SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DE LA DIPUTACIÓN DE CASTELLÓN

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 Castellón.

Conclusiones

El índice de madurez general de los CBCS muestra un valor del 63,7%, pero todavía debe mejorar para alcanzar el objetivo del 80%. No se han identificado deficiencias graves de control y todos los CBCS analizados alcanzan un nivel de madurez N2, pero existen claras posibilidades de mejora para alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información. Para subsanar las principales deficiencias detectadas se han realizado las pertinentes recomendaciones.

Hemos podido verificar que la Diputación tiene establecida una aceptable 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 nivel razonable de adecuación a las normas legales. No obstante, 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 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 los procedimientos de seguridad existente para todos los controles analizados, implantar soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa (CBCS 1), elaborar y aprobar un plan anual de mantenimiento y un catálogo de aplicaciones autorizadas (CBCS 2) y la ejecución de pruebas periódicas de recuperación de copias de seguridad (CBCS 7).

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 Castellón

Ejercicio 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

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

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

En 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 fundamental[2] 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 debe mejorar

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 63,7%**, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles se realizan, pero existen controles parcialmente establecidos o no formalizados documentalmente. Los resultados detallados obtenidos para cada uno de los CBCS se muestran en el cuadro 1.

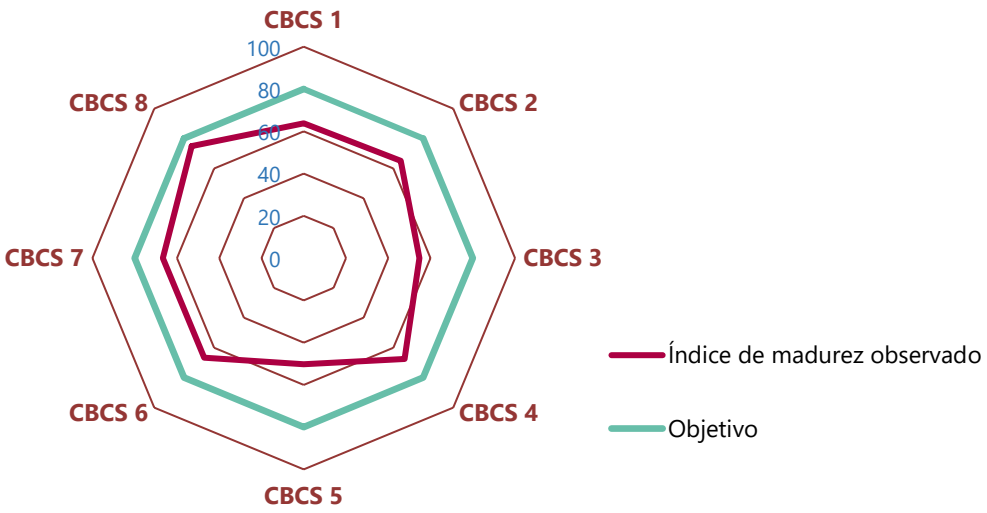
Cuadro 1. Índice de madurez de los controles básicos de ciberseguridad

Control	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	63,8%	N2	79,7%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	65,0%	N2	81,3%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	54,8%	N2	68,4%
CBCS 4 Uso controlado de privilegios administrativos	67,5%	N2	84,3%
CBCS 5 Configuraciones seguras del *software* y *hardware*	50,3%	N2	62,8%
CBCS 6 Registro de la actividad de los usuarios	66,7%	N2	83,3%
CBCS 7 Copias de seguridad de datos y sistemas	66,7%	N2	83,3%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	75,0%	N2	93,8%
General	63,7%	N2	79,6%

El índice de cumplimiento de los CBCS es del 79,6%, 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



Por tanto, si bien no se han identificado graves deficiencias de control y se dispone de un nivel de madurez homogéneo en todos los aspectos analizados, existen claras posibilidades de mejora para alcanzar los niveles exigidos por el ENS para la protección de los sistemas

de información. 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 Castellón tiene establecida una aceptable gobernanza de la ciberseguridad, pero 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 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.

Durante la auditoría hemos podido verificar la existencia de este compromiso con la ciberseguridad por parte de los órganos superiores de la Diputación, lo que, junto con la existencia de unos adecuados procesos de gestión, nos permite afirmar que la gobernanza de ciberseguridad presenta un nivel aceptable.

No obstante, los órganos superiores de la Diputación deben reforzar el actual nivel de apoyo y compromiso con la seguridad de los sistemas de información, con objeto de alcanzar los niveles de madurez de los controles requeridos por el ENS y solventar las deficiencias identificadas. Con esta finalidad resulta preciso impulsar de forma proactiva iniciativas para mejorar la ciberhigiene y la ciberresiliencia.

