SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SEGUIMIENTO DE LAS RECOMENDACIONES REALIZADAS EN EL INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE ORIHUELA DEL AÑO 2019

Situación a 31 de diciembre de 2021

RESUMEN

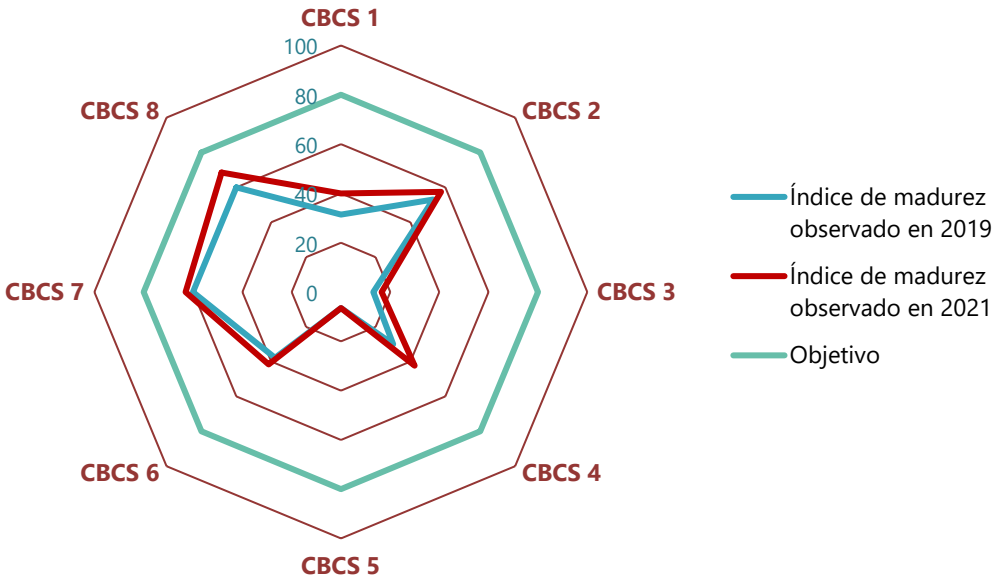
La transformación digital que están experimentando todas las Administraciones públicas y su interconexión a través de complejas redes informáticas las expone de forma cada vez más intensa a amenazas provenientes del ciberespacio. Esto origina un incremento de los riesgos asociados a los sistemas de información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

Atendiendo a esta realidad, y en sintonía con su actual plan estratégico, la Sindicatura de Comptes ha realizado un trabajo de seguimiento de los controles básicos de ciberseguridad (CBCS) del Ayuntamiento de Orihuela respecto a la situación mostrada en la auditoría del año 2019.

Conclusiones

Aunque se han realizado cambios importantes en los sistemas de información, determinadas circunstancias han dificultado mejorar los aspectos relacionados con la ciberseguridad.

El índice de madurez general de los controles básicos de ciberseguridad es muy bajo y refleja un nivel de riesgo inaceptable. El objetivo es alcanzar un 80%, pero muestra un valor del 42,0% (36,5% en 2019), es decir, el nivel de efectividad en los controles analizados sigue siendo muy deficiente.



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

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

Es preciso que el comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad, se reúna regularmente con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna. Los roles establecidos en la política de seguridad del Ayuntamiento deben definirse correctamente y ejercer sus funciones de manera efectiva.

Es necesaria la implantación de una cultura en materia de ciberseguridad que afecte a todos los niveles de la organización. Dicha cultura de ciberseguridad debe ser impulsada por la dirección en forma de planes estratégicos que definan objetivos y medidas concretas, además de incluir planes periódicos de formación y concienciación de los trabajadores.

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

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

NOTA

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

Informe de seguimiento de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Orihuela del año 2019

Situación a 31 de diciembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

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

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

En 2019 y 2020 la Sindicatura de Comptes realizó sendas auditorías sobre la situación de los controles básicos de ciberseguridad (CBCS) de los ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes y el 16 de enero de 2020 el Consell de la Sindicatura de Comptes aprobó el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Orihuela, Ejercicio 2019. Posteriormente, el Consell de la Sindicatura incluyó en los programas anuales de actuación de 2021 y 2022 realizar un trabajo de seguimiento de la situación de los controles básicos de ciberseguridad de ese ayuntamiento y de los otros 14 ayuntamientos analizados.

