

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

**INFORME DE AUDITORÍA DE LOS
CONTROLES BÁSICOS DE CIBERSEGURIDAD
DE LA DIPUTACIÓN DE VALENCIA**

Ejercicio 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 una auditoría de los controles básicos de ciberseguridad (CBCS) de la Diputación de Valencia.

Conclusiones

El índice de madurez general de los CBCS muestra un valor del 51,0%, por lo que todavía debe mejorar para alcanzar el objetivo del 80%. Se han identificado diversas deficiencias significativas y en todos los controles analizados se deben realizar esfuerzos para su mejora, ya que ninguno alcanza el nivel de madurez requerido. En particular, existen cuatro que tienen un nivel de madurez deficiente, sobre los que se debe trabajar con mayor intensidad para reforzar la protección de los sistemas de información.

Hemos podido verificar que la Diputación no tiene establecida una adecuada gobernanza de la ciberseguridad. Los órganos superiores de la Diputación, como responsables del sistema de control, deben reforzar el actual nivel de compromiso y apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

La revisión del cumplimiento de legalidad en materia relacionada con la seguridad de la información ha puesto de manifiesto un bajo nivel de adecuación a las normas legales. El informe señala varios aspectos pendientes de mejora sobre los que se debe actuar para su pronta subsanación.

Respecto del Esquema Nacional de Seguridad, la Diputación debe realizar los nombramientos necesarios, en especial el responsable de seguridad, y solventar las no conformidades identificadas en la auditoría de cumplimiento realizada, de forma que le permita obtener la certificación de conformidad y el distintivo correspondiente para su publicación en la sede electrónica.



También hemos realizado una serie de recomendaciones con el propósito de contribuir a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de gestión de la ciberseguridad de la Diputación. Entre ellas aconsejamos actualizar y mejorar la normativa de seguridad, implantar soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa (CBCS 1), identificar y actualizar todos los sistemas que se encuentran fuera del período de soporte (CBCS 2) y resolver las vulnerabilidades de nivel crítico identificadas (CBCS 3).

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 auditoría de los controles básicos de ciberseguridad de la Diputación de Valencia

Ejercicio 2021

Sindicatura de Comptes
de la Comunitat Valenciana



ÍNDICE (con hipervínculos)

1. Introducción	3
2. Responsabilidades de los órganos superiores de la Diputación en relación con los controles de ciberseguridad	4
3. Responsabilidad de la Sindicatura de Comptes	5
4. Conclusiones	5
5. Recomendaciones y medidas para el cumplimiento de la legalidad	8
Apéndice 1. Metodología aplicada	16
Apéndice 2. Situación de los controles básicos de ciberseguridad	33
Apéndice 3. Buenas prácticas destacables	45
Acrónimos y glosario de términos	48
Trámite de al·legacions	51
Aprobación del informe	52



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 la reunión de la Comisión de Coordinación en el ámbito local entre el Tribunal de Cuentas y los órganos de control externo (OCEX) del 18 de noviembre de 2019 se planteó la posibilidad de realizar una fiscalización coordinada sobre la implantación de la administración electrónica en las entidades locales, cuyos resultados se exponen en otro informe de la Sindicatura. Dada la importancia de los controles de ciberseguridad en entornos digitalizados, la Sindicatura amplió el ámbito objetivo del citado trabajo e incluyó en los programas anuales de actuación de 2020 y de 2021 la realización de una auditoría de los controles básicos de ciberseguridad de las tres diputaciones provinciales.

Además, la Sindicatura también está llevando a cabo una auditoría del entorno de control de los ayuntamientos con población superior a 50.000 habitantes y las tres diputaciones, uno de cuyos apartados se refiere a los controles básicos de ciberseguridad, en el que se integrarán de forma sintética los resultados reflejados en este informe.

La necesidad de una adecuada ciberhigiene

Los actuales sistemas de información que dan soporte a toda la gestión pública, complejos e interconectados, "están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, los ciberincidentes, que siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto"¹. Estos ciberincidentes tienen

¹ Proyecto de Real Decreto por el que se regula el ENS, de 16 de junio de 2021.



consecuencias potencialmente perturbadoras sobre los servicios que las diputaciones prestan a los ciudadanos y a los ayuntamientos de su ámbito de actuación.

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

En estos entornos actuales de administración electrónica avanzada adquieren todo su sentido conceptos como la ciberresiliencia y la ciberhigiene. Por ciberresiliencia puede entenderse la capacidad de una entidad para evitar o resistir y recuperarse de un ciberataque en un tiempo razonable para continuar prestando sus servicios. La ciberhigiene es un principio fundamental² 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 DE LA DIPUTACIÓN EN RELACIÓN CON LOS CONTROLES DE CIBERSEGURIDAD

Los órganos superiores de la Diputación (en particular el presidente o la presidenta 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.

² *Review of Cyber Hygiene Practices*, European Union Agency for Cybersecurity (ENISA), 2016.



3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

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. 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.

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

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 insuficiente y debe mejorar para alcanzar los niveles exigidos por el ENS

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el grado de control existente en la gestión de los controles básicos de ciberseguridad alcanza un **índice de madurez general del 51,0%**, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles se realizan, pero



existen controles parcialmente establecidos o no formalizados documentalmente. Los resultados detallados obtenidos para cada uno de los CBCS se muestran en el cuadro 1.

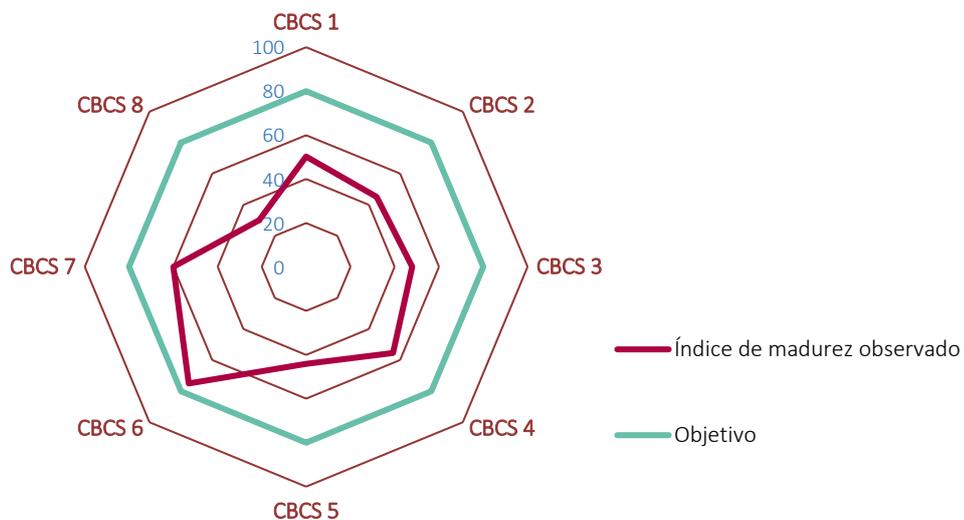
Cuadro 1. Índice de madurez de los controles básicos de ciberseguridad

Control	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	50,3%	N2	62,8%
CBCS 2 Inventario y control de <i>software</i> autorizado y no autorizado	45,0%	N1	56,3%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	47,9%	N1	59,8%
CBCS 4 Uso controlado de privilegios administrativos	55,5%	N2	69,3%
CBCS 5 Configuraciones seguras del <i>software</i> y <i>hardware</i>	44,1%	N1	55,1%
CBCS 6 Registro de la actividad de los usuarios	75,0%	N2	93,8%
CBCS 7 Copias de seguridad de datos y sistemas	60,0%	N2	75,0%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	30,0%	N1	37,5%
General	51,0%	N2	63,7%

El índice de cumplimiento de los CBCS es del 63,7%, 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% o *N3, proceso definido*.

De una forma más sintética y gráfica, la situación observada de los controles queda reflejada en el gráfico 1.