En ese sentido, los órganos de gobierno ostentan responsabilidad no solo en el cumplimiento legal, sino que deben liderar y ser ejemplarizantes en sus acciones y decisiones, como parte de un proceso de concienciación de la entidad. La existencia de un liderazgo reconocible por toda la corporación puede fomentar los avances en términos de concienciación, permitiendo vencer las naturales resistencias que puedan existir en la organización a los cambios necesarios.

Por otra parte, y si bien hemos verificado el alto nivel de compromiso de los gestores y responsables de la seguridad, su dedicación es compartida entre múltiples competencias, dado que ninguno de los roles existentes dispone de dedicación completa a la seguridad de la información y la protección de los datos, que consideramos indispensable en un ente del tamaño de la Diputación con sus complejos sistemas de información. Esta carencia de roles con dedicación exclusiva impide que el conjunto de acciones y medidas implantados puedan constituirse como procesos de ejecución continua y son percibidos como acciones puntuales, dificultando el establecimiento de un sistema de gestión de la seguridad de la información efectivo.

Es necesario, por tanto, la incorporación de recursos con dedicación exclusiva a la seguridad o la reasignación de responsabilidades, de manera que sea posible una gestión continuada de las medidas y procesos de seguridad.

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

La revisión del cumplimiento de legalidad en materia relacionada con la seguridad de la información ha puesto de manifiesto un nivel razonable de adecuación a las normas legales. No obstante, en el apartado 5 se señalan varios aspectos pendientes de mejora sobre los que se debe actuar para su pronta subsanación.

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

Para subsanar las deficiencias de control, 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 y procedimientos de seguridad existentes 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. Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa y finalizar la implantación de medidas compensatorias actualmente en fase de despliegue.

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

3. Actualizar la normativa y procedimientos de seguridad existentes 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 plan anual de mantenimiento y un catálogo de aplicaciones autorizadas, documentos previstos en el procedimiento aprobado existente.

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

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

5. Modificar el procedimiento actual 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.
   - El uso de la herramienta de gestión de flujos de trabajo, que ya está disponible en la entidad, para dar soporte a las tareas que se realizan actualmente en la identificación y remediación de vulnerabilidades.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

6. Modificar y mejorar el procedimiento de gestión de usuarios y privilegios actualmente aprobado, de manera que detalle las acciones actualmente implantadas. Por otra parte, aplicar los principios y medidas detallados en el procedimiento, en particular lo siguiente:

   - 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)

7. Actualizar y mejorar el actual procedimiento de 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 que permitan asegurar la eficacia del control. 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 incluir la gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad, en el procedimiento existente, o desarrollar un procedimiento específico. Dicho procedimiento debe contemplar las medidas actualmente implantadas en determinados sistemas críticos y

la monitorización y revisión periódica de los cambios no autorizados en el resto de sistemas.

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

8. Modificar y mejorar el procedimiento actualmente aprobado para el tratamiento de los registros de actividad de los usuarios, de manera que detalle las acciones actualmente implantadas. También se deben aplicar de forma efectiva los principios y medidas detallados en el procedimiento, particularmente los siguientes:

   – Establecer las medidas necesarias para cumplir los periodos de retención especificados en el procedimiento vigente.

   – Incluir la totalidad de sistemas de la entidad en las herramientas de gestión de registros de actividad disponibles.

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

9. Aunque existe un procedimiento de copias aprobado, existen varios aspectos a mejorar, en particular:

   – Debe incluirse de forma detallada el control realmente implantado y recoger el uso de herramientas de control de tareas o flujos de trabajo.

   – La ejecución de pruebas periódicas de recuperación planificadas.

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

Aunque el grado de cumplimiento es elevado, existen varios aspectos sobre los que la Diputación debe actuar para subsanarlos:

10. 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 de nivel MAYOR identificadas en la auditoría de cumplimiento realizada, que le permitirá obtener la certificación de conformidad y el distintivo correspondiente para su publicación en la sede electrónica.

11. En relación con la protección de datos personales, la Diputación debe planificar y ejecutar las auditorías de cumplimiento en materia de protección de datos y aplicar las medidas organizativas y técnicas necesarias para proteger los datos personales, de acuerdo con el artículo 24.1 del Reglamento General de Protección de Datos.

