SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME SOBRE LAS ACTUACIONES REALIZADAS POR EL AYUNTAMIENTO DE SAN VICENTE DEL RASPEIG MEDIANTE LAS SUBVENCIONES DESTINADAS A LA TRANSFORMACIÓN DIGITAL Y MODERNIZACIÓN, EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA, Y DE SEGUIMIENTO DE LAS RECOMENDACIONES SOBRE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD

Situación a 31 de diciembre de 2023

Nuestras condolencias a los familiares de las víctimas de la DANA y nuestra solidaridad con todos los damnificados.

RESUMEN

La Unión Europea, con objeto de promover la recuperación económica y social tras la pandemia del coronavirus, dispuso de una serie de fondos destinados a programas de reforma e inversión para los siguientes años, conocidos como Fondos Next Generation EU, para cuya articulación el Gobierno de España impulsó el Plan de Recuperación, Transformación y Resiliencia (PRTR), alineado con los objetivos de los fondos EU y estructurado en distintas áreas, una de las cuales es la transformación digital y la modernización de la Administración pública.

Entre las líneas estratégicas del PRTR se encuentra la ciberseguridad y particularmente el proyecto prioritario denominado "Puesta en marcha de un Centro de Operaciones de Ciberseguridad".

Atendiendo a la importancia de estos mecanismos y a su potencial impacto sobre la ciberseguridad de las Administraciones locales, aspecto que viene siendo tratado por la Sindicatura de Comptes en los últimos años y que se encuentra incluido en su actual plan estratégico, hemos realizado un trabajo para evaluar la aplicación y ejecución de dichas subvenciones.

Adicionalmente, hemos realizado un trabajo de seguimiento de la situación de los controles básicos de ciberseguridad (CBCS) del Ayuntamiento de San Vicente del Raspeig respecto a la situación mostrada en las anteriores auditorías realizadas.

Conclusiones

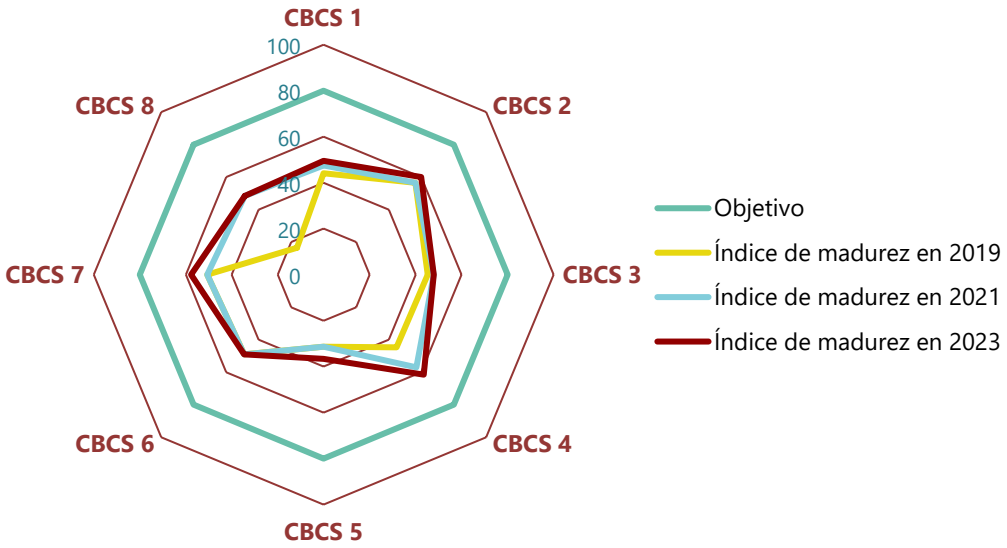
El Ayuntamiento de San Vicente del Raspeig no ha ejecutado en tiempo y forma los dos proyectos propuestos de la línea estratégica de transformación digital y modernización de la Administración pública del PRTR, y ha reintegrado los importes recibidos.

El Ayuntamiento no dispone de los recursos e infraestructura administrativa necesarios para gestionar este tipo de ayudas. Esta carencia supone un menoscabo en la capacidad del Ayuntamiento para captar, gestionar y justificar proyectos subvencionables y actúa como elemento disuasorio para la promoción de nuevos proyectos y la solicitud de subvenciones.

Sobre el Centro de Operaciones de Ciberseguridad (SOC), el Ayuntamiento no ha ejecutado el proyecto "Puesta en marcha de un Centro de Operaciones de Ciberseguridad", ni dispone de los recursos necesarios para la puesta en operación de un SOC. No obstante, el Ayuntamiento se ha adherido al Plan de Choque de Ciberseguridad de la Generalitat y ha desplegado herramientas proporcionadas por la Dirección General de Tecnologías de la Información y las Comunicaciones de la Generalitat, mejorando el nivel de seguridad general.

Sobre el estado de los CBCS, apenas se han realizado progresos desde nuestra anterior auditoría. El índice de madurez general de los controles muestra un valor del 51,3% (48,5%

en 2021) que continúa siendo muy deficiente y debe mejorar para alcanzar los niveles exigidos por el Esquema Nacional de Seguridad. En el siguiente gráfico se muestra la situación actualizada de los controles, así como la situación en las dos anteriores auditorías.



El Ayuntamiento de San Vicente 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.

Recomendaciones

Para subsanar las deficiencias de control relativas a los CBCS identificadas en la presente auditoría y mejorar los niveles de control, reformulamos las recomendaciones que se efectuaron en la anterior auditoría, considerando, en su caso, las mejoras realizadas desde entonces. De las once recomendaciones realizadas en ese informe, seis no se han atendido y cinco lo han sido solo parcialmente.

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.

NOTA

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

Informe sobre las actuaciones realizadas por el Ayuntamiento de San Vicente del Raspeig mediante las subvenciones destinadas a la transformación digital y modernización, en el marco del Plan de Recuperación, Transformación y Resiliencia, y de seguimiento de las recomendaciones sobre los controles básicos de ciberseguridad.

Situación a 31 de diciembre de 2023

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.

Plan de Recuperación, Transformación y Resiliencia

El Plan de Recuperación, Transformación y Resiliencia (PRTR) se estructura en distintas áreas, una de las cuales es la transformación digital y la modernización de la Administración pública, que se encuentra recogida en el Componente 11 del Plan (en adelante "el Componente 11").

Para desarrollar estas ayudas, mediante la Orden TER/1204/2021, de 3 de noviembre, se aprobaron las bases reguladoras y se efectuó la convocatoria correspondiente a 2021 de subvenciones destinadas a las entidades locales, en particular las destinadas a los municipios de más de 50.000 habitantes, así como los de población inferior que tengan la consideración de capital de provincia. La ejecución de estas ayudas debía realizarse hasta el 31 de diciembre de 2023.