La necesidad de una adecuada ciberhigiene

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

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

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

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

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

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

3. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

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

La responsabilidad de la Sindicatura de Comptes es concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación sobre su diseño y eficacia operativa, sobre el cumplimiento de la normativa básica relativa a la

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

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.

La presente auditoría se ha centrado en el análisis de la situación actualizada de los ocho CBCS revisados en la auditoría del año 2019, relacionados con las aplicaciones y sistemas que soportan el proceso contable-presupuestario, la gestión tributaria y recaudatoria y otros sistemas de interés general.

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

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

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

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

4. CONCLUSIONES

El índice de madurez general de los controles básicos de ciberseguridad es muy deficiente y refleja un nivel de riesgo inaceptable.

Aunque se han realizado cambios importantes en los sistemas de información, determinadas circunstancias han dificultado mejorar los aspectos relacionados con la ciberseguridad. Los máximos responsables del Ayuntamiento deben reforzar la seguridad de la información con medidas urgentes, incluyendo recursos presupuestarios y personal con la dedicación suficiente en esta materia, tal y como establece el ENS.

Como resultado del trabajo realizado, con el alcance señalado en el apartado anterior, cabe concluir que el **índice de madurez general** en la gestión de los controles básicos de ciberseguridad alcanza un **43,2%**, que se corresponde con un nivel de madurez *N1, inicial/ad hoc*; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada.

Durante el tiempo transcurrido desde nuestra anterior auditoría, los técnicos del departamento TIC han priorizado su trabajo en aspectos como la adaptación de las redes y sistemas al cambio de edificio principal del ayuntamiento, la adaptación al teletrabajo, la migración de determinados sistemas o el cambio del gestor de expedientes (que finalmente fue revertido), que han requerido casi todo su tiempo, imposibilitando la dedicación necesaria a la seguridad de los sistemas de información.

Esta situación ha ocasionado que el Ayuntamiento únicamente ha atendido de forma parcial algunas de nuestras recomendaciones y el índice de madurez general solo ha mejorado levemente desde el 36,5% identificado en nuestra auditoría de 2019. Por lo tanto, el índice de madurez actual sigue siendo insuficiente para garantizar un adecuado grado de seguridad y alcanzar el 80% requerido por el ENS.

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

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

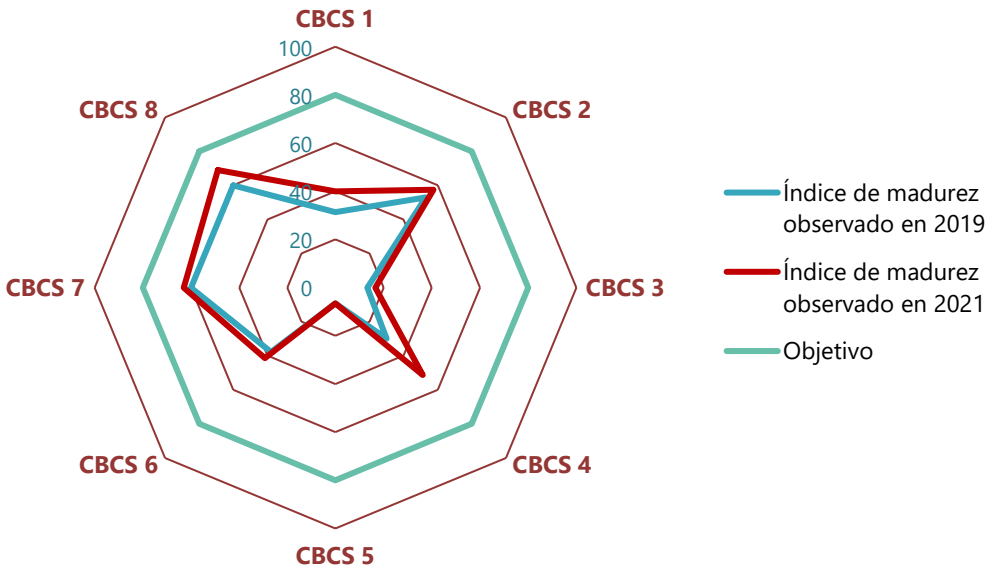
Control	2019			2021		
	Índice de madurez	Nivel de madurez	Índice de cumplimiento	Índice de madurez	Nivel de madurez	Índice de cumplimiento
CBCS 1 Inventario y control de dispositivos físicos	*31,4%*	***N1***	*39,2%*	40,0%	**N1**	50,0%
CBCS 2 Inventario y control de *software* autorizado y no autorizado	*53,0%*	***N2***	*66,3%*	57,5%	**N2**	71,9%
CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	*13,2%*	***N1***	*16,5%*	16,5%	**N1**	20,6%
CBCS 4 Uso controlado de privilegios administrativos	*30,0%*	***N1***	*37,5%*	51,3%	**N2**	64,1%
CBCS 5 Configuraciones seguras del *software* y *hardware*	*6,6%*	***N0***	*8,3%*	6,6%	**N0**	8,3%
CBCS 6 Registro de la actividad de los usuarios	*37,8%*	***N1***	*47,3%*	41,5%	**N1**	51,9%
CBCS 7 Copias de seguridad de datos y sistemas	*60,0%*	***N2***	*75,0%*	63,0%	**N2**	78,8%
CBCS 8 Cumplimiento normativo y gobernanza de ciberseguridad	*60,0%*	***N2***	*75,0%*	69,0%	**N2**	86,3%
General	36,5%	***N1***	45,6%	43,2%	**N1**	54,0%

