ha verificado que algunos de estos servidores tienen aplicadas medidas de protección adicionales (únicamente son accesibles desde determinadas IP dentro de la red). Sin embargo, la existencia de sistemas obsoletos pone en riesgo todo el sistema de información, puesto que no se reciben ni actualizaciones funcionales, ni parches, ni actualizaciones de seguridad.

La falta de documentación del proceso establecido, la existencia de sistemas obsoletos, la inexistencia de aplicaciones que permitan la gestión centralizada de *software* (instalaciones, revisiones, actualizaciones y parches, bloqueo de aplicaciones, etc.) o de un plan integral de mantenimiento de *software* hace que el control no pueda alcanzar niveles superiores.

La valoración global del control existente sobre el inventario y control de *software* es que el Ayuntamiento alcanza un **índice de madurez del 56,5%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento de este CBCS 2 del 70,6%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

Objetivo del control

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

Situación del control

El Ayuntamiento no dispone de un procedimiento formalmente aprobado que establezca el proceso de gestión de vulnerabilidades, desde su identificación hasta su resolución.

Si bien en el momento de finalizar la auditoría se estaba elaborando un pliego para la instalación de determinadas aplicaciones del CCN-CERT que permitirán mejorar la gestión de vulnerabilidades en la red corporativa, en 2021 únicamente se había desplegado la herramienta microCLAUDIA en los equipos de la entidad.

También ha sido realizada, por parte del CSIRT-CV, una auditoría de la red corporativa, pero este hecho no ha sido considerado en el cálculo de los índices de madurez por haberse realizado con posterioridad al 31 de diciembre de 2021.

El Ayuntamiento no ha realizado más cambios desde nuestra anterior auditoría, por lo que nuestras recomendaciones siguen vigentes.

Existe cierto nivel de control sobre la gestión de vulnerabilidades, siendo la valoración global del control de un **índice de madurez del 47,9%,** que se corresponde con un **nivel de madurez *N1, inicial/adhoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 3 del 59,8%**.

La situación del control en el informe realizado en el año 2020 mostraba un índice de madurez del 45,3% que se corresponde con un nivel de madurez *N1, inicial/adhoc*. Por tanto, se ha producido una leve mejora de 2,6 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

Se han implantado algunas mejoras para el inventario y el control de las cuentas de usuarios administradores desde nuestra anterior auditoría. El departamento de informática ha creado usuarios nominativos para la gestión de la mayoría de los sistemas revisados (sistema de virtualización, servidores, controlador de dominio, etc.), permitiendo la trazabilidad de las acciones y evitando así el uso de usuarios genéricos no nominativos. Sin embargo, todavía existen sistemas donde se utilizan los usuarios genéricos, como los *firewalls*, aunque únicamente son administrados por una persona.

El Ayuntamiento ya disponía de normativa para la creación y uso de contraseñas, que ha sido formalmente aprobada. El departamento de informática ha cambiado las contraseñas por defecto de todos los sistemas, aunque existen sistemas en los que los mecanismos de autenticación no son robustos, como las aplicaciones de contabilidad o recaudación.

Uno de los cambios más significativos ha sido la creación de usuarios nominativos para el personal del departamento TIC, distinguiendo entre el acceso a servidores o a equipos de usuario, además de sus usuarios locales. Además, se han creado usuarios nominativos con privilegios de administración sobre las máquinas de los usuarios.

Aunque se han realizado acciones para mejorar el control de los usuarios administradores, dichas acciones no están recogidas en un procedimiento formalmente aprobado.

Existe un cierto nivel de control sobre las cuentas con privilegios administrativos alcanzando la valoración global del control un **índice de madurez del 57,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han

sido formalizados documentalmente. Esto representa un **índice de cumplimiento de este CBCS 4 del 71,3%**.

La situación del control en el informe realizado en el año 2020 mostraba un índice de madurez del 44,7%, que se corresponde con un nivel de madurez *N1*. Por tanto, se ha producido una mejora de 12,3 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

No se han introducido mejoras respecto a la auditoría de 2020.

El Ayuntamiento disponía, durante nuestra auditoría anterior, de un procedimiento de gestión de cambios y configuración segura de sistemas que no había sido formalmente aprobado. Además, se aplicaban determinadas acciones relacionadas con la seguridad a los dispositivos y sistemas.

Sin embargo, el procedimiento anterior no estaba formalmente aprobado, los sistemas no se configuraban de manera que se garantizase la seguridad por defecto, ni existía un proceso de gestión de la configuración que notificase los cambios no autorizados en la configuración de los sistemas críticos de la entidad. Por estos motivos, mantenemos nuestras recomendaciones anteriores.

La valoración global del control se mantiene como en la anterior auditoría, en un **índice de madurez del 31,4%,** que se corresponde con un **nivel de madurez *N1, inicial/adhoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 5 del 39,2%**.