En el artículo 5 de la citada orden se estipula que las entidades deberán destinar las subvenciones contempladas en el Componente 11 a financiar proyectos de modernización y digitalización que se enmarquen en alguna de las cinco líneas estratégicas enunciadas en el apartado 2 de dicho artículo. En los apartados 3 y 4 se establece que las entidades beneficiarias priorizarán los proyectos, estableciendo como "Prioridad 1. Proyecto en la Línea 5. Puesta en marcha de un Centro de Operaciones de Ciberseguridad", y que este proyecto deberá incluirse necesariamente en las propuestas. En el caso de que la entidad beneficiaria dispusiera ya de proyectos en marcha relacionados con aquel, o tuviera cubiertas las necesidades en este ámbito, quedará exenta, pudiendo dedicar la financiación contemplada a la priorización establecida en el apartado 3 o, en su caso, a las actuaciones subvencionables recogidas en el apartado 2 de ese artículo.

Los centros de operaciones de ciberseguridad (SOC, por sus siglas en inglés) que se desplieguen formarán parte de la Red Nacional de Centros de Operaciones de Ciberseguridad (RNS).

El interés en fiscalizar el Componente 11 del PRTR es doble. Por una parte, guarda una relación directa con la problemática planteada por la ciberseguridad y los controles de

ciberseguridad, ya que una de las prioridades fundamentales de las ayudas es mejorar su situación. Por otra parte, el PRTR es un tema de gran sensibilidad y los órganos de control deben velar por que se realice una gestión de los fondos recibidos acorde con las normas que los regulan, tanto desde el punto de vista de cumplimiento estricto de las normas como de una gestión eficaz de las ayudas.

El Ayuntamiento de San Vicente del Raspeig solicitó ayudas para los proyectos recogidos en el cuadro 1, en euros.

Cuadro 1. Ejecución de los proyectos financiados con el PRTR

Proyectos ejecutados	Importe solicitado	Importe concedido	Situación de los expedientes a 31-12-2023
Refuerzo de la ciberseguridad en los sistemas informáticos del Ayuntamiento de San Vicente del Raspeig	91.355,00	91.355,00	Se ha reintegrado por falta de justificación
Mejora de la infraestructura y sistemas informáticos del centro de proceso de datos del Ayuntamiento de San Vicente del Raspeig	70.000,00	70.000,00	Se ha reintegrado por falta de justificación
	161.355,00	**161.355,00**	

Ciberseguridad

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 de la ciberseguridad 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, la Sindicatura considera a la ciberseguridad como una de las áreas de alto riesgo y prioritarias para llevar a cabo la tarea fiscalizadora.

Por este motivo, la Sindicatura de Comptes ha realizado informes de auditoría de ciberseguridad en 2019 y de seguimiento en 2021 sobre los 15 ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes. El 18 de junio de 2020 el Consell de la Sindicatura de Comptes aprobó el Informe de auditoría de los controles básicos de ciberseguridad (CBCS) del Ayuntamiento de San Vicente del Raspeig, sobre el ejercicio 2019. Posteriormente, el 9 de noviembre de 2022 el Consell de la Sindicatura aprobó el informe sobre la situación de esos controles a 31 de diciembre de 2021 y el seguimiento de las recomendaciones del primer informe. Todos estos informes están accesibles en nuestra página web.

Transcurridos dos años del anterior informe y de acuerdo con las prioridades establecidas por la Sindicatura, hemos realizado un informe sobre el seguimiento de la situación de los CBCS a 31 de diciembre de 2023 y del grado de implantación de nuestras recomendaciones para mejorar la situación del Ayuntamiento de San Vicente del Raspeig frente a los ciberriesgos.

Objetivos de la auditoría

El primer objetivo ha consistido en evaluar la correcta aplicación y ejecución de las subvenciones del Componente 11 del PRTR para la transformación digital y la modernización de la Administración realizada por el Ayuntamiento de San Vicente del Raspeig.

El segundo objetivo ha consistido en realizar un seguimiento de las medidas adoptadas por el Ayuntamiento para atender las recomendaciones realizadas en nuestros anteriores informes sobre los controles básicos de ciberseguridad y valorar el nivel e índice de madurez actualizado a 31 de diciembre de 2023 de dichos controles.

Metodología

Para alcanzar el primer objetivo hemos aplicado la guía MFSC-1733, "Auditorías focalizadas inmediatas"[1], de nuestro *Manual de fiscalización*. Particularmente hemos:

- obtenido conocimiento sobre la gestión realizada de las subvenciones a los proyectos incluidos en el Componente 11 y la aplicación de las prioridades establecidas en la Orden TER/1204/2021, particularmente sobre la "Prioridad 1. Puesta en marcha de un Centro de Operaciones de Ciberseguridad",

- revisado las memorias de los proyectos subvencionados (incluyendo resumen ejecutivo, hitos y objetivos para el seguimiento), y todos los documentos que se han considerado relevantes para los objetivos de la auditoría, y verificado que el objeto de estos se ajusta a los requerimientos del Componente 11,

- revisado los justificantes de cumplimiento de objetivos y los justificantes del cobro, entre otros,

- realizado entrevistas personales y solicitado cumplimentar cuestionarios para analizar si se ha efectuado adecuadamente la gestión administrativa y la justificación de la aplicación de los fondos a los proyectos previstos,

- valorado la idoneidad de los recursos administrativos puestos a disposición por la corporación para una gestión administrativa eficiente de estos fondos y la coordinación municipal con los departamentos beneficiarios de estos,

- verificado si el proyecto para puesta en marcha de un centro de operaciones de ciberseguridad se ha ejecutado correctamente y se han realizado las integraciones con los SOC de referencia.

[1] Actualizada por la GPF-OCEX 1810, "Auditorías focalizadas inmediatas".

La auditoría no ha incluido una revisión de cumplimiento de la legalidad en la gestión de las ayudas, objetivo que es abordado, en su caso, en otros informes de la Sindicatura.

En relación con el segundo objetivo de nuestra auditoría, hemos analizado las acciones realizadas para atender a nuestras recomendaciones y la evolución de la situación de los controles desde el 31 de diciembre de 2021, fecha de nuestra anterior auditoría, y hemos actualizado las recomendaciones para adaptarlas a la situación a 31 de diciembre de 2023. Para ello, hemos utilizado la metodología establecida en la guía práctica de fiscalización GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad", y en la guía GPF-OCEX 1735, "Las recomendaciones y su seguimiento", de nuestro *Manual de fiscalización*. En nuestros informes anteriores se incluía con detalle la metodología utilizada y en el apéndice 3 sintetizamos los criterios de evaluación aplicados.

Con carácter general, la metodología, técnicas y demás procedimientos se realizarán de acuerdo con las distintas guías prácticas de fiscalización incluidas en el *Manual de fiscalización* de la Sindicatura de Comptes.

Confidencialidad

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 al 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.

2. CONCLUSIONES

Sobre la gestión de los fondos del PRTR

El Ayuntamiento no ha ejecutado los proyectos del Componente 11 subvencionados y ha reintegrado los importes recibidos.

El motivo de la no ejecución es que el Ayuntamiento no dispone de los recursos e infraestructura administrativa necesarios para gestionar este tipo de ayudas. Esta carencia supone un menoscabo en la capacidad para captar, gestionar y justificar proyectos subvencionables y actúa como elemento disuasorio para la promoción de nuevos proyectos y la solicitud de subvenciones.