El índice de cumplimiento de los CBCS es del 54,0%, 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%. Aunque siete de los ocho controles ha mejorado ligeramente, esta mejora es claramente insuficiente dado el bajo grado de atención a nuestras recomendaciones.

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

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

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



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

El Ayuntamiento de Orihuela no tiene establecida una adecuada gobernanza de la ciberseguridad, tal como exige la normativa y un adecuado sistema de control interno.

Esta situación debe ser prontamente subsanada, siendo los órganos superiores quienes deben impulsar el establecimiento de un adecuado sistema de gestión de la seguridad de la información.

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

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

Aunque el Ayuntamiento ha iniciado determinadas acciones en este sentido, existen carencias significativas que impiden que la gobernanza en materia de seguridad de la información pueda considerarse efectiva. Dichas carencias son:

- La falta de liderazgo e implicación en materia de ciberseguridad de los órganos superiores del Ayuntamiento. Las iniciativas al respecto son llevadas a cabo por el departamento TIC.

- El comité de seguridad, órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas del Ayuntamiento, no está constituido.

- Con objeto de salvaguardar formalmente su independencia, debe evitarse que los contratos de los servicios de DPD y del responsable de seguridad sean gestionados por el departamento de informática.

- La necesidad de disponer de personal con la dedicación suficiente en materia de seguridad, tal y como establece el ENS.

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

El grado de cumplimiento de la normativa relativa a la seguridad de la información es insuficiente

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

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

Para subsanar las deficiencias de control identificadas por la Sindicatura en la presente auditoría y mejorar los niveles de control señalados en el apartado 4 anterior, reformulamos

las recomendaciones que se efectuaron en la auditoría de 2019, considerando las mejoras realizadas desde entonces. El Ayuntamiento deberá dedicar los esfuerzos y recursos necesarios para subsanar las deficiencias pendientes.

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

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

1. Aprobar formalmente el procedimiento existente para la gestión del inventario de forma que recoja el proceso completo, incluyendo las revisiones periódicas de *hardware*.

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

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

3. Aprobar el procedimiento para la gestión integral del *software* de la entidad y definir un plan de mantenimiento que aplique a la totalidad del *software* del Ayuntamiento.

4. Revisar y actualizar los sistemas que se encuentran fuera del periodo de soporte, especialmente aquellos ligados a procesos críticos de la entidad.

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

5. Aprobar un procedimiento de identificación y remediación de vulnerabilidades que contemple las acciones actualmente implantadas. También debe ampliarse su alcance de forma que se aplique a la totalidad de sistemas del Ayuntamiento. Este procedimiento debe contemplar:

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

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

Sobre el uso controlado de privilegios administrativos (CBCS 4)

6. Aprobar el procedimiento de gestión de usuarios que establezca las directrices para los administradores de los sistemas de la entidad. Debe incluir, además de buenas prácticas establecidas en el ENS (usuarios nominativos, principio de mínimo privilegio, política de contraseñas, etc.), revisiones periódicas para todos los sistemas de la entidad.