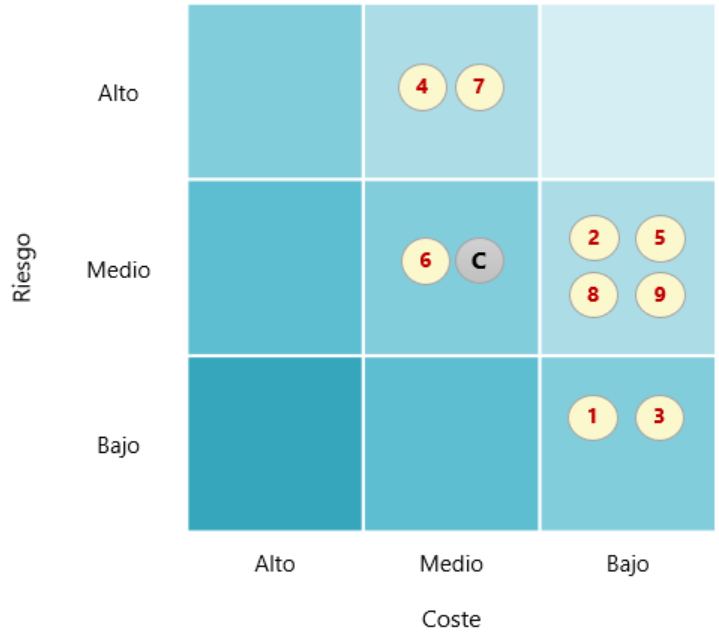
12. En relación con la Ley de Factura Electrónica, la Diputación debe realizar las auditorías de sistemas anualmente tal como exige esa norma.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente 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 10 a 12 anteriores, ya que son medidas de obligado cumplimiento.

También se incluye en el gráfico la recomendación pendiente de implementar de nuestro anterior informe, con la referencia C, que se comenta 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 tres recomendaciones realizadas en ese informe, solo una no se ha atendido.

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	
A	La Diputación debe aplicar estrictamente los procedimientos aprobados para la gestión de usuarios y derechos de acceso, particularmente en la gestión de bajas de usuarios, con objeto de evitar la dependencia de controles manuales por parte del Departamento de Informática. Igualmente, recomendamos que se ejecute periódicamente y según un proceso automatizado una revisión de la actividad de los usuarios de los sistemas críticos de la Diputación, con objeto de identificar usuarios incorrectamente habilitados y verificar la correcta asignación de privilegios.	Hemos verificado que han sido implantadas medidas para la comunicación automática de las bajas por parte de personal al Servicio de Informática. Estas comunicaciones son gestionadas para la desactivación de usuarios en el sistema. Adicionalmente, se han automatizado análisis periódicos para la identificación de usuarios que dispongan de una configuración anómala de cuentas y mecanismos de autenticación.	**Total o sustancialmente aplicada**
B	Recomendamos a la Diputación de Castellón 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. La Diputación de Castellón ha iniciado un proceso de contratación pública para el proyecto de desarrollo de dicho plan de continuidad, que de acuerdo con los plazos establecidos deberá finalizar su ejecución en el primer cuatrimestre del 2019. Una vez establecido y aprobado el plan de continuidad, deberán realizarse pruebas periódicas de este para verificar su correcto funcionamiento en caso de desastre y dejar documentadas dichas pruebas.	Hemos verificado que ha sido aprobado, por parte del Comité de Seguridad, un plan de continuidad de negocio que recoge los aspectos necesarios, incluyendo la identificación de servicios esenciales, las responsabilidades, el análisis del impacto, las estrategias de recuperación, las fases del plan de continuidad y un plan de pruebas. En el momento de redacción del presente informe se está realizando la formación a los intervinientes y gestionando la ejecución del plan de pruebas incluido en el plan de continuidad.	**Total o sustancialmente aplicada**
C	La Diputación debería configurar políticas de control de accesos al sistema Estima para que se ajuste a las buenas prácticas generalmente aceptadas y las exigencias del ENS.	Hemos constatado que la recomendación está pendiente de aplicación.	**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 buena parte de las recomendaciones anteriores. Estas actuaciones se encuentran en su mayoría recogidas en el plan de la Diputación para la corrección de no conformidades con el ENS o se han iniciado como consecuencia de las observaciones realizadas en el transcurso de esta auditoría. La implantación efectiva de estas 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:

- La implantación efectiva de un plan de continuidad del negocio (PCN). Dicho plan ha sido elaborado y aprobado, y en el momento de redacción del presente informe se está realizando la formación pertinente y gestionando la ejecución del plan periódico de pruebas incluido en el PCN.