Basamos nuestras conclusiones en que:

- Los proyectos inicialmente propuestos no se han ejecutado, ya que el Ayuntamiento no dispone de los recursos e infraestructura administrativa necesarios para proporcionar el apoyo adecuado a los departamentos para la ejecución de proyectos subvencionados por el PRTR y otras líneas de financiación europeas.

Con fecha 27 de noviembre de 2023, se acordó la devolución de los fondos recibidos correspondiente al pago anticipado de la subvención, más los intereses de demora a favor de la Dirección General de Cooperación Autonómica y Local.

- La carencia de un departamento o servicio especializado que proporcione soporte administrativo especializado para la gestión de fondos europeos, que generan mucha burocracia, supone un menoscabo en la capacidad del Ayuntamiento para captar, gestionar y justificar proyectos subvencionables.

  Debido a esta carencia, el departamento de informática, beneficiario de los proyectos designados como subvencionables del Componente 11, línea 5, ha sido encargado de la gestión administrativa, pero su lógica falta de recursos humanos con conocimientos y experiencia en la gestión de fondos europeos ha derivado en incumplimientos que han causado la pérdida de financiación.

  Además, la obligación de gestionar administrativamente los proyectos por parte de los departamentos receptores de los proyectos subvencionables, sin el personal adecuado actúa como elemento disuasorio para la promoción de nuevos proyectos y la solicitud de subvenciones.

Sobre el Centro de Operaciones de Ciberseguridad (SOC)

La entidad no ha ejecutado el proyecto "Puesta en marcha de un Centro de Operaciones de Ciberseguridad", ni dispone de los recursos necesarios para la puesta en operación de un SOC; pero se ha adherido al plan de choque de ciberseguridad de la Generalitat.

Basamos esta conclusión en que:

- La entidad no dispone de los recursos necesarios ni ha contratado los servicios equivalentes para la puesta en operación de un SOC. No obstante, el Ayuntamiento se ha adherido al Plan de Choque de Ciberseguridad de la Generalitat y ha desplegado herramientas proporcionadas por la Dirección General de Tecnologías de la Información y las Comunicaciones de la Generalitat (DGTIC), mejorando el nivel de seguridad general.

- La entidad no se ha integrado/federado con el SOC del Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV), dado que aún no se ha formalizado e iniciado el proceso de integración por parte de la DGTIC.

Sobre el estado de los controles básicos de ciberseguridad (CBCS)

Apenas se han realizado progresos desde nuestra anterior auditoría. El índice de madurez general de los CBCS (51,3%) sigue siendo muy deficiente, refleja un nivel de riesgo inaceptable y está alejado del objetivo marcado por el Esquema Nacional de Seguridad (ENS) (80,0%). El Ayuntamiento debe adoptar medidas para reconducir la situación.

Como resultado del trabajo realizado, cabe concluir que los controles básicos de ciberseguridad alcanzan un **índice de madurez general del 51,3%**, que se corresponde con un **nivel de madurez *N2, reproducible, pero intuitivo***; es decir, existen procedimientos de control, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

El Ayuntamiento ha atendido de forma parcial nuestras recomendaciones y el índice de madurez general apenas ha mejorado desde el 48,5% identificado en nuestra anterior auditoría, y 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 2.

Cuadro 2. Índice de madurez de los controles básicos de ciberseguridad

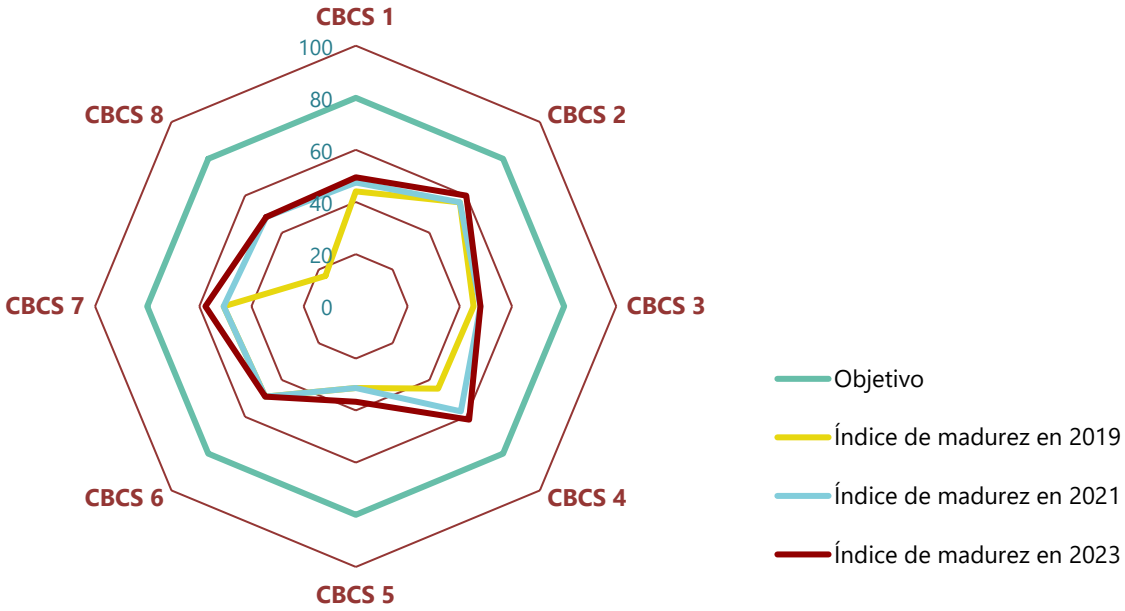
Control		31-12-2021		31-12-2023	
		Índice de madurez	Nivel de madurez	Índice de madurez	Nivel[2] de madurez
CBCS 1	Inventario y control de dispositivos físicos	47,5%	**N1**	49,5%	**N1**
CBCS 2	Inventario y control de *software* autorizado y no autorizado	56,5%	N2	60,0%	N2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	47,9%	**N1**	47,9%	**N1**
CBCS 4	Uso controlado de privilegios administrativos	57,0%	N2	61,5%	N2
CBCS 5	Configuraciones seguras del *software* y *hardware*	31,4%	**N1**	36,6%	**N1**
CBCS 6	Registro de la actividad de los usuarios	49,0%	**N1**	49,0%	**N1**
CBCS 7	Copias de seguridad de datos y sistemas	50,7%	N2	57,7%	N2
CBCS 8	Gobernanza de ciberseguridad y cumplimiento normativo	48,5%	**N1**	48,5%	**N1**
General		**48,5%**	**N1**	**51,3%**	N2

Siguen existiendo claras posibilidades de mejora, particularmente sobre los controles CBCS 1, CBCS 3, CBCS 5, CBCS 6 y CBCS 8, que presentan deficiencias significativas y no alcanzan el nivel de madurez **N2**.

La situación observada de los controles queda reflejada en el gráfico 1, tanto de la presente auditoría como la situación en las dos anteriores.

[2] **N1, "Inicial", N2, "Repetible pero intuitivo"**. Véase apéndice 3 para más explicación.