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

7. Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN[2].

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

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

8. Aprobar formalmente un procedimiento para el tratamiento de los registros de actividad de los usuarios, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Para su revisión es aconsejable la centralización en sistemas dedicados a tal efecto.

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

9. Actualizar el procedimiento existente de copia de seguridad de forma que incluya las acciones actualmente implantadas, además de contemplar la realización de pruebas periódicas de recuperación, periodicidad de las pruebas, sistemas recuperados y personal necesario.

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

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

    – Completar la implantación de las medidas de seguridad recogidas en su declaración de aplicabilidad.

[2] Las guías STIC (seguridad de las tecnologías de la información y de las comunicaciones) están estructuradas en series. Las series a las que hace referencia la recomendación corresponden a "guías generales", "guías de entornos Windows" y "guías de otros entornos" respectivamente.

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

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

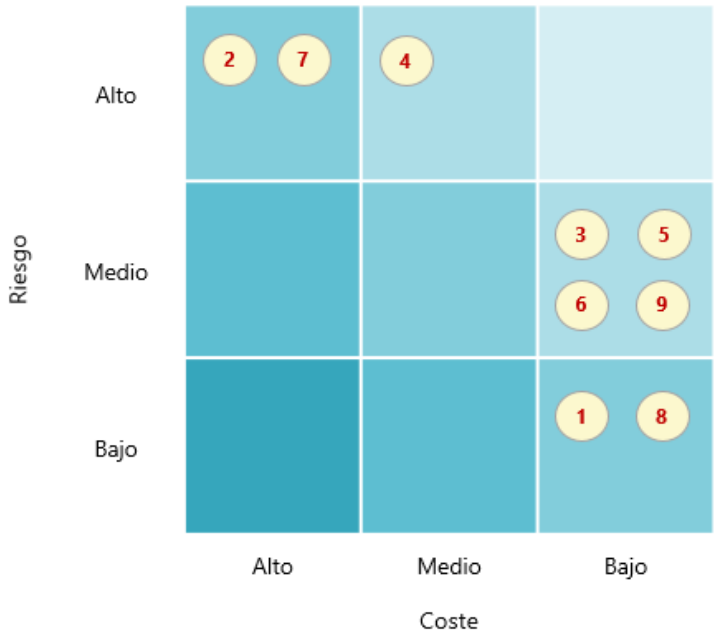
11. En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular debe planificar y ejecutar las auditorías pertinentes en materia de protección de datos.

12. Llevar a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el gráfico 2 se muestra la clasificación de las recomendaciones según los criterios combinados de **riesgo potencial a mitigar** y **coste estimado de su implantación**. Este gráfico ha sido actualizado respecto al trabajo realizado en el año 2019, adaptando la relación riesgo/coste de cada recomendación considerando las mejoras realizadas desde la anterior revisión. No se incluyen los puntos 10 a 12 anteriores, ya que son medidas de obligado cumplimiento.