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





A la vista de los resultados obtenidos en la revisión, se concluye que el nivel de efectividad en los controles analizados es insuficiente y existen claras posibilidades de mejora para alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información, y particularmente sobre aquellos controles que presentan deficiencias significativas y no alcanzan el nivel de madurez N2 (CBCS 2, CBCS 3, CBCS 5 y CBCS 8). En el apartado 6 se realizan las recomendaciones pertinentes con esa finalidad.

Nuestra auditoría y los indicadores reflejan la situación a 30 de septiembre de 2021.

La Diputación de Valencia no tiene establecida una adecuada gobernanza de la ciberseguridad y debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información

Los órganos superiores de la Diputación 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.

A pesar de las carencias que señalamos, hemos podido verificar la existencia de un cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores de la Diputación y los gestores y responsables de las áreas implicadas.

Las carencias más relevantes identificadas son las siguientes:

- La falta de actualización del documento de políticas de seguridad de la información.
- La falta de actividad efectiva y continuada del comité de seguridad, que hemos verificado que no se ha reunido en los últimos tres años.
- La inexistencia, actualmente, de determinados roles clave en la organización, como el responsable de seguridad, constituye una de las deficiencias más graves en términos de gobernanza, puesto que su responsabilidad, la gestión de la seguridad de la información y de los servicios prestados, no puede considerarse adecuadamente asumida por el resto de los responsables de la organización. Consideramos indispensable que un ente del tamaño de la Diputación con sus complejos sistemas de información disponga de, al menos, una persona con dedicación completa a las tareas de seguridad.

Es muy conveniente, por tanto, solventar de forma urgente las carencias identificadas, que tienen un impacto negativo en el nivel de seguridad de la información, y la explotación de las fortalezas existentes, que potencialmente facilitarán la aplicación de medidas necesarias, incluidas las recomendaciones efectuadas en el presente informe.

Son necesarios esfuerzos para impulsar la aplicación de las mejoras destacadas en el informe con el fin de alcanzar el nivel de madurez requerido. La existencia de un liderazgo reconocible por toda la corporación puede fomentar los avances en términos de



concienciación, ayudando a vencer las naturales resistencias de la organización a los cambios exigidos por la implantación de una administración electrónica avanzada.

Existe un bajo grado de cumplimiento de la normativa relativa a la seguridad de la información

La revisión del cumplimiento de legalidad en materia relacionada con la seguridad de la información ha puesto de manifiesto un deficiente nivel de cumplimiento de la normativa. 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 que se detallan en el apéndice 2, y mejorar los niveles de control señalados en el apartado anterior, formulamos las recomendaciones que se señalan a continuación, para cuya atención la Diputación deberá dedicar los esfuerzos y recursos necesarios. 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. Actualizar la normativa de seguridad existente o aprobar procedimientos específicos, de manera que recojan, amplíen y representen con fidelidad el conjunto de medidas implantadas en la práctica para el control de los dispositivos físicos.
2. Finalizar la implantación de las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa, actualmente en fase de planificación o inicio de ejecución.

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

3. Actualizar la normativa de seguridad existente o aprobar procedimientos específicos para el control de *software*, de manera que recojan, amplíen y representen con fidelidad el conjunto de medidas ya implantadas. Adicionalmente, recomendamos elaborar un catálogo de aplicaciones autorizadas y un plan anual de mantenimiento; este último documento está previsto en la normativa aprobada existente.
4. Identificar y actualizar todos los sistemas operativos que se encuentran fuera del período de soporte, ya que representan un riesgo para la seguridad.



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

5. Modificar la normativa de seguridad existente o aprobar un procedimiento de seguridad específico para la identificación y remediación de vulnerabilidades, que recoja las acciones que actualmente se realizan y que adicionalmente contemple:
 - La priorización basada en el análisis de riesgos para su resolución.
 - La realización de pruebas de penetración.
 - Explotar adecuadamente las herramientas disponibles de gestión de flujos de trabajo, que ya se encuentran configuradas para gestionar la identificación y remediación de vulnerabilidades.
6. Resolver las vulnerabilidades de nivel crítico identificadas.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

7. Elaborar y aprobar un procedimiento unificado de gestión de usuarios con privilegios de administración que establezca las directrices para todos los sistemas de la entidad, que detalle las medidas actualmente implantadas y considere particularmente:
 - Eliminar todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. 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.
 - Crear y utilizar, en aquellos sistemas en los que no se ha implantado el uso dedicado de cuentas de administración, diferentes cuentas nominativas para un mismo usuario con distintos niveles de privilegios administrativos, adecuando la asignación de permisos a los distintos tipos de tareas a realizar

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

8. Actualizar y mejorar la normativa existente o aprobar un procedimiento específico para la configuración segura de los sistemas, de manera que considere la seguridad por defecto, el criterio de mínima funcionalidad y la aplicación de medidas de gestión del proceso. Para ello, proponemos 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 de seguridad de las series 400, 500 y 600 del Centro Criptológico Nacional.

Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración 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 un procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.

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

9. Actualizar y mejorar la normativa de seguridad existente o aprobar un procedimiento de seguridad específico para el tratamiento de los *logs* de auditoría de la actividad de los usuarios, que contemple, como mínimo, los sistemas afectados, la información que se registra, el periodo de retención, las copias de seguridad, la gestión de derechos de acceso al registro y un proceso para su revisión.

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

10. Aunque la normativa de seguridad existente recoge parcialmente el control de copias de seguridad actualmente implantado, existen varios aspectos a mejorar, en particular:
 - La revisión y actualización de la normativa de seguridad existente o aprobación de un procedimiento de seguridad específico, detallando adecuadamente el control implantado e incluyendo el uso de herramientas de control de tareas o flujos de trabajo en todas las secciones del servicio de informática.
 - La ejecución de un plan de pruebas periódicas de recuperación que incluya todos los tipos de copia.
 - La implantación efectiva de las herramientas y soluciones que actualmente están en fase de planificación y su formalización en el procedimiento o normativa.

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

Existen varios aspectos sobre los que la Diputación debe actuar para subsanarlos:

11. Para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad, la Diputación debe:
 - Atender y solventar las no conformidades identificadas en la auditoría de cumplimiento realizada en el año 2017.
 - Actualizar la documentación relativa al proceso de adecuación al ENS, incluyendo la política de seguridad, la normativa de seguridad, el Plan de Adecuación y la Declaración de Aplicabilidad.
 - Realizar los nombramientos necesarios para los roles definidos en la Política de Seguridad, en especial el responsable de seguridad.
 - Realizar las auditorías de seguridad previstas en el artículo 34 del Real Decreto 3/2010.



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

12. En relación con la protección de datos personales, la Diputación debe:

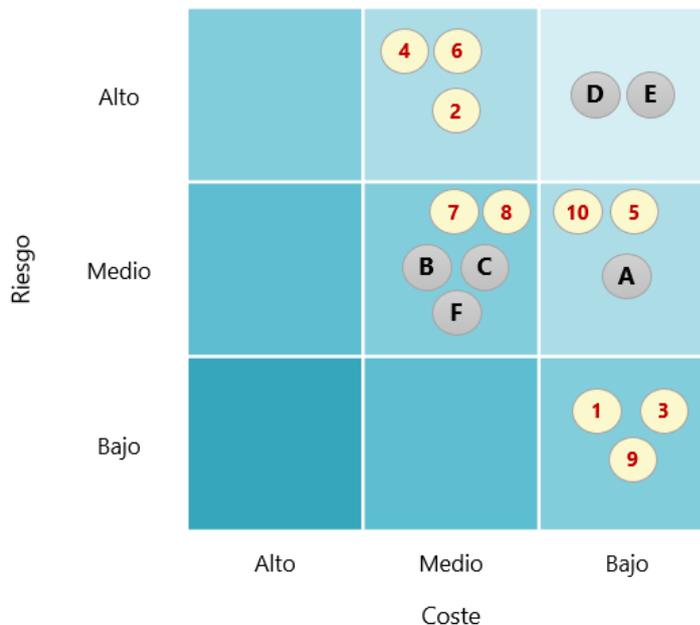
- Finalizar el análisis de riesgos sobre los tratamientos de datos personales conforme al artículo 32.2 del RGPD.
- Realizar las evaluaciones de impacto de los riesgos detectados de nivel alto.
- Realizar auditorías en materia de protección de datos.