- La implantación de un sistema de provisión de aplicativos y escritorios virtualizados en la totalidad de la organización (véase apéndice 3, "Buenas prácticas destacables"). El despliegue del sistema, que actualmente afecta a dos tercios de la organización, está planificado para ser completado a finales del año 2021.

- La implantación de un sistema de autenticación de doble factor en la totalidad de la organización (véase apéndice 3, "Buenas prácticas destacables"). El sistema ha sido implantado para un tercio del personal. Se ha licitado un proyecto para la provisión de certificados a la totalidad de empleados y se encuentra en estudio su integración con el sistema de provisión de aplicativos y escritorios virtualizados.

- La implantación de un sistema de gestión de eventos e información de seguridad (SIEM). Ha sido contratada la implantación del SIEM proporcionado por el Centro Criptológico Nacional, que analizará los registros de actividad de los sistemas más relevantes desde el punto de vista de la seguridad. El proyecto se encuentra en la actualidad en fase de planificación.

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 INES[3] del CCN revela que las organizaciones no siempre implementan ni tan siquiera las medidas más básicas que podrían haber evitado o mitigado el daño causado. Por otro lado, el hecho de que los ciberataques permanezcan en muchos casos sin ser detectados durante mucho tiempo puede ser evidencia de que las medidas básicas no están correctamente implementadas.

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 diseño[4] como sobre su eficacia operativa[5] para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte, 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.

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

[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.

- 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.

También consideramos de interés, para comprender mejor la importancia de los CBCS, la lectura de nuestro informe "Auditoría de los controles básicos de ciberseguridad de los mayores ayuntamientos de la Comunitat Valenciana. Ejercicios 2019 y 2020", en cuyo apartado 5 hay, para cada uno de los controles, un apartado denominado **"Por qué es importante este control básico de ciberseguridad"**.

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 2. Los CBCS y el ENS

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

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

Los CBCS como medidas de ciberhigiene

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

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

En esa dirección, ENISA establece diez puntos de acción para una adecuada ciberhigiene. Como se observa en el cuadro 3, de los siete CBCS, sin contar el de cumplimiento normativo, cinco son coincidentes con los puntos de acción prioritarios recomendados por ENISA como buenas prácticas de ciberhigiene.

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

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

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

Cuadro 3. Puntos de acción de ENISA

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

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

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 4. Los CBCS y sus subcontroles

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

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

Evaluación de los resultados del trabajo

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

Subcontroles

Los CBCS son controles globales compuestos por varios controles detallados o subcontroles (tal como puede verse en el cuadro 4 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 5. Evaluación de los subcontroles

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

Controles

Para determinar la situación global de cada control de ciberseguridad hemos utilizado el **modelo de nivel de madurez** de los procesos de control de acuerdo con lo establecido en la GPF-OCEX 5313, que a su vez están basadas en la *Guía de seguridad CCN-STIC 804* del CCN, usando una escala que se resume en el siguiente cuadro.

Cuadro 6. Niveles de madurez

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

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

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

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

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

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

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indicadores globales

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

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

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

Gobernanza de ciberseguridad

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Seguimiento de las recomendaciones

En el presente trabajo se ha realizado el seguimiento de las recomendaciones recogidas en el 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 acciones para mantener actualizado el inventario y control de activos físicos de la entidad que se encuentran respaldadas por la normativa de seguridad vigente, que establece formalmente la responsabilidad del inventariado de dispositivos.

La Diputación dispone de diversas herramientas e inventarios destinados a administrar los activos físicos y puede considerarse que, en conjunto, proporcionan un adecuado control sobre estos activos. Los equipos de usuario y el equipamiento de red son gestionados mediante dos aplicativos que realizan el descubrimiento automático de los elementos, bien mediante la instalación de un agente en el bastionado inicial, bien mediante detección automática. Para el resto de los activos se dispone de inventarios de gestión manual.

Adicionalmente, hemos verificado que existe un adecuado proceso de gestión y aprobación de nuevos activos y retirada o sustitución de activos existentes. Además, la Diputación ha configurado las herramientas de inventariado para relacionar los activos físicos con las licitaciones y contratos de mantenimiento correspondientes.

Por otra parte, no se dispone de un sistema o control integral que impida la conexión de dispositivos físicos no autorizados a la red, pero se encuentran en fase de despliegue determinadas medidas y configuraciones que, en conjunto, pueden compensar parcialmente la ausencia de esos controles. Adicionalmente, se dispone de diferentes controles compensatorios robustos que detectan, impiden o limitan la actividad de los dispositivos físicos no autorizados en determinadas zonas críticas o vulnerables de la red.