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



En el apartado 5 se realizan las recomendaciones pertinentes para la mejora de todos los controles.

Sobre la gobernanza de la ciberseguridad

El Ayuntamiento de San Vicente 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 (que 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), que son los responsables de articular y facilitar la ejecución de las actividades establecidas por la alta dirección en materia de ciberseguridad.

Hemos podido verificar la existencia de carencias relevantes que impiden que la gobernanza pueda considerarse efectiva, principalmente:

- la existencia de competencias incompatibles entre sí del responsable del departamento TIC, que pertenece al órgano colegiado de delegado de protección de datos (DPD) y es además responsable de seguridad de la información del ENS,

- la falta de recursos en el departamento TIC, tanto económicos como de personal,

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

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.

3. RESPONSABILIDADES DE LOS ÓRGANOS DEL AYUNTAMIENTO

Los órganos superiores y la dirección del Ayuntamiento 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 (ENS): confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Adicionalmente, la responsabilidad sobre el establecimiento y aplicación práctica de las medidas de seguridad la deben asumir los órganos y roles designados en las políticas de seguridad de la información aprobadas por el Ayuntamiento, principalmente el Comité de Seguridad TIC y el responsable de seguridad.

Además de las responsabilidades sobre la seguridad de los sistemas de información, los órganos municipales también deben garantizar que las actividades de la entidad resultan conformes con las normas aplicables y establecer los sistemas de control interno que consideren necesarios para esta finalidad. En particular, deben garantizar que las actividades relativas a los procesos de gestión de las subvenciones recibidas y de la contratación se realizan de acuerdo con la normativa correspondiente.

4. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

La responsabilidad de la Sindicatura de Comptes ha consistido en revisar y evaluar si la gestión de las ayudas relacionadas con el Componente 11 del PRTR ha sido adecuada, y obtener una seguridad limitada y concluir sobre la situación a 31 de diciembre de 2023 de los CBCS, valorar las mejoras realizadas desde nuestra anterior auditoría y, en su caso, formular recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control.

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. 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.

Dadas las especiales características del trabajo realizado sobre los sistemas de información, este se ha efectuado por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI).

Consideramos que la evidencia de auditoría obtenida proporciona una base suficiente y adecuada para fundamentar nuestras conclusiones, de acuerdo con el alcance limitado que se ha señalado previamente.

5. RECOMENDACIONES

Para subsanar las deficiencias de control relativas a los controles básicos de ciberseguridad identificadas por la Sindicatura en la presente auditoría y mejorar los niveles de control señalados en el apartado 2 anterior, reformulamos las recomendaciones que se efectuaron en la anterior auditoría, 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 en que se deben realizar.

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

    - La 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. Mejorar la aplicación del procedimiento elaborado para la gestión de copias de seguridad de datos y sistemas, particularmente mediante la realización de pruebas de recuperación y la mejora de las medidas de protección de las copias.

Sobre gobernanza de la ciberseguridad y el cumplimiento normativo (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 31 del Real Decreto 311/2022.

    - 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.

    - Eliminar la actual incompatibilidad existente en los roles asumidos por el responsable de seguridad de la información, que es el coordinador del departamento de informática y forma parte del órgano colegiado de delegado de protección de datos (DPD).

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.

Sobre el Centro de Operaciones de Ciberseguridad

12. Proporcionar los recursos internos necesarios y/o contratar los servicios que permitan explotar los sistemas de seguridad disponibles, de manera que el conjunto de sistemas y servicios de seguridad existentes en la entidad puedan configurar un SOC.

    Esto incluye finalizar la adquisición, despliegue y puesta en operación de las herramientas de seguridad, no incluidas en el Plan de choque de ciberseguridad de la Generalitat, necesarias para el despliegue de un SOC, incluyendo herramientas de monitorización, auditoría, gestión de SOC y específicas de la participación en la RNSOC (LUCIA y herramienta MISP-Malware Information Sharing Platform)[3].

13. Llevar a cabo la federación con el SOC del CSIRT-CV e integrarse en la RNSOC y mediante un modelo de seguridad federado beneficiarse de los recursos y servicios de estos, lo que aumentaría significativamente el nivel de seguridad general.

Sobre la gestión de los fondos del PRTR

14. Crear una oficina de gestión exclusiva de fondos europeos que proporcione los recursos e infraestructura de apoyo necesarios a los distintos departamentos en la ejecución de proyectos subvencionados por el PRTR y otras líneas de financiación europeas.

    Esta oficina debe proporcionar un servicio transversal y promover la ejecución de proyectos de interés general para el municipio. Para ello debe disponer de un catálogo de servicios y su actividad debe proporcionar acompañamiento en todas las fases de proyecto a los beneficiarios, incluyendo el análisis y captación de fondos, la gestión administrativa y coordinación interna, y la justificación.

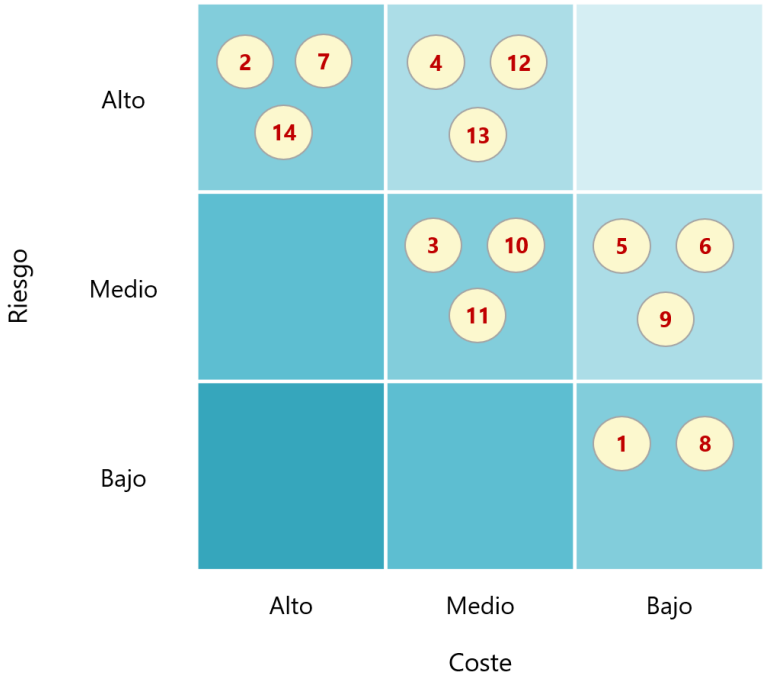
Priorización de las recomendaciones

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 a la anterior auditoría, adaptando la relación

[3] Véase documento *Centros de operaciones de ciberseguridad (SOC) y Red Nacional de SOC (RNS)*. Centro Criptológico Nacional, 2023.

riesgo/coste de cada recomendación considerando las mejoras realizadas desde la anterior revisión. También se ha añadido las nuevas recomendaciones 12 a 14.

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



Seguimiento de las recomendaciones de informes anteriores

Hemos realizado un seguimiento de las recomendaciones efectuadas en el anterior informe de auditoría. Tal como se muestra en el cuadro 3, de las once recomendaciones realizadas en ese informe, seis no se han atendido y cinco lo han sido solo parcialmente.