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



Seguimiento de recomendaciones anteriores

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

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

Cuadro 2. Seguimiento de recomendaciones

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
1	Aprobar formalmente un procedimiento para la gestión del inventario y el control de activos físicos que recoja el proceso completo, incluyendo las revisiones periódicas de *hardware*, actualizando debidamente el inventario e incluyendo las fechas de dichas revisiones. A la hora de garantizar un nivel de actualización adecuado del inventario, es aconsejable primar el uso de herramientas para la detección y actualización automática de los elementos del sistema de información frente a procedimientos manuales.	El Ayuntamiento ha elaborado un procedimiento para la gestión del inventario y el control de activos físicos. Sin embargo, el procedimiento no ha sido formalmente aprobado. Además, se ha dotado de recursos humanos para tareas relacionadas con el mantenimiento del inventario.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
2	Implantar las soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a la red corporativa.	Las medidas adoptadas para impedir la conexión de dispositivos físicos a la red corporativa no son efectivas ni están incluidas en el procedimiento de gestión de *hardware*.	**No aplicada**	Se mantiene la redacción.
3	Elaborar y aprobar un procedimiento para la gestión integral del *software* de la entidad que contemple: - La elaboración de listas de *software* autorizado (listas blancas) como complemento del procedimiento existente, la implantación de las medidas técnicas que impidan la ejecución del no autorizado y la realización de revisiones periódicas de *software*. - La definición de un plan de mantenimiento de la totalidad del *software* utilizado, incluyendo tanto el gestionado mediante licitaciones y cláusulas contractuales como el resto de *software* utilizado en el Ayuntamiento.	El Ayuntamiento dispone de un procedimiento que describe la gestión del *software* e incluye el listado de aplicaciones autorizadas. Sin embargo, el procedimiento no ha sido aprobado formalmente. Se dispone de reglas de *firewall* para control de aplicaciones en el perímetro de la entidad.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
4	Revisar y actualizar todos los sistemas que se encuentran fuera del periodo de soporte.	El departamento TIC ha actualizado parte de los sistemas que se encontraban fuera de soporte, pero no su totalidad.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
5	Aprobar un procedimiento de identificación y remediación de vulnerabilidades que contemple las acciones actualmente implantadas, amplíe su alcance de forma que se aplique a la totalidad de sistemas del Ayuntamiento y sea aplicado por todos los miembros del departamento de sistemas. Este procedimiento debe contemplar: - La identificación de vulnerabilidades, incluyendo el escaneo mediante herramientas específicas y el análisis previo a la entrada en producción de los sistemas y el seguimiento de anuncios de los fabricantes y boletines oficiales en materia de seguridad. - La priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas. - El uso de herramientas que permitan la gestión unificada y automatizada de parches de seguridad y otras actualizaciones.	Se ha desplegado el sistema microCLAUDIA para la provisión de vacunas frente a código dañino de tipo *ransomware*. El Ayuntamiento no ha implantado una solución efectiva que permita identificar, priorizar y resolver vulnerabilidades, y gestionar las actualizaciones y parches en los sistemas. No se dispone de un procedimiento aprobado a tal efecto.	**Aplicada parcialmente**	Se mantiene la redacción dada en 2019.
6	Formalizar un procedimiento unificado de gestión de usuarios con privilegios de administración que establezca las directrices para todos los sistemas de la entidad y que incluya: - La eliminación, siempre que sea posible desde el punto de vista técnico, de todos los usuarios no nominativos con privilegios administrativos de todos los sistemas. Todas las actividades de gestión deberán realizarse con usuarios nominativos. - Cuando existan razones de índole técnica que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas. - La utilización, para cada administrador de sistemas, de diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar (gestión del dominio y servidores, administración de equipos de usuario o tareas ofimáticas no administrativas). - La política de autenticación a aplicar a este tipo de cuentas.	El Ayuntamiento ha desarrollado normativa que regula las cuentas de administración y las contraseñas; sin embargo, dicha normativa no está formalmente aprobada. Los trabajadores del departamento de informática ya disponen de usuarios con distintos niveles de privilegios en función del tipo de tarea a realizar. Se ha realizado una revisión de los usuarios en distintos sistemas, eliminando o deshabilitando los usuarios administradores no nominativos de determinados sistemas cuya existencia no se encontraba justificada.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
7	Aprobar e implantar un procedimiento de configuración segura o bastionado de los sistemas que considere la seguridad por defecto y el criterio de mínima funcionalidad. Para ello, se propone el desarrollo de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN. Paralelamente, se aconseja desarrollar un procedimiento de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos de la entidad. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la revisión periódica de los cambios realizados, bien mediante procedimiento manual o mediante herramientas automatizadas de monitorización de la configuración.	Sin variación.	**No aplicada**	Se mantiene la redacción.
8	Aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de actividad de usuario, que especifique, como mínimo, los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Para la revisión de *logs* es aconsejable la centralización de estos en sistemas dedicados a tal efecto.	El departamento ha ampliado el espacio de almacenamiento para los *logs* del servidor de correo. No existe un procedimiento aprobado para el tratamiento de *logs* de auditoría, ni un sistema centralizado para su revisión.	**No aplicada**	Se mantiene la redacción.
9	Ampliar el alcance del procedimiento existente de copia de seguridad de forma que contemple: - La realización de pruebas periódicas de recuperación, estableciendo, como mínimo, periodicidad de las pruebas, alcance y personal necesario. - El establecimiento de un nivel adicional de protección, de manera que existan copias de seguridad en soporte desconectado o no accesibles de forma directa a nivel de red.	El Ayuntamiento ha añadido a su sistema de copias un dispositivo NAS que únicamente se conecta mientras se realiza la copia. Sin embargo, dicha copia no incluye todos los sistemas críticos de la entidad. No se realizan pruebas de recuperación planificadas, si bien hemos comprobado que se realizan recuperaciones puntuales de datos.	**Aplicada parcialmente**	Se mantiene la redacción dada en 2019.