Existe cierto nivel de control sobre el inventario y el control de activos físicos, y su valoración global alcanza un **índice de madurez del 63,8%,** que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 1 del 79,7%**.

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, si bien la responsabilidad del inventariado de *software* se encuentra establecida en la normativa de seguridad vigente, el control implantado no ha sido completamente detallado en el conjunto de procedimientos formalmente aprobados.

La Diputación ha implantado una elaborada solución basada en la virtualización de puestos de trabajo y aplicaciones que es utilizada para la provisión de la mayor parte de aplicativos. La configuración específica aplicada permite una gestión eficiente del inventario de aplicaciones, así como de sus vulnerabilidades, versiones, licencias y derechos de acceso de los usuarios.

Para el resto de *software* utilizado, la Diputación dispone de un inventario de gestión automatizada para la administración de los activos *software* instalados en los equipos de usuario. El inventario incluye la información suficiente para una adecuada gestión de versiones y licencias.

Por otra parte, se ha evidenciado la existencia de un reducido número de equipos, servidores y equipos de usuario, con sistemas operativos fuera del periodo de soporte del fabricante, hecho que supone un riesgo para los sistemas de información.

La gestión del licenciamiento y el mantenimiento de aplicaciones se realiza mediante un proceso adecuado, pero que no está formalizado, dado que no se ha elaborado y aprobado un plan anual de mantenimiento del *software*.

La entidad cuenta con medidas orientadas a impedir el uso de *software* no autorizado que pueden considerarse razonablemente efectivas, además de disponer de un proceso de autorización para la instalación y uso de nuevo *software*.

Existe cierto nivel de control sobre el inventario y control de *software* autorizado, que alcanza un **índice de madurez del 65,0%,** que se corresponde con un **nivel de madurez *N2*, *repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 2 del 81,3%**.

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 la gestión de vulnerabilidades realizada por la Diputación y hemos observado que se realizan diferentes acciones con el objeto de identificar y remediar vulnerabilidades, acciones que se encuentran parcialmente recogidas en un procedimiento formalmente aprobado.

La identificación y remediación de vulnerabilidades se realiza sobre todos los sistemas que hemos revisado, bien por parte de terceros mediante contratos de mantenimiento, bien directamente por parte del personal del Servicio de Informática.

La identificación de vulnerabilidades realizada por la propia Diputación se articula mediante suscripción a listas de difusión de fabricantes y organismos de referencia, y a través de una herramienta que permite la identificación automática de vulnerabilidades de los sistemas críticos.

La priorización y resolución se gestionan de manera informal, pero no se encuentran recogidas en el procedimiento aprobado. El proceso completo no se encuentra totalmente definido ni está soportado por herramientas de gestión de flujos de trabajo, lo que impide una gestión totalmente eficaz.

Sobre la aplicación de parches y actualizaciones de seguridad, se aplican de forma sistemática mediante una herramienta para el despliegue centralizado de actualizaciones y parches en el caso de sistemas con numerosos activos, y de manera manual en el resto de sistemas, incluidos los sistemas críticos.

Existe un determinado número de sistemas críticos sobre los que la Diputación ha identificado vulnerabilidades que no han sido resueltas, lo que supone un riesgo relevante. La Diputación nos ha indicado que se ha aceptado el riesgo de dichas vulnerabilidades porque se ha experimentado, durante la aplicación de parches y actualizaciones, diversos incidentes con afección a la operativa de estos sistemas críticos y su resolución puede suponer un riesgo mayor que el que se pretende eliminar.

Existe cierto nivel de control sobre la gestión de vulnerabilidades, siendo la valoración global del control de un **índice de madurez del 54,8%,** que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 3 del 68,4%**.

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 que realiza la Diputación para el control de las cuentas de administración y hemos verificado que existe un control parcialmente efectivo, pero únicamente determinadas acciones del proceso se encuentran recogidas en un procedimiento aprobado.

La gestión 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 el procedimiento que establece las políticas comunes de gestión de privilegios administrativos no ha sido implantado de manera general en la Diputación. Hemos verificado una correcta aplicación del principio del mínimo privilegio en la gestión de privilegios administrativos realizada por el Servicio de Informática.

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

El uso dedicado de cuentas de administración se encuentra correctamente implantado en la entidad para la mayor parte de los sistemas, disponiendo los administradores de cuentas diferenciadas dependiendo de las tareas a realizar. No obstante, en las aplicaciones que soportan los procesos de gestión contable y recaudatoria, dichas cuentas no son creadas y utilizadas de manera adecuada.