Cuadro 3. Seguimiento de recomendaciones

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2023 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 cambios significativos.	**No aplicada**	Se mantiene la redacción, ya que sigue vigente
2	Implantar soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Se ha iniciado la preparación de un pliego para la adquisición de una solución para restringir el acceso de dispositivos físicos no autorizados a la red corporativa. Como medida parcialmente compensatoria hasta la adquisición del sistema, se está implementando una segmentación de la red corporativa mediante la configuración de los *switches* de la red municipal en base a tipos de dispositivo.	**Aplicada parcialmente**	Se mantiene la redacción, ya que sigue vigente
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.	El Ayuntamiento ha aprobado formalmente un catálogo de aplicaciones autorizadas. Este documento se mantiene actualizado por el Comité de Seguridad de la Información, conforme las distintas áreas municipales comunican a Informática sus necesidades de *software* y este evalúa la viabilidad de instalación.	**Aplicada parcialmente**	Se mantiene la redacción, ya que sigue vigente
4	Identificar y actualizar todos los sistemas que se encuentran fuera del periodo de soporte.	Sin cambios significativos.	**No aplicada**	Se mantiene la redacción, ya que sigue vigente

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2023 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
5	Documentar los controles actualmente existentes, completarlos y aprobar formalmente unos procedimientos, 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 de seguridad. - La priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.	Sin cambios significativos.	**No aplicada**	Se mantiene la redacción, ya que sigue vigente
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 técnica que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas. - La política de autenticación a aplicar a este tipo de cuentas.	El Ayuntamiento ha eliminado usuarios no nominativos de determinados dispositivos y sistemas, siempre que no existiera un impedimento técnico. Además, para cada uno de los administradores del sistema, se han creado distintos usuarios con diferentes niveles de privilegio, dependiendo de la naturaleza de las actividades a realizar. No obstante, no se dispone de un procedimiento aprobado que establezca el proceso general de gestión de privilegios de administración utilizado.	**Aplicada parcialmente**	Se mantiene la redacción, ya que sigue vigente
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, 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.	El Ayuntamiento ha utilizado guías elaboradas por el CCN para la configuración de sistemas operativos y equipos, en casos puntuales ante avisos de vulnerabilidades, pero no existe un proceso sistemático que asegure el bastionado de todos los sistemas ni se dispone de un procedimiento aprobado que detalle dicho proceso.	**Aplicada parcialmente**	Se mantiene la redacción, ya que sigue vigente

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2023 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 dicha revisión es aconsejable centralizarlos en sistemas dedicados a tal efecto.	Sin cambios significativos.	**No aplicada**	Se mantiene la redacción, ya que sigue vigente
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.	El Ayuntamiento ha elaborado un procedimiento específico sobre el proceso de copia de seguridad de sistemas, aunque no se han realizado mejoras sobre las pruebas de recuperación, el periodo de retención o la protección de las copias. El procedimiento ha sido formalmente aprobado mediante resolución de Alcaldía.	**Aplicada parcialmente**	Se actualiza la redacción anterior
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.	Sin cambios significativos.	**No aplicada**	Se mantiene la redacción, ya que sigue vigente
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.	Sin cambios significativos.	**No aplicada**	Se mantiene la redacción, ya que sigue vigente

APÉNDICE 1
Los fondos europeos del PRTR

Plan de Recuperación, Transformación y Resiliencia (PRTR)

La Unión Europea, con objeto de promover la recuperación económica y social tras la pandemia del coronavirus, dispuso de una serie de fondos destinados a programas de reforma e inversión para los siguientes años, comúnmente conocidos como Fondos Next Generation EU.

Para articular el uso de los Fondos Next Generation EU, el Gobierno de España impulsó el Plan de Recuperación, Transformación y Resiliencia (PRTR), alineado con los objetivos de los fondos EU y estructurado en distintas áreas, una de las cuales es la transformación digital y la modernización de la Administración pública, que se encuentra recogida en el Componente 11 del Plan[4].

Subvenciones destinadas a la transformación digital y modernización de la Administración de las entidades locales

Para desarrollar estas ayudas, mediante la Orden TER/1204/2021, de 3 de noviembre, se aprueban las bases reguladoras y se efectúa la convocatoria correspondiente a 2021 de subvenciones destinadas a las entidades locales, en particular las destinadas a los municipios de más de 50.000 habitantes, así como los de población inferior que tengan la consideración de capital de provincia.

En el artículo 5 de la citada Orden TER/1204/2021 se estipula que las entidades deberán destinar las subvenciones contempladas en el Componente 11 a financiar proyectos de modernización y digitalización que se enmarquen en alguna de las cinco líneas estratégicas enunciadas en su apartado 2:

- Línea estratégica 1. Administración orientada al ciudadano.
- Línea estratégica 2. Operaciones inteligentes.
- Línea estratégica 3. Gobierno del dato.
- Línea estratégica 4. Infraestructuras digitales.
- Línea estratégica 5. Ciberseguridad.

En los apartados 3 y 4 se establece que, al objeto de garantizar la máxima eficiencia en la aplicación de los fondos y lograr, con las actuaciones, el mayor impacto para la ciudadanía en su conjunto, las entidades beneficiarias priorizarán los proyectos, estableciendo como **"Prioridad 1. Proyecto en la Línea 5. Puesta en marcha de un Centro de Operaciones de Ciberseguridad"**, y que este proyecto deberá incluirse necesariamente en las propuestas. En el caso de que la entidad beneficiaria dispusiera ya de proyectos en marcha relacionados con este o tuviera cubiertas las necesidades en este ámbito, deberá justificarlo mediante declaración responsable y quedará, por tanto, exenta, pudiendo dedicar la financiación al

[4] https://planderecuperacion.gob.es/politicas-y-componentes/componente-11-modernizacion-de-las-administraciones-publicas y https://planderecuperacion.gob.es/sites/default/files/2023-10/0310203_adenda_plan_de_recuperacion_componente11.pdf

resto de prioridades establecidas en el apartado 3 o, en su caso, a las actuaciones subvencionables recogidas en el apartado 2 de ese artículo.

Una vez entrada en vigor la Orden TER/1204/2021, fue publicada por la Secretaría General de Administración Digital (SGAD) la "Guía de requisitos para proyectos de Entidades Locales", que proporciona ayudas sobre aspectos generales y específicos de las distintas líneas de actuación y sobre el formato del proyecto o memoria técnica. El porcentaje del presupuesto dedicado a la subvención en la Línea 5 que se considera adecuado para el proyecto de puesta en marcha de un SOC, según la Guía de requisitos es, estimativamente, del 20% del total de la subvención a percibir.

Componente 11. Línea 5. Proyecto "Puesta en marcha de un Centro de Operaciones de Ciberseguridad"

La Línea Estratégica 5, Ciberseguridad, contiene el proyecto "Puesta en marcha de un Centro de Operaciones de Ciberseguridad" que es de máxima prioridad y debe ser incluido obligatoriamente en las propuestas de las entidades beneficiarias.