13. En relación con la Ley de Factura Electrónica, la Diputación debe realizar las auditorías de sistemas anualmente tal como exige esa norma.

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**. No se incluyen los puntos 11 a 13 anteriores, ya que son medidas de obligado cumplimiento. Se incluyen en el gráfico las recomendaciones pendientes de implementar de nuestro anterior informe, con referencias A a F, que se comentan en el siguiente apartado.

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





Seguimiento de recomendaciones anteriores

Hemos realizado un seguimiento de las recomendaciones sobre el control interno del [Informe sobre auditoría operativa de la gestión y recaudación delegada en las diputaciones de la Comunitat Valenciana. Ejercicio 2016](#). Tal como se muestra en el siguiente cuadro, de las seis recomendaciones realizadas en ese informe, cuatro no se han atendido y dos lo han sido solo parcialmente, por lo que todas siguen vigentes.



Cuadro 2. Seguimiento de recomendaciones

Recomendaciones sobre los controles generales de tecnologías de la información del informe anterior	Situación a 30 de septiembre de 2021	
<p>A Proponemos a la Diputación de Valencia aprobar procedimientos que garanticen los principios de segregación de funciones y de mínimos privilegios para las funciones asignadas en el Departamento de Sistemas de Información.</p>	<p>Hemos verificado que no han sido aprobados procedimientos o normativas que regulen específicamente la segregación de funciones y la aplicación del principio de mínimo privilegio.</p>	<p>No aplicada</p>
<p>B Recomendamos a la Diputación de Valencia la realización periódica de pruebas de las interfaces para garantizar la integridad, validez y la completitud de la información.</p>	<p>Sin variación.</p>	<p>No aplicada</p>
<p>C Es conveniente que la Diputación de Valencia apruebe un procedimiento para la revisión de eventos de seguridad y de accesos a la información y la implantación de herramientas que faciliten el análisis de los eventos y las actividades relevantes del sistema de información.</p>	<p>Hemos verificado que no han sido aprobados procedimientos o normativas que regulen específicamente la revisión de eventos de seguridad y de accesos a la información.</p> <p>Hemos verificado que se ha iniciado un proyecto, en colaboración con la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) de la Generalitat y el Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV), para la monitorización, almacenamiento e interpretación de los registros de actividad de determinados sistemas y servicios críticos que son ofrecidos por la Diputación a los ayuntamientos.</p>	<p>Aplicada parcialmente</p>
<p>D Proponemos a la Diputación de Valencia aprobar formalmente un procedimiento de gestión de usuarios, y que la gestión de las funcionalidades de los usuarios se base en perfiles predefinidos según el puesto de trabajo, aplicando el principio de asignar las mínimas capacidades para poder realizar las tareas asignadas. El procedimiento debe incluir la revisión periódica de usuarios que permita mantener en el tiempo el principio señalado.</p>	<p>Hemos verificado que no han sido aprobados procedimientos o normativas que regulen específicamente la gestión de usuarios y la asignación de privilegios a estos.</p>	<p>No aplicada</p>



Recomendaciones sobre los controles generales de tecnologías de la información del informe anterior	Situación a 30 de septiembre de 2021	
<p>La Diputación de Valencia debería configurar políticas de control de accesos a sistemas y aplicaciones para que se ajusten a las buenas prácticas generalmente aceptadas y a las exigencias del ENS.</p> <p>E De acuerdo con la información facilitada a fecha de emisión de este informe, la Diputación de Valencia ha mejorado las políticas de control de accesos a la aplicación Estima, aunque consideramos que se debe reforzar todavía más hasta alcanzar los parámetros exigidos por el ENS.</p>	<p>Hemos verificado que han sido implantadas determinadas mejoras en el proceso de autenticación de los usuarios. No obstante, el conjunto de medidas implantadas para el control de los accesos a aplicaciones y sistemas no alcanza los niveles exigidos por el ENS.</p>	Aplicada parcialmente
<p>Recomendamos a la Diputación de Valencia aprobar lo antes posible un plan de continuidad de la actividad y de recuperación ante desastres, documentados por escrito y aprobados formalmente por la Dirección. Previamente será necesario realizar un análisis de riesgos o un análisis de impacto en los servicios prestados para establecer la criticidad y prioridad de los activos de la entidad (servicios, información, aplicativos, dispositivos de red y servidores, etc.), así como los puntos y plazos necesarios para la recuperación de la información y los sistemas.</p> <p>F</p>	<p>Hemos verificado que no ha sido elaborado y aprobado un plan de continuidad de la actividad y de recuperación ante desastres.</p>	No aplicada



Actuaciones en curso

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

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

- Implantación de un nuevo control de acceso a red que conllevará una mejora relevante en el control de activos físicos no autorizados.
- Implantación de un nuevo sistema para la gestión centralizada de las cuentas de administradores locales, que limita los riesgos en caso de compromiso de un equipo.
- Implantación de un sistema que proporciona las características técnicas necesarias para mejorar los procesos de copia de seguridad actuales, según los nuevos requisitos identificados.
- Implantación de una estrategia de adopción masiva de sistemas *cloud*. Este modelo permite una mayor escalabilidad, tanto de la infraestructura tecnológica como de las aplicaciones de gestión, para hacer frente a demandas que no son asumibles con un despliegue exclusivamente local.
- Implantación de una gestión avanzada y auditoría de sistema de ficheros y directorio activo, mediante el uso combinado de herramientas comerciales y del Centro Criptológico Nacional, que posibilite un mantenimiento más eficiente y seguro de los permisos de acceso a información por parte de los usuarios, y que mantenga la información cifrada y clasificada, de forma que proporcione una protección adicional contra los ataques de *ransomware*.
- Implantación de un sistema para la monitorización, almacenamiento e interpretación de los registros de actividad de determinados sistemas y servicios críticos que son ofrecidos por la Diputación a los ayuntamientos, en el marco de un proyecto en colaboración con la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) de la Generalitat y el Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV).
- Puesta en marcha de varias iniciativas para promover la concienciación en materia de seguridad de la información entre el personal de la Diputación.



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 las diputaciones en particular, no son ajenas a esta preocupación por 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.

Es imperativo que los responsables de las diputaciones 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 INES³ 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.

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) –en definitiva, 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

Nuestro objetivo ha sido obtener una seguridad limitada y concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación tanto sobre su diseño⁴ como sobre su eficacia operativa⁵ para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte, 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.

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.

Alcance

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

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

Dada la naturaleza del objeto material a revisar –la gran amplitud, complejidad y diversidad de los sistemas de información de un ente local de tamaño grande– ha sido necesario delimitar y concretar qué sistemas se iban a analizar. En este sentido, hemos analizado las aplicaciones que soportan los procesos de gestión contable y presupuestaria y la gestión tributaria y recaudatoria, así como los controles que tienen implantados.

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.



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 en 2021. La auditoría se inició en diciembre de 2020 y el trabajo de campo finalizó el 30 de septiembre de 2021, fecha sobre la que se han calculado los indicadores del Informe, ya que hasta entonces es admitida cualquier evidencia adicional disponible. Por tanto, con carácter general el Informe refleja la situación en ese momento, ya que es frecuente que, desde que se inicia el trabajo de campo, determinadas deficiencias observadas y señaladas a los gestores sean subsanadas y son consideradas de esta forma en las conclusiones y en los indicadores.