	Recomendaciones del informe anterior	Situación a 31 de diciembre de 2021 respecto al informe anterior	Estado de la recomendación	Consecuencia en el informe
10	Implantar las medidas necesarias para dar cumplimiento a los requisitos del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad. Específicamente, el Ayuntamiento debe: - Completar la implantación de las medidas de seguridad recogidas en su declaración de aplicabilidad. - Realizar las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010. - Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS del 13 de octubre de 2016.	Sin variación.	**No aplicada**	Se mantiene la redacción.
11	En relación con la protección de datos personales, el Ayuntamiento debe adaptarse a lo establecido por el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre. En particular debe planificar y ejecutar auditorías periódicas en esta materia.	El Ayuntamiento cambió de DPD y fue notificado a la AEPD. El DPD elabora actas periódicas con sus actuaciones y participa periódicamente en las cuestiones de su competencia.	**Aplicada parcialmente**	Se actualiza la redacción dada en 2019.
12	Llevar a cabo las auditorías del registro de facturas exigidas por la Ley 25/2013, de 27 de diciembre.	Sin variación.	**No aplicada**	Se mantiene la redacción.

Actuaciones en curso

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

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

- Análisis comparativo de herramientas con objeto de adquirir un *software* de gestión centralizada de actualizaciones y parches.

- El departamento TIC ha elaborado un borrador de procedimiento que define la organización de la seguridad de la información, los roles y las responsabilidades en esta materia, que está pendiente de aprobar.

- Despliegue de servicios y herramientas proporcionados por el CSIRT-CV, como parte del Plan de Choque de Ciberseguridad para las Entidades Locales de la Comunitat Valenciana, y la adquisición y despliegue de soluciones financiadas mediante los fondos europeos Next Generation EU.

    - SAT-INET (Sistema de Alerta Temprana de Internet), servicio desarrollado e implantado por el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes.

    - ARGOS, módulo de monitorización y recolección de eventos de seguridad dentro de la arquitectura de GLORIA, y TRITÓN, módulo de inteligencia para la correlación en GLORIA. GLORIA es la plataforma ofrecida por el CCN para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos. Basado en los sistemas SIEM (*security information and event management*), va un paso más allá de las capacidades de monitorización, almacenamiento e interpretación de los datos relevantes.

- Otras actuaciones previstas en materia de ciberseguridad.

  La concesión de subvenciones como las incluidas en el Plan de Recuperación, Transformación y Resiliencia o la inversión en transformación digital y modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las CCAA han motivado la elaboración de un conjunto de medidas que han sido incluidas

en un borrador de plan de actuación municipal elaborado por el departamento TIC, que está pendiente de aprobación por los órganos superiores:

- Acciones de formación y concienciación en materia de ciberseguridad.
- Implantación de herramientas como CLAUDIA, LUCIA o un sistema EDR.
- Integración en la red nacional de centros operativos de ciberseguridad.

APÉNDICE 1
Metodología aplicada

Introducción

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

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

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

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

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

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

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

Objetivo de la auditoría

De acuerdo con lo previsto en los programas anuales de actuación de 2021 y 2022, nuestro objetivo ha sido realizar el seguimiento de la situación de los controles básicos de ciberseguridad y de las recomendaciones efectuadas en el Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Orihuela. Ejercicio 2019 y obtener una seguridad limitada y concluir sobre la situación de los controles básicos de ciberseguridad revisados, proporcionando una evaluación tanto sobre su diseño[4] como sobre su eficacia operativa[5] para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información, los servicios y los sistemas de información que les dan soporte, así como sobre el cumplimiento de la normativa básica relativa a la seguridad de la información.