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

Hemos analizado los procedimientos aplicados en el Ayuntamiento para el control de la actividad de los usuarios en los sistemas y hemos verificado que siguen existiendo los mismos controles en funcionamiento vistos durante nuestro trabajo de auditoría de 2020.

Las actividades relacionadas con este control se aplican de manera informal y no existe un procedimiento aprobado que describa sobre qué sistemas se debe registrar la actividad de los usuarios, qué tipo de actividad registrar, responsables, gestión de derechos de acceso a los registros, tiempo de retención, copia de seguridad, revisiones, etc.

El Ayuntamiento disponía, durante la auditoría de 2020, de un sistema para la monitorización del estado de la red y sus dispositivos, aunque no era un proyecto acabado ni incluía todos los dispositivos críticos de la red. Durante la presente auditoría hemos observado que el proyecto no ha sido continuado por falta de recursos, según nos han informado.

El Ayuntamiento no dispone de una herramienta que permita la gestión centralizada de registros de actividad de los usuarios que recoja los eventos generados en los sistemas críticos de la entidad.

La situación del control no ha variado respecto del informe realizado en el año 2020 y la valoración global del control es de un **índice de madurez del 49,0%,** que se corresponde con un **nivel de madurez *N1, inicial/adhoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 6 del 61,3%**.

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 no ha aprobado un procedimiento que describa el proceso existente para el control de copias de seguridad de sus datos y sistemas. No obstante, se han implantado acciones para mejorar el control, aunque a 31 de diciembre de 2021 no estaban totalmente implementadas.

El Ayuntamiento ha adquirido una cabina de cintas únicamente accesible desde una máquina y durante el tiempo que dura el proceso de copia. Sin embargo, únicamente guarda los datos de una semana y, durante nuestro trabajo de revisión, se estaba trabajando en mejorar su utilidad.

Adicionalmente, se ha renovado la licencia del *software* de gestión de copias.

Aunque el departamento TIC ha realizado acciones enfocadas en mejorar las copias de seguridad, existen deficiencias que impiden alcanzar un nivel de madurez superior:

- Las acciones llevadas a cabo no están formalmente aprobadas en un procedimiento.
- No se realizan pruebas planificadas de recuperación.
- El número de días de los que se hacen copia es limitado.
- Las decisiones sobre las copias de seguridad dependen de la buena voluntad de los técnicos que las realizan.
- Las mejoras descritas anteriormente están en proceso de implantación y dicho trabajo no ha sido finalizado.

Es por estos motivos por los que se mantienen el nivel de madurez y las recomendaciones realizadas en el pasado informe de 2020.

La valoración global del control alcanza un **índice de madurez del 50,7%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento de este CBCS 7 del 63,3%**.

CBCS 8. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD

Objetivo del control

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

Situación del control

Cumplimiento del ENS

El Ayuntamiento ha realizado determinadas acciones que incrementan el nivel de cumplimiento exigido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

Durante el ejercicio de 2021, el Ayuntamiento creó y aprobó la política de seguridad de la Información. Además, se han establecido los roles en materia de seguridad y se ha creado el Comité de Seguridad de la Información, estableciendo formalmente sus funciones.

Aunque se han realizado acciones encaminadas al cumplimiento del ENS, el Ayuntamiento debe subsanar las carencias y cumplir las recomendaciones que siguen vigentes: declaración de aplicabilidad, realización de auditorías de cumplimiento y obtención del certificado de conformidad con el ENS.

Cumplimiento del RGPD

En cuanto al cumplimiento en materia de protección de datos personales, desde la revisión realizada en el año 2020, el Ayuntamiento ha subsanado algunas de las carencias detectadas.

El Ayuntamiento ha realizado la designación del DPD y lo ha notificado a la Agencia Española de Protección de Datos. El DPD es un órgano colegiado formado por la secretaria general y el responsable del departamento TIC. La asignación de múltiples tareas al responsable del departamento TIC puede suponer una limitación de su disponibilidad para todas sus obligaciones.

El Ayuntamiento ha elaborado y publicado el registro de actividades de tratamiento de datos personales. Sin embargo, no se ha realizado un análisis de riesgos ni se llevan a cabo auditorías periódicas sobre los sistemas en dicha materia.

Cumplimiento de la legalidad del registro de facturas

El Ayuntamiento ha realizado la auditoría de sistemas del registro de facturas exigida por la Ley 25/2013, de 27 de diciembre.

Indicadores

En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad incluidos en la revisión es que el Ayuntamiento alcanza un **índice de madurez del 48,5%**, que se corresponde con un **nivel de madurez N1,** que indica que existen incumplimientos significativos generalizados de la normativa, y hay aspectos que se deben mejorar.

La situación del control en el informe realizado en el año 2020 mostraba un índice de madurez del 16,5%, que se corresponde con un nivel de madurez *N2*. Por tanto, se ha producido una mejora de 32 puntos en el índice de madurez del control.