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

Metodología

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

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

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



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

La guía práctica de fiscalización de los OCEX 5313

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

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

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

Alineación de los CBCS con el Esquema Nacional de Seguridad

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

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



Cuadro 3. Los CBCS y el ENS

Control	Medida de seguridad del ENS*
CBCS 1 Inventario y control de dispositivos físicos	op.exp.1
CBCS 2 Inventario y control de <i>software</i> 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 <i>software</i> y <i>hardware</i>	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) señala⁷ 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 ciberriesgos⁸.

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 día⁹.

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

⁷ [Review of Cyber Hygiene Practices](#), ENISA, diciembre de 2016. Vease 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* <https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf>, 2017.



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 <i>hardware</i>	CBCS 1
2. Tener un registro de todo el <i>software</i> 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 <i>hardware</i> 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 <i>software</i> autorizado	Gestionar activamente todo el <i>software</i> en los sistemas, de forma que solo se pueda instalar y ejecutar <i>software</i> 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 <i>software</i> y <i>hardware</i> 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 <i>logs</i> de auditoría)	Recoger, gestionar y analizar <i>logs</i> de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	CBCS 6-1: Activación de <i>logs</i> de auditoría	El <i>log</i> 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 <i>logs</i> : Retención y protección	Los <i>logs</i> 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 <i>logs</i>	Los <i>logs</i> 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 <i>logs</i> de auditoría, de forma que se facilite su revisión.
		CBCS 6-4: Monitorización y correlación	La entidad dispone de un SIEM (<i>security information and event management</i>) o una herramienta de analítica de <i>logs</i> para realizar correlación y análisis de <i>logs</i> .
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: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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 están basadas 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. <i>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.</i>
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. <i>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.</i>
N3 Proceso definido	80	Los procesos están estandarizados, documentados y comunicados con acciones formativas. <i>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).</i> <i>El éxito es algo más que buena suerte: se merece.</i> <i>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.</i>
N4 Gestionado y medible	90	La dirección controla y mide el cumplimiento de los procedimientos y adopta medidas correctoras cuando se requiere. <i>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.</i> <i>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.</i>
N5 Optimizado	100	Se siguen buenas prácticas en un ciclo de mejora continua. <i>El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras.</i> <i>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.</i> <i>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.</i>



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

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

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

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

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

- a) Alcanzar sus objetivos.
- b) Proteger los activos a su cargo.
- c) Cumplir sus obligaciones diarias de servicio.
- d) Respetar la legalidad vigente.
- e) Respetar los derechos de las personas.

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

Confidencialidad Es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Integridad Es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.

Disponibilidad Se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran.



Autenticidad Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Trazabilidad Es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

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

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

- a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
- b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
- c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

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

De acuerdo con la categoría de cada sistema, los niveles mínimos de exigencia o de madurez requeridos son¹⁰:

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 ciberseguridad¹³. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información¹⁴ 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 TIC¹⁵, 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 apéndice 5 del ["Informe sobre auditoría operativa de la gestión y recaudación delegada en las diputaciones de la Comunitat Valenciana. Ejercicio 2016"](#).

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 30 de septiembre 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 de la Diputación 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

Hemos verificado que la Diputación realiza diversas acciones para mantener actualizado el inventario y control de activos físicos de la entidad, pero estas no han sido detalladas en un procedimiento formalmente aprobado y la normativa existente únicamente especifica la necesidad de disponer de un inventario de activos.

La Diputación dispone de diversas herramientas para la administración de los activos que permiten el inventariado automático de los elementos.

La electrónica de red se encuentra inventariada por una herramienta propietaria del fabricante que permite, adicionalmente, la administración de todos los dispositivos.

Los equipos de usuarios, servidores y resto de dispositivos se encuentran inventariados mediante una herramienta que se encuentra integrada con el servicio de directorio y la plataforma de virtualización, en una implementación particularmente efectiva que permite la obtención automática de datos de los activos. Para elementos que no se encuentran en dominio o no son máquinas virtuales, el inventariado se realiza manualmente o mediante la instalación de un agente.

Adicionalmente, hemos verificado que existe un adecuado proceso de gestión y aprobación de nuevos activos y de retirada o sustitución de activos existentes, proceso que se encuentra adecuadamente establecido en el gestor de flujos de trabajo. La configuración de las distintas herramientas junto con el proceso de gestión definido permite confirmar que los inventarios existentes se encuentran aceptablemente actualizados para todos sus elementos.

Por otra parte, pese a que se encuentra en fase de ejecución un proyecto destinado a la implantación de un sistema de control de acceso a la red, este sistema no se encuentra operativo y en la actualidad no se aplican controles compensatorios que detecten, impidan o limiten la actividad de los dispositivos físicos no autorizados en la red interna de la Diputación.

Existe cierto nivel de control sobre el inventario y el control de activos físicos, y su valoración global alcanza un **índice de madurez del 50,3%**, que se corresponde con un **nivel de madurez N2, repetible pero intuitivo**; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 1 del 62,8%**.



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

Hemos analizado la gestión que realiza la Diputación sobre el inventario y control de *software* y hemos verificado que el proceso implantado no ha sido detallado en un procedimiento formalmente aprobado y la normativa existente únicamente especifica la necesidad de disponer de un inventario de activos.

Existen determinadas aplicaciones que proporcionan soporte a procesos esenciales que se encuentran virtualizadas, de manera que su inventariado y control está centralizado en la herramienta de gestión de aplicaciones virtualizadas.

Para aquellas aplicaciones instaladas directamente en los equipos de usuario, la Diputación dispone de un inventario de gestión automatizada para la administración de los activos *software* gestionados por el Servicio de Informática. El inventario incluye el *software* instalado en los dispositivos de la entidad, la versión, el número de licencias disponibles y número de licencias instaladas, entre otra información, y se encuentra relacionado con el inventario de activos físicos de la entidad.

En cuanto a la gestión del *software* no autorizado, la entidad cuenta con medidas orientadas a impedir su uso que en conjunto pueden considerarse parcialmente efectivas.

La gestión del licenciamiento, la autorización para la instalación y uso de nuevo *software* y el mantenimiento de ciertas aplicaciones, se realizan mediante un proceso que se encuentra adecuadamente establecido en el gestor de flujos de trabajo, pero que no ha sido formalizado en un procedimiento aprobado ni se dispone de un plan de mantenimiento.

Se ha evidenciado la existencia de un elevado número de equipos con sistemas operativos fuera del periodo de soporte del fabricante, incluyendo servidores y equipos de usuario, hecho que supone un grave riesgo para los sistemas de información y constituye una deficiencia de control muy significativa.

Existe un insuficiente nivel de control sobre el inventario y control de *software* autorizado, que alcanza un **índice de madurez del 45,0%**, que se corresponde con un **nivel de madurez N1, inicial/ad hoc**; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 2 del 56,3%**.



CBCS 3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

Objetivo del control

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

Situación del control

Hemos analizado las acciones llevadas a cabo por la Diputación para la gestión de vulnerabilidades y parcheo de sistemas y hemos observado que, aunque existe una normativa aprobada que recoge determinadas obligaciones con respecto al control, el documento no describe adecuadamente la gestión realmente implantada.

La identificación y remediación de vulnerabilidades se realiza por parte del personal del Servicio de Informática, si bien se dispone de contratos con terceros que proporcionan soporte para la actualización de determinados sistemas.

La Diputación utiliza diversos medios para la identificación de vulnerabilidades, como la suscripción a comunicaciones de fabricantes u organismos de referencia o la realización de auditorías por parte del CSIRT-CV, Centro de Seguridad TIC de la Comunitat Valenciana.

Las vulnerabilidades son priorizadas y resueltas mediante un proceso informal que no se encuentra adecuadamente descrito en la normativa existente. Únicamente una parte del proceso completo se encuentra soportada por el uso de herramientas de gestión de flujos de trabajo, lo que impide gestionar completamente el control.