La guía antes citada establece que los centros de operaciones de ciberseguridad (SOC) que se desplieguen formarán parte de la Red Nacional de Centros de Operaciones de Ciberseguridad (RNS), que integra el Centro de Operaciones de Ciberseguridad de la Administración General del Estado y los de las demás Administraciones públicas del ámbito nacional.

El apartado 5 de la citada guía de la SGAD especifica los servicios a implantar en el marco de despliegue del Centro de Operaciones de Ciberseguridad y los requisitos de integración con la Red Nacional de Centros de Operaciones de Ciberseguridad:

- Implantación de las tecnologías necesarias que permitan la vigilancia del perímetro y de la red interna implantando las tecnologías disponibles en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC 105) o haciendo uso de los sistemas de alerta desplegados por el CCN-CERT.

- Despliegue de la herramienta microCLAUDIA del CCN-CERT en toda la organización.

- Capacidad de recolección y correlación básica de los registros de trazabilidad (*logs*) necesarios para la vigilancia (mediante productos recogidos en el catálogo CCN-STIC 105).

- Actividades de formación y concienciación en todas las organizaciones atendidas.

- Despliegue de tecnologías de detección y respuesta en el punto final (EDR) implantando las tecnologías disponibles en el catálogo CCN-STIC 105.

- Intercambio automático y fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes mediante la implantación y operación

de la herramienta de gestión de incidentes LUCIA[5] del CCN-CERT, que operará en modo federado con el de la Plataforma Nacional.

Los aspectos técnicos de un SOC se detallan en el siguiente apéndice.

Seguimiento y justificación de los proyectos

La certificación o justificación del gasto constituye una de las principales obligaciones que deben cumplir los organismos a los cuales se les ha concedido una ayuda para la realización de algún proyecto en el ámbito de aplicación del PRTR.

Esta obligación queda recogida en el artículo 22 de la Orden TER/1204/2021, que especifica: "1. Las entidades beneficiarias deberán justificar el cumplimiento de la finalidad para la que se concedió la subvención y la aplicación de los fondos percibidos ante el órgano concedente. 2. La justificación se efectuará por vía electrónica a través de la aplicación o aplicaciones que designe la Dirección General de Cooperación Autonómica y Local, con arreglo a las normas y a los modelos electrónicos que se determinen y de acuerdo con las instrucciones que se dicten en aplicación de esta orden."

Para la correcta justificación de los proyectos, el Ministerio de Política Territorial y Memoria Democrática publicó las "Instrucciones para la justificación de los proyectos relativos a: Plan de Recuperación, Transformación y Resiliencia. Subvenciones destinadas a la transformación digital y modernización de las Administraciones de las entidades locales (componente 11. inversión 3)", que detallan y desarrollan las obligaciones recogidas en el artículo 22 de la citada orden.

Además, durante la ejecución de los proyectos, las entidades beneficiarias **deben implementar un sistema de seguimiento y acreditación del cumplimiento de los hitos y objetivos** comprometidos en el PRTR. La Orden HFP/1030/2021 y la Orden HFP/1031/2021, de 29 de septiembre, configuran este sistema de gestión y el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable.

El Ministerio de Hacienda y Función Pública ha publicado la "Guía del sistema de seguimiento y acreditación del cumplimiento de hitos y objetivos en el ámbito del Plan de Recuperación, Transformación y Resiliencia", que aporta unas orientaciones básicas a tener en cuenta a la hora de implementar un sistema de seguimiento y acreditación del cumplimiento de los hitos y objetivos comprometidos en el PRTR y que se configura como una guía de mínimos, que debe adaptarse a la estructura y especificidades de cada ministerio y completarse con aquellos otros procedimientos que, en su caso, se considere oportuno desarrollar.

El artículo 18 de la Orden TER/1204/2021 establece la emisión y notificación de la resolución una vez realizadas las comprobaciones sobre la actuación subvencionable y el cumplimiento del resto de requisitos exigidos en esta orden.

[5] Listado Unificado de Coordinación de Incidentes y Amenazas (LUCIA).

Oficinas de gestión de fondos europeos

La gestión de fondos europeos es, en general, realizada por departamentos, servicios u oficinas específicas, que realizan una labor especializada sobre la gestión de los diversos instrumentos de la Unión Europea para la financiación de proyectos, incluyendo los fondos FEDER y Next Generation. La complejidad en la coordinación de proyectos entre los distintos actores implicados y en la justificación del gasto derivado de las actuaciones aconseja la existencia de órganos especializados para su gestión.

Estas oficinas de gestión de fondos europeos deben disponer de los recursos económicos y humanos suficientes para asegurar la capacidad mínima de captación y gestión de fondos, tanto en el volumen de las ayudas gestionadas como en los servicios proporcionados a los departamentos del Ayuntamiento en la ejecución de proyectos subvencionados.

Para optimizar su labor en los ayuntamientos, estas oficinas deben proporcionar un servicio transversal, facilitar la planificación estratégica y promover la ejecución de proyectos de interés general para el municipio. Deben disponer de un catálogo de servicios y su actividad debe proporcionar acompañamiento en todas las fases de proyecto a los beneficiarios, incluyendo el análisis y captación de fondos, la gestión administrativa y coordinación interna, y la justificación.

Además, resulta aconsejable para su funcionamiento:

- Disponer de personal propio del Ayuntamiento, dado que el personal externo no se encuentra autorizado para determinadas gestiones administrativas y de justificación.

- Disponer de personal cualificado para la gestión de fondos europeos, debido a la especificidad de la actividad desarrollada.

- Establecer una cultura colaborativa e integral en los departamentos del Ayuntamiento mediante actividades formativas e informativas, maximizando los beneficios de los proyectos dada la tipología de las convocatorias.

- Disponer de herramientas informáticas específicas para la gestión de fondos y proyectos.

- Establecer un marco normativo y procedimental que describa y detalle los servicios del departamento en todas las áreas de actividad.

- Coordinar la actividad institucional relativa a la inversión y a la captación de fondos mediante órganos de coordinación interna, que incluyan, como mínimo, la participación de los servicios económicos del Ayuntamiento, Alcaldía, Contratación y el departamento de gestión de fondos europeos. Cuanto más elevada sea la dependencia funcional de la oficina/departamento más se facilitan sus tareas transversales y de coordinación.

APÉNDICE 2[6]

Los centros de operaciones de ciberseguridad (SOC) y la Red Nacional de SOC (RNS)

[6] Los conceptos recogidos en este apéndice están basados en distinta documentación publicada por el Centro Criptológico Nacional (CCN) en su página web sobre la Red Nacional de SOC y particularmente en el documento *Centros de operaciones de ciberseguridad (SOC) y Red Nacional de SOC (RNS).*

Qué es un centro de operaciones de ciberseguridad (SOC)

El CCN entiende que **un centro de operaciones de ciberseguridad (SOC) es un conjunto de tecnologías, procesos y personas que mediante su interrelación, cooperación y coordinación prestan servicios de ciberseguridad a su comunidad.**

Su misión es actuar como medida principal para la protección de la ciberseguridad de la propia comunidad, pudiendo ser dicha comunidad de diversa índole, desde organismos tanto públicos como privados hasta individuales o colectivos. Su institucionalización es decisión del organismo que lo promueve y su reconocimiento se obtiene por la participación en diferentes foros de intercambio.