Gobernanza de ciberseguridad

El Ayuntamiento de Sant Vicent del Raspeig no tiene establecida una adecuada gobernanza de la seguridad de la información.

El Ayuntamiento ha elaborado y aprobado una política de seguridad de la información, definiendo los roles en esta materia y constituyendo el comité de seguridad, por lo que existe cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento y particularmente de los responsables de las áreas implicadas. Sin embargo, existen carencias relevantes que indican que la gobernanza no puede considerarse efectiva.

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

- Baja actividad del Comité de Seguridad de la Información, órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas del Ayuntamiento, que únicamente se ha reunido tres veces en 2021. En una entidad del tamaño de Sant Vicent del Raspeig y dada la complejidad de sus sistemas, el comité debería reunirse al menos mensualmente.

- Ausencia de un marco procedimental único formalmente aprobado. Aunque el Ayuntamiento ha desarrollado y aprobado un marco normativo (uso correcto de equipos, servicios, instalaciones, aplicaciones autorizadas, control físico de accesos, etc.), este debe completarse con documentos que detallen cómo se realizan las tareas habituales, responsables, reporte de comportamientos anómalos, etc. Este marco procedimental es requerido en el ENS para garantizar una efectiva organización global de la seguridad de la información.

- La falta de recursos en el departamento TIC, tanto económicos como de personal, para atender la problemática de la seguridad de la información. La carencia de personal ha sido reportada por el responsable del departamento y es atendida parcialmente mediante becas o contrataciones temporales, que no solucionan el problema.

- El responsable del departamento TIC tiene dedicación compartida entre múltiples tareas y competencias, como liderar el departamento, pertenecer al órgano colegiado de delegado de protección de datos (DPD) del Ayuntamiento o ser responsable de seguridad de la información.

  En una entidad del tamaño y complejidad del Ayuntamiento de Sant Vicent del Raspeig, la existencia de múltiples tareas asignadas al responsable del departamento TIC implican los siguientes riesgos:

  - Que su disponibilidad para tareas relacionadas con la seguridad de la información pueda verse limitada.

  - Que no disponga del tiempo suficiente para cumplir con las funciones de DPD, por el conflicto entre prioridades de sus distintas responsabilidades. El artículo 38 del RGPD, que establece que el DPD ha de participar "[…] de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales […]".

- Algunos de los roles en materia de seguridad de la información están desactualizados o incorrectamente asignados.

  - El responsable del sistema no pertenece al departamento TIC. La persona nombrada responsable del sistema ha sido ubicada en otro departamento, y este rol, de acuerdo con el ENS, debe ser del responsable "de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo", es

decir, son tareas del responsable del departamento TIC o de una persona que forme parte del mismo.

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

- La falta de una cultura de ciberseguridad en la entidad, representada por la falta de proyectos transversales que afecten a toda la organización, incluyendo:

  - Acciones para concienciar a todo el personal de la organización en materia de seguridad de la información.

  - Existencia de proyectos importantes que afectan a todo el sistema de información sin soporte económico, político o en forma de recursos humanos, cuyo éxito depende de la buena voluntad de los miembros del departamento TIC. Ejemplo de esto es el cambio del sistema de copias de seguridad o el intento de implantación de un sistema de monitorización.

- La inexistencia de planes estratégicos desarrollados por la corporación que establezcan un plan de acción y los objetivos necesarios para alcanzar los niveles exigidos por la normativa.

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

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

ENS: Esquema Nacional de Seguridad

INES: Informe Nacional del Estado de la Seguridad

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

PSI: Política de seguridad de la información

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de gestión de seguridad de la información

SIC: Sistemas de información y comunicaciones

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

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

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

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

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

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

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

EDR:[16] Un sistema EDR, sigla en inglés de *endpoint detection and response*, es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

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

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

Política de seguridad de la información: Es un documento de alto nivel que define lo que significa "seguridad de la información" en una organización de acuerdo con el artículo 11 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

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

breve, y que deje los detalles técnicos para otros documentos más precisos que ayuden a llevar a cabo lo propuesto: normas de seguridad y procedimientos de seguridad.

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

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

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

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, un borrador previo del Informe de auditoría se discutió con la secretaria general, la concejala de Nuevas Tecnologías y el responsable del área de informática y modernización para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

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

Transcurrido dicho plazo no se han recibido alegaciones.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y del artículo 55.1.h) de su Reglamento de Régimen Interior y de los programas anuales de actuación de 2021 y 2022 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 9 de noviembre de 2022, aprobó este informe de auditoría.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Infome seguimiento CBCS Sant Vicent 2020_cas - SEFYCU 3641920

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 Z9Q2 TCXW QWEZ CWJQ

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 - 21/11/2022 7:35 VICENT CUCARELLA TORMO