Sobre la aplicación de parches y actualizaciones, se realiza en general de manera automatizada mediante diversas herramientas de gestión centralizada de parches, en el caso de aquellos tipos de sistemas con numerosos activos. Hemos verificado que el control se encuentra adecuadamente implantado y gestionado para la mayor parte de los sistemas.

Hemos verificado que, debido a la existencia de sistemas que no disponen de soporte del fabricante, han sido detectadas múltiples vulnerabilidades de nivel crítico que se encuentran pendientes de resolución o sobre las que no se dispone de parche de seguridad correspondiente. Dicha situación constituye una grave deficiencia de control y un elevado riesgo para los sistemas de información de la Diputación.

Existe un insuficiente 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/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 3 del 59,8%**.



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

Hemos analizado las acciones realizadas para el control de las cuentas de administración y hemos verificado que, aunque se han aplicado determinadas medidas, estas no han sido detalladas en un procedimiento formalmente aprobado y la normativa existente únicamente especifica determinados aspectos que no describen adecuadamente el control.

La gestión de la asignación de privilegios administrativos en los sistemas revisados se realiza con distinto grado de efectividad dependiendo del sistema y de manera independiente para cada uno de ellos, dado que no ha sido aprobado ni implantado un procedimiento que establezca las políticas comunes de gestión de privilegios administrativos de manera general en la Diputación. Hemos verificado que el control completo se aplica de manera particularmente eficaz sobre el sistema que proporciona soporte a la gestión tributaria y recaudatoria.

Con carácter general, se hace un uso adecuado de cuentas nominativas para los usuarios con privilegios administrativos. No obstante, en determinados sistemas revisados se ha detectado el uso de cuentas no nominativas compartidas, lo que dificulta la trazabilidad de las acciones en caso de incidentes. Dicha deficiencia se encuentra parcialmente compensada por un adecuado inventariado y control en el uso de dichas cuentas.

Se ha evidenciado una adecuada provisión de privilegios en los servicios y sistemas de la Diputación, que incluye un proceso de autorización mediante el gestor de flujos de trabajo por parte del responsable del solicitante y el responsable del Servicio de Informática. No obstante, no se ha establecido un proceso periódico de revisión, lo que implica un riesgo de incumplimiento de los principios de asignación de privilegios por cambios en servicio y constituye una deficiencia de control.

Se realiza una correcta aplicación del uso dedicado de cuentas de administración en los sistemas revisados, disponiendo los usuarios administradores de cuentas diferenciadas para tareas que requieran distintos niveles de privilegios administrativos. Esta medida ha sido recientemente implantada.

La Diputación no dispone de una política que defina específicamente los mecanismos de autenticación de los sistemas de la entidad, de manera que, si bien se han establecido en determinados sistemas requisitos de autenticación y una política de contraseñas robusta, estos criterios no se aplican de manera homogénea en todos los sistemas de la entidad.



Finalmente, aunque estos registros se encuentran activados en todos los sistemas revisados y son almacenados y centralizados en sistemas de gestión de *logs*, no existe un proceso de revisión sistemático.

Existe cierto nivel de control sobre las cuentas con privilegios administrativos, por lo que la valoración global del control existente alcanza un **índice de madurez del 55,5%**, 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 4 del 69,3%**.

CBCS 5. CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE

Objetivo del control

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

Situación del control

Hemos analizado las acciones realizadas para el control de la configuración segura en aplicaciones y dispositivos y hemos verificado que no se encuentran completamente recogidas en la normativa aprobada existente, que carece del detalle necesario y no representa con total fidelidad el control implantado.

La entidad realiza acciones para configurar la seguridad en determinados sistemas, pero dichas acciones no son suficientes para garantizar la efectividad del control. Se ha verificado que se dispone de plantillas y protocolos informales para la configuración de determinados dispositivos que contemplan la aplicación de ciertas configuraciones que proporcionan un determinado nivel de seguridad. No obstante, dichas plantillas y protocolos no tienen carácter de bastionado ni la seguridad por defecto es el objeto de estas.

Adicionalmente, hemos identificado la aplicación de un conjunto de configuraciones específicas para la securización de las conexiones remotas según las recomendaciones del CSIRT-CV, como consecuencia de la implantación mayoritaria del teletrabajo en respuesta a la crisis sanitaria del COVID-19.

Sobre la monitorización de las configuraciones existentes, hemos verificado que se han establecido medidas que permiten gestionar las configuraciones de determinados dispositivos críticos de la entidad, pero dichas medidas no permiten monitorizar posibles modificaciones no autorizadas de las configuraciones.

La valoración global del control existente sobre las configuraciones seguras es que la organización alcanza un **índice de madurez del 44,1%**, que se corresponde con un **nivel de madurez N1, inicial/ad hoc**; es decir, el proceso existe, pero no se gestiona o su



gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 5 del 55,1%**.

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 las acciones de la Diputación para el registro de la actividad de los usuarios en los distintos sistemas y hemos verificado que las medidas aplicadas no se encuentran completamente recogidas en la normativa aprobada existente, que carece del detalle necesario y no representan con total fidelidad el control implantado.

Hemos verificado que el registro de actividad se encuentra activado en todos los sistemas revisados. Si bien se mantiene la configuración por defecto en algunos sistemas, hemos verificado que se han aplicado, en determinados sistemas críticos, configuraciones específicas para retención de registros conforme a las necesidades identificadas y según las recomendaciones del fabricante.

La Diputación dispone de varios sistemas para la gestión centralizada de registros de actividad de determinados grupos de activos, lo que supone una mejora sobre la configuración básica por defecto de los *logs* de auditoría. No obstante, la revisión de dichos registros de actividad se realiza de forma informal, no procedimentada.

La Diputación ha iniciado el proyecto colaborativo vSOC (Centro de Operaciones de Seguridad Virtual) con la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC), para la gestión centralizada de la seguridad de entidades locales. Dicho proyecto, articulado mediante la participación del CSIRT-CV, incluye el uso de la herramienta Gloria del Centro Criptológico Nacional, sistema SIEM para la monitorización, almacenamiento e interpretación de datos, que recoge y analiza los registros de actividad de determinados sistemas de la Diputación y de servicios críticos que son ofrecidos a los ayuntamientos.

La valoración global del control existente sobre el registro de la actividad de los usuarios es que la organización alcanza un **índice de madurez del 75,0%**, que se corresponde con un **nivel de madurez N2, repetible pero intuitivo**; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 6 del 93,8%**.



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

La Diputación realiza diversas acciones en relación con las copias de seguridad de los datos y sistemas y la responsabilidad sobre estas acciones se encuentra recogida en la normativa de seguridad, pero no existe un procedimiento aprobado que detalle el control implantado.

Las distintas secciones que componen el Servicio de Informática realizan copias de seguridad sobre los activos que gestionan de manera independiente. Los recursos y medios técnicos son compartidos por toda la organización, pero la gestión sobre la realización de copias se realiza de manera autónoma por parte de cada sección, habiéndose verificado una gestión con un nivel de madurez muy desigual entre las distintas secciones.

La Diputación dispone de un conjunto de herramientas y sistemas para la realización de copias que dispone de características técnicas adecuadas y cubre las necesidades de la organización en cuanto al proceso de realización de copias de seguridad establecido. Las políticas de copia aplicadas han sido desarrolladas de acuerdo con las necesidades identificadas desde el servicio de informática, pero no se ha realizado un ejercicio de definición de necesidades por parte de los responsables funcionales de los servicios.

Hemos verificado que la gestión y revisión de copias realizada por la Sección de Sistemas y Comunicaciones es un proceso manual que se realiza de manera correcta pero que no se encuentra soportado por herramientas de control de tareas o flujos de trabajo, hecho que no garantiza la eficacia del control en todos los casos.