Cuando se trata de definir un SOC se tiende a pensar en la infraestructura tecnológica que cubra el parque tecnológico del organismo. Sin embargo, **el principal componente de un SOC son las personas encargadas de proporcionar la vigilancia constante de estos sistemas, en la que se exige un nivel de conocimiento técnico muy específico**.

Así pues, los organismos públicos, además de las herramientas de seguridad, que en el caso de las entidades locales pueden adquirir con los fondos europeos del PRTR y el Plan de Choque, deben aportar y asumir en sus presupuestos ordinarios los recursos humanos necesarios o contratar servicios de seguridad gestionada.

Los SOC deben destacar por su proactividad, ser capaces de detectar multitud de tipos de ataques, evitar su expansión, responder de forma rápida ante el incidente detectado y generar normas de actuación que eviten futuros incidentes.

Y muy importante, deben intercambiar la información sobre las amenazas y notificar sus incidentes, de manera que la inteligencia colectiva ayude a proteger a la sociedad en su conjunto.

Debemos destacar la labor de los SOC gubernamentales, que prestan estos servicios a una o varias instituciones públicas de un país, actuando como componente fundamental de la capacidad nacional de prevención, protección, detección, coordinación y respuesta ante ciberincidentes. En estos casos la institucionalización viene impulsada y patrocinada por una institución pública con competencias en materia de seguridad nacional.

Servicios de SOC

Los servicios de ciberseguridad que puede prestar un SOC son:

- Servicio de **Prevención**. Para ampliar el conocimiento respecto de sus vulnerabilidades, tanto técnicas como humanas, para reducir la superficie de exposición.

  - Análisis de vulnerabilidades para identificar y remediar vulnerabilidades existentes en los sistemas y aplicaciones, y evitar que sean explotadas por los atacantes.

  - Inspecciones técnicas de seguridad y test de intrusión para ayudar a identificar las vulnerabilidades y debilidades de la infraestructura de TI, así como a evaluar la eficacia de las medidas de seguridad existentes.

- Vigilancia digital para detectar de forma proactiva amenazas y riesgos antes de que se materialicen en un incidente de seguridad.

- Servicio de **Protección**. Para aplicar medidas de bloqueo, en diferentes puntos de la infraestructura, para impedir o limitar los ciberataques.

  - Operación de ciberseguridad para implementar medidas de seguridad como cortafuegos, antivirus, sistemas de detección/prevención de intrusiones (IDS/IPS) que protegen la infraestructura de TI; para mantener actualizado el *software* y *firmware* de los sistemas y dispositivos, corregir vulnerabilidades y mejorar la seguridad; y para implementar un proceso de aplicación oportuna de parches de seguridad y corregir vulnerabilidades conocidas.

- Servicio de **Detección**. Para observar todo lo que ocurre en la organización, para buscar las amenazas existentes.

  - Monitorización de ciberseguridad para monitorizar la infraestructura de TI y detectar de forma temprana posibles incidentes de seguridad.

  - Análisis de *logs* para recopilar y analizar los *logs* de seguridad e identificar posibles intrusiones o actividades anómalas.

  - *Threat Hunting* o búsqueda proactiva de amenazas para detectar anomalías que podrían indicar un ataque en curso o inminente.

- Servicio de **Respuesta**. Para actuar ante los ciberincidentes, para minimizar el impacto sobre la organización.

  - *Incident Response Team (IRT)*, mediante un equipo especializado, para gestionar los incidentes de ciberseguridad y contener el daño, remediar el incidente y restaurar los sistemas afectados; para definir y operar un plan de respuesta a incidentes que establezca las acciones a tomar en caso de un ciberincidente; y para realizar análisis forenses y determinar la causa del incidente y el alcance del daño.

- Servicio de **Gestión de la ciberseguridad**. Para establecer el rumbo del resto de servicios, para desempeñar una correcta gobernanza.

  - Asesoramiento en ciberseguridad para asesorar a la organización sobre cómo mejorar su seguridad y cumplir con las normativas vigentes.

  - Cumplimiento legal y normativo para asegurar que la organización cumple con las leyes y regulaciones relacionadas con la seguridad de la información.

  - Formación en seguridad para promover que el personal de la organización reciba formación en seguridad y que pueda ser consciente de las amenazas y saber cómo actuar en caso de un incidente.

  - Definir e implantar cuadros de mando que proporcionen información sobre el estado de la seguridad de la organización, como el número de incidentes de seguridad, las vulnerabilidades existentes y el estado de las medidas de seguridad.

Red Nacional de SOC (RNS)

La **Red Nacional de SOC es una iniciativa del CCN-CERT para integrar a todos los SOC del territorio nacional**, ya sean públicos o privados y cuyo objetivo principal es impulsar el servicio de protección de sus miembros mediante el bloqueo de cualquier indicio de actividad anómala que se esté detectando en cualquier punto de la Administración.

El CCN-CERT tradicionalmente ha colaborado y colabora en varios SOC de diferente magnitud, ya sea a nivel de ministerios, comunidades y ciudades autónomas, diputaciones/cabildos o entidades locales, a los que se han venido a añadir últimamente operadores de servicios esenciales. En esta dinámica surgió la necesidad de crear una herramienta que interconectara los SOC para que, de manera inmediata, se pudiera detener cualquier intento sospechoso de ciberataque, incluso antes de determinar si consistía realmente en tal o no.

A finales de 2020, la Comisión Europea lanzó su Estrategia de Ciberseguridad para la Década Digital, en la que adquiere un papel relevante una red europea de SOC, basada en herramientas de inteligencia artificial. La intención de la Comisión es focalizar los esfuerzos de detección y protección en los SOC, dado que Europa había sufrido una pandemia de *ransomware* y la red de CSIRT[7] existente a nivel europeo no había sido capaz de pararla.

En este contexto, el CCN-CERT crea a finales del año 2021 la Red Nacional de SOC a través de su versión piloto. Y a mediados de 2022 inició un periodo de apertura con la entrada de nuevos miembros.

La RNS se encuentra en constante redefinición y evolución, y el CCN-CERT trabaja de manera continuada para mejorar la organización de los SOC adheridos, enriquecer la información compartida con el objetivo de lograr una panorámica completa y veraz de las ciberamenazas, y reformular los requisitos de admisión y las condiciones de permanencia.

A la RNS podrán adherirse entidades de las siguientes categorías:

- Entidades públicas. Organismos de la Administración pública española en los que generalmente los servicios de seguridad los prestan proveedores contratados.
- Entidades proveedoras. Empresas del sector privado que prestan servicios de SOC en otras entidades, ya sean públicas o privadas, protegiendo activos españoles.
- Entidades privadas. Empresas del sector privado, con un SOC propio protegiendo sus activos españoles, sin prestar dichos servicios de SOC a otras entidades.