Se han establecido formalmente requisitos de autenticación en una política de contraseñas, que ha sido adecuadamente implementada en los sistemas Windows y en aquellos que han implementado SSO (*single sign-on*) con el controlador de dominio, integración que ha sido realizada de manera particularmente efectiva en la Diputación, proporcionando una política de autenticación homogénea en estos sistemas. En el resto de los sistemas, no se realiza una configuración de requisitos de autenticación conforme a la política establecida.

Finalmente, los registros de actividad de los usuarios administradores se encuentran activados y almacenados en todos los sistemas revisados, disponiendo la Diputación de diversas aplicaciones y sistemas que permiten la centralización de estos registros de actividad, lo que facilita su gestión y revisión.

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 67,5%**, 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 84,3%**.

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 de la Diputación para el control de la configuración segura en aplicaciones y dispositivos y hemos verificado que existe un procedimiento formalmente aprobado. No obstante, este procedimiento no dispone del detalle suficiente y no representa con total fidelidad el control implantado.

Hemos verificado que se han establecido configuraciones y se dispone de plantillas para la configuración de determinados sistemas que, si bien no tienen como único objeto la seguridad, sí tienen en consideración ciertos criterios de bastionado y proporcionan un nivel de seguridad homogéneo en los sistemas. No obstante, no se han identificado medidas de gestión que permitan asegurar la correcta elaboración y aplicación de configuraciones seguras, hecho que, si bien no implica necesariamente una aplicación incorrecta del control, sí impide asegurar su eficacia en todos los casos.

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 y monitorizar cambios no autorizados, asegurando la integridad de las configuraciones de estos sistemas.

La valoración global del control sobre las configuraciones seguras es que la organización 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 5 del 62,8%**.

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 y medidas aplicadas por la Diputación para el registro de la actividad de los usuarios en los distintos sistemas y hemos verificado que, aunque se dispone de un procedimiento formalmente aprobado, este no describe con total exactitud 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 que define el fabricante y no se han aplicado configuraciones o medidas específicamente destinadas al cumplimiento de los requisitos detallados en el procedimiento aprobado.

No obstante, la Diputación dispone de diversos sistemas para la gestión de registros de actividad de determinados activos, lo que supone una mejora notable de la configuración básica por defecto de los registros de auditoría. Estas herramientas integran la mayor parte de los sistemas relevantes desde el punto de vista de la ciberseguridad y facilitan la retención y protección de los registros.

La centralización de registros de actividad en sistemas externos simplifica el análisis de los datos disponibles en caso de incidente de seguridad, si bien hemos verificado que la revisión de dichos registros de actividad se realiza de forma reactiva e informal.

Los sistemas disponibles para la gestión de registros no pueden ser considerados un SIEM por sus especificaciones técnicas y funcionales, pero pueden considerarse una medida de seguridad compensatoria parcialmente eficaz. No obstante, la Diputación ha contratado recientemente un proyecto para el despliegue de una solución SIEM del CCN, que integrará información de determinados sistemas críticos desde el punto de vista de la seguridad y que se encuentra en fase de planificación.

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 66,7%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 6 del 83,3%**.

CBCS 7. COPIA DE SEGURIDAD DE DATOS Y SISTEMAS

Objetivo del control

Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.

Situación del control

La Diputación realiza diversas acciones para el control de la copia de seguridad de los datos y sistemas que se encuentran recogidas en un procedimiento aprobado. No obstante, este procedimiento se encuentra desactualizado y no representa con total fidelidad el control implantado.

Adicionalmente, la entidad cuenta con un plan de continuidad de negocio que considera la realización de copias de seguridad como parte de las estrategias de recuperación frente a determinados escenarios

La Diputación ha finalizado recientemente el despliegue de una solución de copia que dispone de las 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 departamento TIC.

Hemos verificado que la gestión y revisión de copias 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, si bien no implica necesariamente una aplicación incorrecta del control de copias, sí impide asegurar la eficacia del control en todos los casos.

La solución técnica incluye distintos mecanismos destinados a la protección de las copias de seguridad que pueden considerarse efectivos frente a una diversidad de amenazas.

No se realizan de forma sistemática pruebas de recuperación planificadas como parte de un proceso de pruebas, si bien hemos confirmado que se realizan y registran frecuentes recuperaciones satisfactorias de diversos tipos de copias en caso de pérdida de datos o servicios.

La valoración global del control existente sobre las copias de seguridad es que la Diputación alcanza un **índice de madurez del 66,7%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 7 del 83,3%**.