La gestión sobre las copias realizada por la Sección de Bases de Datos se encuentra soportada por un uso particularmente adecuado de la herramienta de control de tareas o flujos de trabajo. Además, se encuentran en avanzado estado de elaboración un conjunto de guías y procedimientos que detallan adecuadamente el control implementado.

Se realizan de forma sistemática pruebas de recuperación planificadas en un entorno de preproducción, aunque únicamente se incluyen determinados tipos de copias. Adicionalmente, se realizan y registran frecuentes recuperaciones satisfactorias de diversos tipos de copias en caso de pérdida de datos o servicios.

El conjunto de herramientas y sistemas disponibles para la realización de copias incluye distintos mecanismos destinados a su protección que pueden considerarse efectivos frente a determinadas amenazas. No obstante, hemos verificado que se encuentra en fase de planificación un proyecto que proporcionará un nivel de seguridad adicional a determinados tipos de copia.



La valoración global del control existente sobre las copias de seguridad es que la Diputación alcanza un **índice de madurez del 60,0%**, que se corresponde con un **nivel de madurez N2, repetible pero intuitivo**; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 7 del 75,0%**.

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

La Diputación ha realizado diferentes acciones orientadas a dar cumplimiento a lo 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:

- En 2013, el Pleno de la Diputación aprobó la Política de Seguridad de la Información (PSI), cuyo contenido se adecua a los requisitos establecidos por el ENS.
- Como consecuencia de la aprobación de la PSI, se designaron los responsables previstos en la política y fue creado el Comité de Seguridad.
- Se ha desarrollado la normativa asociada a la PSI, que incluye una normativa específica para los usuarios de los sistemas de información y otra normativa para el personal técnico de los sistemas.
- El Comité de Seguridad aprobó la Declaración de Aplicabilidad y el Plan de Adecuación.
- Se ha cumplimentado y remitido Informe del Estado de la Seguridad (Informe INES) hasta el año 2018.
- Se han realizado auditorías de cumplimiento previstas en el artículo 34 hasta el año 2017, en las que se han identificado no conformidades.

A pesar de las iniciativas anteriores, existen carencias que se deben subsanar:

- No han sido desarrollados procedimientos operativos de seguridad que completen el marco normativo existente.



- No han sido solventadas las numerosas no conformidades identificadas en las auditorías, ni se ha certificado el cumplimiento del ENS.
- Desde el año 2018, y debido al nombramiento como delegado de protección de datos al funcionario que ostentaba el rol de responsable de seguridad, se ha producido el cese de las actividades relativas al cumplimiento de las obligaciones con respecto al Esquema Nacional de Seguridad y, como resultado, nos han indicado que desde el año 2018:
 - No han sido actualizados los documentos que soportan el proceso de adecuación al ENS ni la política de seguridad.
 - No se han remitido los informes del estado de la seguridad.
 - No se han celebrado reuniones del Comité de Seguridad TIC.
 - No ha sido nombrado un nuevo responsable de seguridad.

Cumplimiento RGPD

En cuanto al cumplimiento en materia de protección de datos personales, la Diputación ha realizado diversas acciones que han sido revisadas durante el presente trabajo de auditoría:

- La Diputación ha nombrado delegado de protección de datos y lo ha notificado a la Agencia Española de Protección de Datos, tal y como exige el artículo 37 del RGPD.
- Se ha elaborado un registro de actividades del tratamiento, que incluye el detalle necesario. Además, dicho registro ha sido publicado y es accesible por medios electrónicos.
- Se encuentra en fase de redacción un pliego para la contratación de un servicio de consultoría y apoyo técnico en materia de seguridad de la información al departamento de protección de datos y seguridad de la información.
- Se han establecido iniciativas por parte del Departamento de Protección de Datos y Seguridad de la Información que han sido galardonadas con el premio de Protección de Datos 2018, "Buenas prácticas en privacidad y protección de datos personales sobre iniciativas para adaptarse al Reglamento Europeo de Protección de Datos", que otorga la Agencia Española de Protección de Datos. Las iniciativas identificadas son:
 - La elaboración y difusión de una guía de teletrabajo, que, en respuesta a la regulación del teletrabajo y a la crisis sanitaria del COVID-19, detalla los aspectos a considerar desde la perspectiva de la protección de datos y la seguridad de la información.
 - La ejecución de proyecto DivalData, que consta de un conjunto de iniciativas destinadas a las entidades locales para dotarlas de herramientas con las que se les pretende facilitar el cumplimiento de la normativa actual de protección de datos.



No obstante, se han identificado las siguientes carencias:

- No ha sido finalizado un análisis de riesgos sobre los tratamientos de datos personales conforme al artículo 32.2 del RGPD.
- No se han realizado las evaluaciones de impacto de los riesgos detectados de nivel alto
- No se han realizado auditorías en materia de protección de datos desde el año 2017.

Cumplimiento legalidad del registro de facturas

Está pendiente de realizar la auditoría del registro de facturas de 2020 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 la Diputación alcanza un **índice de madurez del 30,0%**, 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.

Gobernanza de ciberseguridad

La Diputación de Valencia tiene establecida una insuficiente gobernanza de la seguridad de la información.

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

Si bien en la auditoría hemos observado la existencia de un cierto nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores de la Diputación y los gestores y responsables de las áreas implicadas, **existen carencias relevantes que indican que la gobernanza no es adecuada**. Las carencias más relevantes identificadas, que dificultan el establecimiento de un sistema de gestión de la seguridad de la información (SGSI) efectivo, son las siguientes:

- La **falta de actualización de políticas y formalización de objetivos estratégicos** de la entidad, lo que invalida la utilidad de las políticas existentes, dado que estas no se corresponden con las necesidades reales de la organización.
- La **inexistencia de determinados roles clave** en la organización, como el responsable de seguridad, o la falta de actividad efectiva y continuada de los roles existentes en cuanto a los procesos relacionados con la seguridad de la información.

La inexistencia de un responsable de seguridad constituye probablemente la deficiencia más grave en términos de gobernanza, puesto que su responsabilidad, la



gestión de la seguridad de la información de los servicios prestados, no puede considerarse adecuadamente asumida por el resto de los responsables de la organización.

Del mismo modo, hemos verificado que ninguno de los recursos existentes en el Servicio de Informática dispone de dedicación completa a la seguridad de la información, dado que su dedicación es compartida entre múltiples competencias. Esta carencia de roles con dedicación exclusiva impide que el conjunto de acciones y medidas implantados puedan constituirse como procesos de ejecución continua y sean percibidos como acciones puntuales, dificultando el establecimiento de un SGSI efectivo.

- La **falta de actividad continuada del Comité de Seguridad**. Hemos verificado que, si bien el Comité de Seguridad ha sido formalmente constituido, este no ha tenido actividad en los últimos tres años ni existen grupos de trabajo auxiliares que hayan asumido total o parcialmente las funciones del comité en este periodo.

Esta falta de actividad del órgano, clave en el gobierno de la seguridad en tanto que promueve la toma de medidas, la mejora continua y la coordinación de los esfuerzos de las distintas áreas, impide la organización efectiva de la seguridad en la entidad.

- La **falta de cumplimiento normativo**. Tal y como se detalla en subapartados anteriores, existe un insuficiente nivel de cumplimiento de la legalidad en materia relacionada con la seguridad de la información.

No obstante, sí se han identificado algunos aspectos positivos:

- Apoyo en forma de inversiones y la articulación de medidas para la gestión de riesgos. Hemos verificado el incremento de las inversiones previstas para el ejercicio 2022 (en el momento de redactar este informe estaba pendiente de su incorporación definitiva al presupuesto) que permitirán el desarrollo de proyectos y la implantación de sistemas que tendrán un potencial impacto positivo en el nivel de seguridad de la organización.
- La coordinación por parte de los responsables de las áreas implicadas en la seguridad de la información con órganos de referencia, con objeto de promover proyectos comunes, mejoras en la gestión de la seguridad, y coordinar el tratamiento de incidentes.