Las entidades que soliciten la adhesión han de estar bajo la protección de un SOC, ya sea propio o externo:

- SOC externo. SOC perteneciente a una entidad proveedora, protegiendo a una o varias entidades tanto públicas como privadas.

[7] CSIRT significa *Computer Security Incident Response Team* (equipo de respuesta a incidentes de seguridad informática).

- SOC propio. SOC perteneciente a la propia entidad pública o privada, ya sea con personal propio o subcontratado (a una o varias entidades proveedoras).

Participación en la RNS

La participación en la RNS reporta importantes beneficios a las entidades adheridas. El beneficio más inmediato para las entidades públicas es el acceso a todos los indicadores de compromiso y de ataque compartidos en la RNS desde un inicio.

Además, se proporciona acceso a un foro de compartición en donde podrán intercambiar recomendaciones respecto a la gestión y dirección de los SOC, como pudieran ser modelos de contratación, recomendaciones sobre proveedores, definición de indicadores para la medición de los servicios, etc.

Por otra parte, el modelo de funcionamiento planteado para la adhesión a la RNS es el de un **modelo federado** donde determinados servicios son provistos por entidades superiores.

El objetivo de un modelo federado es que no todas las entidades tengan que invertir la misma cantidad de dinero dedicado a la ciberseguridad, generando duplicidades en el gasto e infraestructura. Las entidades organizarán el gasto en ciberseguridad atendiendo a los criterios de tamaño, capacidad y posición de la entidad, siendo las entidades de orden superior las que realicen el mayor gasto y proporcionen determinados servicios a las entidades dependientes. Se consigue de esta forma mejorar la eficiencia de las inversiones.

En la mayoría de los casos y según las particularidades de la Administración, las comunidades autónomas harán la mayor inversión en ciberseguridad, posteriormente las diputaciones/cabildos/consejos insulares, para finalizar por las entidades locales.

La adhesión a la RNS como entidad pública tiene determinados requisitos que deben cumplirse durante todo en el periodo de permanencia, particularmente:

- Pertenecer al sector público.
- Disponer de servicios de ciberseguridad o de SOC.
- Aceptar el código ético y de conducta profesional de la RNS.
- Tener instalado y utilizar LUCIA (o estar en proceso de instalación).
- Utilizar las herramientas a disposición de la RNS: acceder de manera continua a la solución de mensajería y estar al corriente de la información intercambiada; acceder puntualmente a la solución de intercambio para tener la capacidad de descargar la información técnica intercambiada, etc.

El CCN hace hincapié en la **importancia de la participación activa** de las entidades adheridas, compartiendo información novedosa y relevante con el resto de la red en los foros y herramientas de intercambio. Esta participación es además evaluada periódicamente y resulta determinante para permanecer en la Red Nacional de SOC.

El Plan de choque de ciberseguridad de la Generalitat

Como consecuencia de los ciberataques contra municipios de la Comunitat Valenciana ocurridos en el año 2021, la Conselleria de Hacienda articuló ese mismo año, mediante la contratación de servicios especializados, un plan para proteger a los municipios de los principales ciberataques, instalar en las localidades que por sus características lo requieran sondas que permitan detectar situaciones de riesgo y, por último, preparar a los municipios para que, en caso de ciberataque, el impacto en los servicios esenciales sea mínimo.

El Plan de Choque de Ciberseguridad, que tuvo una duración de un año, estaba dirigido a todas las entidades locales de la Comunitat Valenciana que desearan participar y contó con la colaboración de la Dirección General de Administración Local y del CCN-CERT.

Para la ejecución del Plan, se contempló la ampliación de los recursos técnicos y humanos del Centro de Seguridad TIC de la Comunitat Valenciana, CSIRT-CV, a fin de que, una vez concluido el contrato para la ejecución del Plan, todos los servicios puestos en marcha se siguieran prestando desde dicho Centro a las entidades locales valencianas.

El Plan fue articulado en el contexto de ejecución de otras dos iniciativas de ciberseguridad: la puesta en operación de la RNS y la disposición de las subvenciones del componente 11, línea 5 del PRTR. Las actuaciones incluidas en el Plan de Choque se encontraban coordinadas con los proyectos para la "Puesta en marcha de un Centro de Operaciones de Ciberseguridad" del PRTR, para que el conjunto de herramientas y servicios desplegados dieran cumplimiento a los requisitos necesarios para la federación de los SOC de las entidades locales con el SOC del CSIRT-CV.

Además, el CSIRT-CV se encuentra incluido en la Red Nacional de Centros de Operaciones de Ciberseguridad, de manera que todos aquellos municipios que ejecuten adecuadamente todas las actividades del Plan de Choque y el proyecto para puesta en marcha de un SOC del PRTR pueden estar incluidos en la Red Nacional de Centros de Operaciones de Ciberseguridad a través de la federación con el SOC del CSIRT-CV.

APÉNDICE 3

Criterios de evaluación de los CBCS y seguimiento de las recomendaciones

Criterios de evaluación de los CBCS

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

Evaluación de los subcontroles

Los CBCS son controles globales compuestos por varios controles detallados o subcontroles. 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 4. Evaluación de los subcontroles

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

Nivel de madurez de los controles

Para determinar la situación global de cada control hemos utilizado el modelo de nivel de madurez de los procesos de control de acuerdo con lo establecido en las GPF-OCEX 5313, que a su vez están basadas en la *Guía de seguridad CCN-STIC 804* del CCN, usando una escala, según se resume en el siguiente cuadro. Las descripciones son las establecidas en el anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Cuadro 5. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	No existe un proceso que soporte el servicio requerido.
N1 Inicial / *ad hoc*	10	Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes. Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.
N2 Repetible, pero intuitivo	50	En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad. Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.
N3 Proceso definido	80	Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.
N4 Gestionado y medible	90	Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.
N5 Optimizado	100	La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

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 verificación 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 y considerando la ponderación o importancia relativa que les asignamos para el cumplimiento del objetivo de control.

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.

Indicador global

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. En particular el **índice de madurez general** sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de controles.

Seguimiento de las recomendaciones

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 6. Situación de las recomendaciones

Total o sustancialmente aplicada	Si el ente auditado 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 auditado 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 auditado 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 auditado, 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 auditado, necesitarían obligatoriamente de alguna prueba adicional para contrastar lo manifestado por el ente auditado que exceden el alcance previsto en el trabajo.

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, un borrador previo del Informe de auditoría se discutió con el responsable del área de informática y modernización, y de seguridad de la información, para su conocimiento y para que, en su caso, efectuara las observaciones que estimara 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, 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, del artículo 55.1.h) de su Reglamento de Régimen Interior y del Programa Anual de Actuación de 2024 de esta institución, el Consell de la Sindicatura de Comptes, en la reunión del día 7 de octubre de 2024, aprobó este informe de auditoría.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe subvenciones PRTR transformación digital y ciberseguridad San Vicente del Raspeig _2023_cas - SEFYCU 5621387

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 ACAA XAR7 22KL AVZX

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 avanzada - ISTEC - 07/11/2024 7:11 VICENT CUCARELLA TORMO