CBCS 8. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD

Objetivo del control

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

Situación del control

Cumplimiento del ENS

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:

- La Diputación ha elaborado una política de seguridad de la información (PSI) que ha sido revisada, actualizada y aprobada por el Pleno de la Diputación. Actualmente se encuentra en vigor la versión 5 y su contenido se adecua a los requisitos establecidos por el ENS.

- Se han designado los responsables previstos en la PSI y se ha creado el Comité de Seguridad.

- Se ha desarrollado la normativa asociada a la PSI, que incluye aspectos para el uso de los sistemas y dispositivos, la política de acceso a internet y correo electrónico, etc.

- La Diputación ha determinado categorizar de nivel ALTO sus sistemas, valorando la importancia de la información manejada y de los servicios prestados en las dimensiones de seguridad correspondientes. No obstante, a efectos de la presente auditoría y con objeto de mantener criterios homogéneos con el resto de las diputaciones auditadas lo hemos considerado como de nivel medio.

- Se dispone de declaración de aplicabilidad.

- Se ha cumplimentado y remitido Informe del Estado de la Seguridad (Informe INES).

- Desde el año 2016 se han ejecutado diversos proyectos de asistencia técnica para adecuación al ENS, con asistencia de un proveedor externo, en el marco de los cuales se realizó en el año 2018 una auditoría de cumplimiento, prevista en el artículo 34 del ENS, en la que se identificaron diversas no conformidades y se han iniciado acciones para solventarlas. Únicamente ha sido identificada una no conformidad de carácter mayor, por ausencia de plan de continuidad. Dicho plan ha sido elaborado y aprobado y su implantación efectiva se encuentra en fase de finalización, incluyendo la formación al personal y la realización de las pruebas periódicas previstas en el plan.

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

- No han sido solventadas la totalidad de no conformidades identificadas en la auditoría de cumplimiento, por lo que no se ha certificado el cumplimiento del ENS.

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 creado una Oficina Provincial de Protección de Datos y Seguridad, con el objetivo de desarrollar las funciones previstas en la normativa nacional y comunitaria relativas al delegado de protección de datos, tanto para la propia Diputación como para los ayuntamientos de la provincia de menos de 20.000 habitantes que así lo soliciten.

- 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 ha llevado a cabo un proceso de análisis de riesgos de manera conjunta con el ENS, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

Sin embargo, no se ha realizado ninguna auditoría específica en materia de protección de datos.

Cumplimiento legalidad del registro de facturas

Están pendientes de realizar las auditorías del registro de facturas, exigidas 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 75,0%**, que se corresponde con un **nivel de madurez N2**, que indica que existe un cumplimiento razonable de la normativa, aunque hay aspectos que se deben mejorar.

Gobernanza de ciberseguridad

Durante el trabajo de revisión de controles, hemos podido verificar la existencia de un conjunto de procedimientos, prácticas y compromisos con la ciberseguridad, por parte de los responsables implicados y la dirección de la entidad, que permiten determinar que la gobernanza de ciberseguridad alcanza un nivel aceptable.

Los aspectos fundamentales identificados que sustentan esta afirmación son:

- El compromiso con la gestión y el cumplimiento de requisitos legales relacionados con la seguridad de la información.
- Tal y como se detalla en los subapartados anteriores, existe un razonable nivel de cumplimiento de la legalidad en materia relacionada con la seguridad de la información.
- La definición y nombramiento de roles, y la creación de órganos de gobierno de la seguridad de la información. Hemos verificado que existen y ejercen de manera efectiva y continuada las funciones establecidas.
- El tratamiento adecuado por parte de la dirección de los objetivos estratégicos de seguridad identificados por el Servicio de Informática, lo que contribuye a la asunción de dichos objetivos como parte de la estrategia general de la entidad
- La asignación de recursos humanos y de inversiones con objeto de dar cumplimiento a los objetivos estratégicos en materia de seguridad, sin perjuicio de las mejoras todavía necesarias.

Los órganos superiores de la Diputación deben reforzar el actual nivel de apoyo y compromiso con la seguridad de los sistemas de información, con objeto de alcanzar los niveles de madurez de los controles requeridos por el ENS y solventar las deficiencias identificadas. Con esta finalidad resulta conveniente impulsar de forma **proactiva** iniciativas para la mejora de la ciberhigiene y la ciberresiliencia[16].