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.



APÉNDICE 3

Buenas prácticas destacables



Introducción

Con carácter general, si una entidad alcanza una valoración del 80% en el índice de madurez de un control significa que está aplicando de forma razonable las buenas prácticas en materia de seguridad de la información establecidas en el ENS o en las guías profesionales correspondientes, que se sintetizan en el cuadro 5 de este informe. En otro caso la entidad debe adoptar medidas para mejorar su ciberseguridad y alcanzar dicha meta.

Adicionalmente a la valoración de los controles básicos de ciberseguridad, es conveniente destacar determinados aspectos, prácticas, soluciones técnicas o sistemas que han sido identificados o revisados durante la realización de la auditoría y que destacan en relación con el estado del arte sobre una determinada materia. Estos aspectos proporcionan por su singularidad un conocimiento adicional que facilita la interpretación, contextualización y evaluación de los resultados obtenidos en los procedimientos de auditoría para la valoración de los controles.

Además, dado el carácter positivo de los aspectos considerados en este apartado, su identificación puede, en determinados casos, constituir la base de sinergias entre administraciones públicas de la misma naturaleza y con características similares, ya que pueden ser replicadas si se dan necesidades y problemáticas comunes.

El criterio para determinar si un aspecto es considerado buena práctica destacable es la existencia de una o varias de las siguientes circunstancias:

- soluciones o sistemas especialmente avanzados o efectivos desde el punto de vista tecnológico,
- procesos de gestión particularmente maduros, y
- soluciones o procesos poco frecuentes entre las entidades auditadas, pero de demostrada eficacia frente a las necesidades de la entidad, independientemente de su complejidad o innovación.

Los aspectos destacados a continuación, en general, han sido considerados en la evaluación de los CBCS. No obstante, algunos no forman parte de los CBCS tal como están definidos en la GPF-OCEX 5313, pero los comentamos por las razones antes indicadas. Cabe aclarar que la existencia de aspectos concretos particularmente relevantes no implica necesariamente que el control global disponga de la madurez requerida, ya que su valoración incluye la consideración de un conjunto de aspectos técnicos, organizativos y formales que se deben alcanzar individualmente y en conjunto, con un determinado nivel de efectividad y madurez.

Coordinación con organismos de referencia en ciberseguridad

La entidad ha establecido una coordinación particularmente efectiva con la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) de la Generalitat y el Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV).



Dicha coordinación se ha materializado en diversos ámbitos:

- La gestión de incidentes de seguridad. Durante la realización del trabajo nos han informado de la materialización de determinadas amenazas a las que se hizo frente de forma conjunta por los técnicos de la Diputación y el personal del CSIRT-CV. Las medidas adoptadas durante la gestión de los incidentes fueron efectivas, minimizando su impacto, sin consecuencias relevantes en la operativa de la entidad. La implantación de las recomendaciones emitidas por el CSIRT-CV, junto con las del presente informe, reducirá la probabilidad de materialización de amenazas de similar naturaleza.
- La ejecución de proyectos colaborativos. Particularmente el proyecto vSOC (Centro de Operaciones de Seguridad Virtual), impulsado por la DGTIC y mediante la participación del CSIRT-CV, para la implantación de un sistema de monitorización, almacenamiento e interpretación de datos de determinados sistemas y servicios críticos que son ofrecidos por la Diputación a los ayuntamientos. Consideramos que la coordinación de distintas entidades en estas cuestiones es esencial.
- El asesoramiento técnico en la implantación de medidas para permitir el teletrabajo durante el periodo de pandemia. La Diputación ha aplicado un conjunto de configuraciones específicas para la securización de las conexiones remotas según las recomendaciones del CSIRT-CV, como consecuencia de la implantación mayoritaria del teletrabajo en respuesta a la crisis sanitaria del COVID-19.

Explotación de la herramienta de ticketing en determinados procesos de la entidad

La entidad ha desplegado una herramienta de *ticketing* y gestión de flujos de trabajo que ha sido integrada con determinados sistemas y procesos internos de una manera particularmente efectiva.

Las implementaciones y funcionalidades más relevantes de la herramienta son:

- La integración con el servicio de directorio y la plataforma de virtualización, que permite la obtención automática de datos de los activos y facilita la actualización y gestión del inventario.
- El registro automático en la herramienta de las vulnerabilidades identificadas como resultado de las auditorías periódicas del CSIRT-CV, facilitando su gestión y resolución.
- La integración de procesos de gestión de determinadas copias de seguridad, en una implementación particularmente adecuada de las tareas relacionadas, creación de registros en la base de datos de conocimientos de la herramienta y soporte documental para formalización de los procesos de gestión.



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 de la Diputación (en particular, el presidente o la presidenta 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.



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 diputado o diputada delegada responsable de los sistemas de información y las comunicaciones, y a los funcionarios directores del departamento TIC y los jefes de área o servicio.

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

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

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

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

Prueba de penetración: Es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos.

Sistema de gestión de eventos e información de seguridad: Un SIEM, del término inglés *security information and event management*, es un sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad. Permite un análisis de la situación desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales.



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



TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, el borrador previo del Informe de auditoría se discutió con la diputada de Informática y Tecnología y el jefe del Servicio de Informática para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

Posteriormente, en cumplimiento del artículo 16 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre, 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 al ejercicio 2021, el mismo se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Dentro del plazo concedido, la Diputación ha formulado las alegaciones que ha considerado pertinentes.

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

- 1) Todas las alegaciones han sido analizadas detenidamente.
- 2) Las alegaciones admitidas se han incorporado al contenido del Informe.

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



APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre, y del artículo 55.1.h) de su Reglamento de Régimen Interior y de los programas anuales de actuación de 2020 y 2021 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 2 de febrero de 2022, aprobó este informe de auditoría.



ANEXO I

Alegaciones presentadas



SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

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

JUSTIFICANTE DE PRESENTACIÓN EN REGISTRO ELECTRÓNICO

NÚMERO DE REGISTRO 202200123	FECHA DE ENTRADA 14/01/2022 8:34
ÁREA Fiscalización - Alegaciones	PROCEDIMIENTO PAA2021/25 Auditoría de los controles básicos de ciberseguridad de las diputaciones
DATOS DEL PRESENTADOR Nombre: MYRIAM VITON GARCIA NIF / CIF: E-mail: Entidad: DIPUTACIÓ PROVINCIAL DE VALÈNCIA	
FIRMA DIGITAL 68186F9F3DA3C6386CB49E6BD1CAF3AC4A76B050	
DOCUMENTOS ENVIADOS Fichero1: 25418608C_2022114_cl_Certificado convocatoria.pdf Fichero2: 25418608C_2022114_cl_alegacion firmada.pdf	

Documento	Identificadores	
FIRMA PRESIDENTE ALEGACIONES INFORME SINDICATUR...		
Código de verificación	Otros datos	Página 1 de 3
928218A2-3272AEFA-A8C79D99-63A66A2		

Muy Sr. Mío:

Habiendo tenido entrada en el Registro de la Diputación de València el pasado 27 de diciembre de 2021 el borrador del Informe realizado por la Sindicatura de Cuentas de los controles básicos de ciberseguridad de la Diputación de Valencia, ejercicio 2021 otorgando plazo de alegaciones a esta misma Diputación hasta el 17 de enero de 2022, se adjuntan las correspondientes alegaciones previo a la emisión del Informe Definitivo.

Estimat senyor:

Havent tingut entrada en el Registre de la Diputació de València el passat 27 de desembre de 2021 l'esborrany de l'Informe realitzat per la Sindicatura de Comptes dels controls bàsics de ciberseguretat de la Diputació de València, exercici 2021 atorgant termini d'al·legacions a aquesta mateixa Diputació fins al 17 de gener de 2022, s'adjunten les corresponents al·legacions previ a l'emissió de l'Informe Definitiu.