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

La presente auditoría se ha centrado en el análisis de la situación actualizada de los ocho CBCS revisados en la auditoría del año 2019, relacionados con las aplicaciones y sistemas que soportan el proceso contable-presupuestario, la gestión tributaria y recaudatoria y otros sistemas de interés general.

Alcance

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

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

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

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

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

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

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

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

Ámbito temporal

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

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

Metodología

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

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

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

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

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

La guía práctica de fiscalización de los OCEX 5313

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

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

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

Alineación de los CBCS con el Esquema Nacional de Seguridad

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

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

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

Cuadro 3. Los CBCS y el ENS

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

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

Los CBCS como medidas de ciberhigiene

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

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

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

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

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

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

Cuadro 4. Puntos de acción de ENISA

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

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

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

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

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

Cuadro 5. Los CBCS y sus subcontroles

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

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

Evaluación de los resultados del trabajo

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

Subcontroles

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

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

Cuadro 6. Evaluación de los subcontroles

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

Controles

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

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

Cuadro 7. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El control no está siendo aplicado en este momento.
N1 Inicial / ad hoc	10	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. *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 el apartado 66 de *Análisis n.º 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE* del Tribunal de Cuentas Europeo.

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Seguimiento de las recomendaciones

En el presente trabajo se ha realizado el seguimiento de las recomendaciones recogidas en el apartado 6 del Informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de Orihuela. Ejercicio 2019.

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

Cuadro 8. Situación de las recomendaciones

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

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

Comunicación y confidencialidad

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

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

APÉNDICE 2
Situación de los controles básicos de ciberseguridad

CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS

Objetivo del control

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

Situación del control

El Ayuntamiento ha elaborado un procedimiento para la gestión del inventario de dispositivos físicos. Sin embargo, el procedimiento no ha sido formalmente aprobado ni describe los mecanismos para restringir el acceso de dispositivos físicos no autorizados a la red municipal.

La herramienta utilizada para la gestión del inventario realiza el descubrimiento automático de activos mediante un agente de red instalado en los equipos. El departamento TIC ha sido dotado de recursos humanos para el despliegue y mantenimiento de la herramienta.

El Ayuntamiento dispone de ciertas medidas para controlar el acceso físico a la red corporativa, como la desconexión de tomas en los *switches* o la asignación dinámica de direcciones IP. No obstante, dichas medidas no son suficientes para garantizar un control efectivo sobre los dispositivos físicos.

Existe un insuficiente nivel de control sobre el inventario y el control de activos físicos, y su valoración global alcanza un **índice de madurez del 40,0%,** que se corresponde con un **nivel N1 de madurez *inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 1 del 50,0%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 31,4%; por tanto, se ha producido una mejora de 8,6 puntos en el índice de madurez del control.

CBCS 2. INVENTARIO Y CONTROL DE SOFTWARE AUTORIZADO

Objetivo del control

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

Situación del control

El Ayuntamiento dispone de un procedimiento que describe el proceso de inventariado y control de *software*, que además se completa con guías de instalación y mantenimiento

que describen las acciones concretas llevadas a cabo. Aunque los procedimientos reflejan la realidad de las acciones llevadas a cabo, no han sido formalmente aprobados.

Dicho procedimiento incluye una lista blanca de aplicaciones permitidas, si bien esta lista no ha sido formalmente aprobada por la corporación, sino por los técnicos responsables, y motivada por la operativa diaria.

Aunque se ha actualizado parte de los equipos que estaban fuera del periodo de soporte con el fabricante durante nuestra anterior auditoría, existen servicios críticos cuyos sistemas han quedado obsoletos, es decir, sin actualizaciones funcionales o parches de seguridad. Este riesgo afecta a todo el sistema de información, por lo que es recomendable priorizar la actualización de estos sistemas.

Respecto al control de aplicaciones, se han implantado dos novedades. Por una parte, nos informan que se ha implantado un *software* MDM para la gestión de dispositivos móviles, aunque no nos aportaron información detallada al respecto. Por otra parte, se han aplicado reglas de *firewall* para el bloqueo de aplicaciones en el perímetro de la red, aunque su uso es limitado.