En ese sentido, los órganos de gobierno ostentan responsabilidad no solo en el cumplimiento legal, sino que deben liderar y ser ejemplarizantes en sus acciones y decisiones, como parte de un proceso de concienciación de la entidad. La existencia de un liderazgo reconocible por toda la corporación puede fomentar los avances en términos de concienciación, potenciando el vencimiento de las naturales resistencias de la organización a los cambios necesarios.

Tal como señalan las mejores prácticas, la alta dirección de la entidad, entre otros cometidos, debe ser responsable[17] de fijar los objetivos estratégicos, organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas, dirigir la actividad y a las personas, promover la mejora continua y comunicar la importancia de una gestión eficaz de la seguridad de la información[18] .

[16] Según la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva 2016/1148, de 26 de noviembre de 2021, "**adoptar un planteamiento proactivo ante las ciberamenzas es vital en la gestión de riesgos de ciberseguridad** y debería posibilitar que las autoridades competentes puedan prevenir de manera efectiva que las ciberamenazas se materialicen en incidentes reales que puedan causar pérdidas materiales o morales considerables".

[17] *Guía de seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad. Responsabilidades y funciones,* CCN, marzo de 2019.

[18] *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información*.

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 la normativa (ENS) o en las guías profesionales correspondientes, que se sintetizan en el cuadro 4 de este informe. En otro caso la entidad debe adoptar medidas para mejorar su ciberseguridad.

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.

Sistema de provisión de aplicativos y escritorios virtualizados

La entidad ha desplegado una solución de virtualización de aplicaciones y escritorios virtuales particularmente avanzada. La eficacia de la solución está basada en:

- La generación de diversos perfiles de usuario en la plataforma de virtualización, proporcionando soporte a todas las casuísticas generales identificadas y de mecanismos para proporcionar soporte a requisitos que no se encuentran en estas casuísticas generales.

- La correcta gestión de la asignación de usuarios al perfil o perfiles correspondientes, proporcionando el servicio requerido y facilitando la aplicación de los principios de mínimo privilegio y necesidad de conocer.

- La implantación del sistema de provisión virtual a la totalidad de equipos de usuario de la entidad (pendiente de finalización, con fecha prevista en diciembre de 2021).

- La configuración de los equipos de usuario como clientes ligeros, que son configurados de manera segura según las recomendaciones de organismos de referencia y fabricantes, limitando las vulnerabilidades de los equipos y minimizando los riesgos.

Este sistema de provisión de aplicativos proporciona ventajas concretas sobre distintos aspectos que tienen afección directa en la seguridad:

- Permiten una gestión integral en la provisión de aplicaciones, maximizando la eficiencia de las actuaciones, dado que estas se realizan una única vez por cada uno de los perfiles de provisión de aplicativos.

- Permiten una gestión integral de actualizaciones y corrección de vulnerabilidades, maximizando la eficiencia de su tratamiento y limitando la superficie de exposición, dado que el número de aplicaciones, versiones de estas e instalaciones se encuentra muy reducido con respecto a la provisión directa en equipos de usuario.

- Permite limitar el riesgo por conexión de equipos físicos no autorizados. Si bien no se han implantado medidas específicas para impedir dicha conexión, la provisión de aplicativos y sistemas virtualizados permite aplicar medidas compensatorias que limitan el riego de un potencial incidente por conexión de dispositivos no autorizados a la entidad.

Sistema de autenticación e inicio de sesión unificado

La entidad ha desplegado un conjunto de medidas, algunas de ellas pendientes de completar, que proporcionan de manera conjunta autenticación de doble factor e inicio de sesión único a la mayor parte de sistemas y aplicaciones que soportan los procesos críticos.

Esta solución está basada en el uso de certificados digitales almacenados en tarjetas criptográficas y está siendo integrada con la aplicación de virtualización que soporta el sistema de provisión de aplicativos y escritorios virtualizados.

La integración del sistema de autenticación con el sistema de provisión de aplicativos, junto con el inicio de sesión unificado implantado en los aplicativos virtualizados, proporcionan un nivel de seguridad adicional y permiten satisfacer los requisitos establecidos en el Esquema Nacional de Seguridad para sistemas de nivel medio.

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

SIEM: Sistema de gestión de eventos e información de seguridad

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 responsable de participación, transparencia y nuevas tecnologías y los responsables correspondientes, 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.

Transcurrido dicho plazo no se han recibido alegaciones.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes 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 19 de enero de 2022, aprobó este informe de auditoría.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe auditoria CBCS Diputació de Castelló_2021_cas - SEFYCU 3022684

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 RR3K 7W47 QY7Y 7R49

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 - 25/01/2022 8:12 VICENT CUCARELLA TORMO