SÍNDIC MAJOR

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

VICENT CUCARELLA TORMO

FIRMADO

Documento	Identificadores	
FIRMA PRESIDENTE ALEGACIONES INFORME SINDICATUR...		
Código de verificación	Otros datos	Página 2 de 3
928218A2-3272AEFA-A8C79D99-63A66A2		

Alegaciones que se formulan al borrador del Informe de Auditoría de los controles básicos de ciberseguridad de la Diputación de Valencia, ejercicio 2021

Primera alegación (y única) al texto:

- Apartado 4 CONCLUSIONES del borrador del Informe, página 8, párrafo *“La Diputación de Valencia no tiene establecida una adecuada gobernanza de la ciberseguridad y debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información”*
- Apartado “Indicadores” del Apéndice 2: Situación de los controles básicos de Ciberseguridad del CBCS 8. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD, página 43, párrafo *“Del mismo modo, hemos verificado que ninguno de los recursos existentes en el Servicio de Informática dispone de dedicación completa a la seguridad de la información, dado que su dedicación es compartida entre múltiples competencias. Esta carencia de roles con dedicación exclusiva impide que el conjunto de acciones y medidas implantados puedan constituirse como procesos de ejecución continua y sean percibidos como acciones puntuales, dificultando el establecimiento de un SGSI efectivo”*

Contenido de la alegación:

Aún siendo conscientes los órganos de gobierno de la Diputación de Valencia de que se hace necesario establecer una adecuada gobernanza de la ciberseguridad en esta institución y dedicar los recursos necesarios para ello, sin embargo, en cuanto a los recursos asignados al departamento de TI y a la seguridad de los sistemas de Información sí se ha intentado evolucionar los recursos humanos del año 2020 al año 2021, incrementando de dos a tres el número de personas dedicadas a la seguridad de los sistemas de información, aunque hasta el momento no haya sido posible cubrir ese puesto de trabajo tal y como se detalla a continuación:

En el pleno extraordinario de la Diputación de 30 de diciembre de 2019 se creó un puesto nuevo de TÉCNICO SUPERIOR DE SEGURIDAD clasificado como A1 20 A3 con las siguientes funciones a realizar:

- Participar y liderar proyectos de análisis, diseño, desarrollo e implantación de plataformas y herramientas de seguridad de sistemas y redes, junto con el personal del servicio de Informática implicado en estas mismas labores.
- Coordinar al Servicio de Informática con la Delegación de Protección de Datos y con los organismos o servicios externos que auditan o supervisan la seguridad TIC, para la resolución de las incidencias relacionadas con la seguridad.
- Liderar la aplicación de las normativas de seguridad y la definición de los procedimientos de seguridad internos en las infraestructuras informáticas de la corporación.

FIRMADO

1.- DIPUTACION - Presidente Diputación

- Antoni F. Gaspar Ramos

14-ene-2022 08:23:13

Documento	Identificadores	
FIRMA PRESIDENTE ALEGACIONES INFORME SINDICATUR...		
Código de verificación	Otros datos	Página 3 de 3
928218A2-3272AEFA-A8C79D99-63A66A2		

- Colaborar en las auditorías de seguridad que periódicamente evalúan los sistemas informáticos de la Diputación de Valencia.

No obstante, si bien la finalidad con la creación de este nuevo puesto era pasar de tener 2 personas dedicadas en el año 2020 a tener 3 personas dedicadas en el año 2021 (adicional a un recurso externo contratado), no ha sido posible cubrir esta vacante por causas que se quedan fuera del alcance de la organización.

Se publicó la convocatoria para cubrir este nuevo puesto en Comisión de Servicios durante el año 2020 (expediente 11227/20/PER) pero no se presentaron candidatos. Posteriormente, en el pleno de la Diputación de 16 de febrero de 2021 se modifica su clasificación a A1 20 C1, mejorando las condiciones retributivas respecto del puesto creado inicialmente. Volvió a publicarse la convocatoria para cubrirlo en Comisión de Servicios durante el ejercicio 2021 (expediente 1696/21/PER), presentándose un único candidato que no cubría el perfil, por lo que se declaró desierta.

Así pues, se quiere enfatizar que teniendo presente la importancia que tiene la Seguridad de Información para nuestra organización y pese a no disponer de todos los recursos humanos para una mejor gestión de la misma, se han continuado realizando nuevas actuaciones encaminadas a mejorar la Seguridad Informática, siendo ello posible debido a la gran implicación del personal ya dedicado a ello.

Documentación justificativa de la alegación (se adjunta):

- Certificado del Jefe de Servicio de Gestión y Desarrollo de los Recursos Humanos de la Diputación de Valencia.

FIRMADO



ANEXO II

Informe sobre las alegaciones presentadas



ANÁLISIS DE LAS ALEGACIONES EFECTUADAS POR LA DIPUTACIÓN DE VALENCIA AL BORRADOR DEL INFORME DE AUDITORÍA DE CIBERSEGURIDAD DEL EJERCICIO 2021

Mediante el escrito de esta Sindicatura de 27 de diciembre de 2021 se remitió a la Diputación de Valencia el borrador del Informe de auditoría, para que efectuase las alegaciones que considerase oportunas. Con fecha 14 de enero de 2022 se recibieron por el registro electrónico las alegaciones formuladas y respecto a estas se señala lo siguiente:

Única alegación

Apartado 4, "Conclusiones", del borrador del Informe, segundo subapartado

"La Diputación de Valencia no tiene establecida una adecuada gobernanza de la ciberseguridad y debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información."

Apartado "Indicadores" del "CBCS 8. Cumplimiento normativo y gobernanza de ciberseguridad" del apéndice 2, "Situación de los controles básicos de ciberseguridad", página 43, segundo párrafo

"Del mismo modo, hemos verificado que ninguno de los recursos existentes en el Servicio de Informática dispone de dedicación completa a la seguridad de la información, dado que su dedicación es compartida entre múltiples competencias. Esta carencia de roles con dedicación exclusiva impide que el conjunto de acciones y medidas implantadas puedan constituirse como procesos de ejecución continua y sean percibidos como acciones puntuales, dificultando el establecimiento de un SGSI efectivo."

Comentarios

En la alegación se indica que la Diputación es consciente de la necesidad de "establecer una adecuada gobernanza de la ciberseguridad en esta institución y dedicar los recursos necesarios".

No obstante, en la alegación se señala que sí se han intentado mejorar los recursos humanos del año 2020 al año 2021, incrementando de dos a tres el número de personas dedicadas a la seguridad de los sistemas de información asignadas al departamento de TI y a la seguridad de los sistemas de información. Este compromiso se ha materializado mediante la creación de un nuevo puesto de técnico superior de seguridad, pero "no ha sido posible cubrir esta vacante por causas que se quedan fuera del alcance de la organización".

En la realización de la auditoría hemos podido comprobar que, en la actualidad, efectivamente el departamento de TI dispone de recursos personales cuya dedicación a las



tareas relacionadas con la seguridad de la información suponen, en conjunto, un esfuerzo aproximado equivalente a dos personas. También hemos comprobado que en 2019 se creó el puesto de "Técnico superior de seguridad" con dedicación plena a esta materia. Pero la realidad es que a fecha de este informe el puesto sigue sin estar cubierto.

Consideramos, por consiguiente, que la alegación presentada no comporta una modificación en el contenido del informe. La creación del nuevo puesto de "Técnico superior de seguridad" supone una actuación acertada, pero la cobertura y la efectiva dotación de responsabilidades de dicho puesto constituyen un requisito imprescindible para alcanzar los niveles requeridos en cuanto a gobernanza de la seguridad y recursos humanos necesarios.

Consecuencias en el Informe

No se modifica.



Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Informe auditoría CBCS Diputación de Valencia 2021 cas - SEFYCU 3048321

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 R2VY ZEKK ZMAT 333N

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 - 08/02/2022 7:36
VICENT CUCARELLA TORMO