El Ayuntamiento no dispone de un plan integral de mantenimiento de *software* que aplique a todo el *software* de la entidad de manera homogénea, ni un proceso de revisiones periódicas, aunque se realizan habitualmente y de manera no documentada.

En resumen, existe un insuficiente nivel de control sobre el inventario y control de *software* autorizado, siendo el **índice de madurez del 57,5%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 2 del 71,9%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 53,0%; por tanto, se ha producido una mejora de 4,5 puntos en el índice de madurez del control.

CBCS 3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

Objetivo del control

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

Situación del control

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

Aunque se han realizado algunas acciones relacionadas con este control, estas son limitadas y no estaban completamente operativas a fecha del trabajo de revisión, por lo que mantenemos nuestras recomendaciones.

El departamento TIC ha implantado dos herramientas relacionadas con la identificación de vulnerabilidades en la red corporativa. Por una parte, ha desplegado microCLAUDIA del CCN en los equipos, aunque durante el trabajo de revisión no aparecían todos los equipos de la organización. Por otra, han desplegado la herramienta CARMEN del CCN y el CSIRT-CV, pero el despliegue se encuentra en fase de pruebas y el Ayuntamiento no disponía todavía de credenciales de gestión.

Una de las deficiencias significativas detectadas ha sido no disponer de herramientas que permitan la gestión centralizada de parches y actualizaciones. Esta carencia impide tener un control efectivo sobre la gestión de actualizaciones, parches y vulnerabilidades de todos los dispositivos y aplicaciones conectados a la red.

El nivel de control sobre la gestión de vulnerabilidades es insuficiente, siendo el **índice de madurez del 16,5%**, que se corresponde con un **nivel de madurez *N1 inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 3 del 20,6%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 13,2%; por tanto, se ha producido apenas una mejora de 3,3 puntos en el índice de madurez del control, claramente insuficiente.

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

El Ayuntamiento ha elaborado un procedimiento de gestión de usuarios que es aplicable a todos los sistemas de la entidad y que incluye la gestión de privilegios. Sin embargo, el procedimiento no ha sido aprobado.

Los miembros del departamento TIC utilizan distintas cuentas en función de las tareas a realizar, y utilizan privilegios de administración únicamente en las tareas que lo requieren.

Hemos verificado que se ha realizado una revisión de los usuarios con privilegios de administración de determinados sistemas de la entidad, eliminando y deshabilitando aquellos cuya existencia no se encontraba justificada.

El Ayuntamiento dispone de normativa para la creación y uso de contraseñas que incluye aspectos como el ámbito de aplicación, la descripción de la directiva de contraseñas

aplicada en el dominio o algunas recomendaciones. No obstante, el documento no ha sido formalmente aprobado.

El control sobre las cuentas con privilegios administrativos es insuficiente, siendo el **índice de madurez del 51,3%**, 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 de este CBCS 4 del 64,1%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 30,0%; por tanto, se ha producido una mejora de 21,3 puntos en el índice de madurez del control.

CBCS 5. CONFIGURACIONES SEGURAS DEL SOFTWARE Y HARDWARE

Objetivo del control

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

Situación del control

El Ayuntamiento no ha realizado mejoras para el control de configuraciones seguras de los distintos dispositivos y aplicaciones.

Aunque se dispone de procedimientos que describen la puesta en marcha de equipos en la red corporativa, no han sido formalmente aprobados, ni describen las acciones llevadas a cabo para garantizar la seguridad de los sistemas previa a su entrada en producción, incluyendo la gestión de los cambios en los dispositivos críticos.

Existen carencias significativas como no disponer de herramientas centralizadas para la gestión de antivirus, lo que impide tener una visión global de la situación de la organización.

Existe, por tanto, un deficiente nivel de control en la aplicación de configuraciones seguras en dispositivos y *software*, por lo que se deberán dedicar esfuerzos y recursos para mejorarla. La valoración global del control alcanza un **índice de madurez del 6,6%**, que se corresponde con un **nivel de madurez *N0, inexistente***; es decir, el proceso no está implementado en la entidad. Esto representa un **índice de cumplimiento del CBCS 5 del 8,3%**. No se ha producido ninguna mejora respecto de nuestra anterior auditoría.

CBCS 6. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

Objetivo del control

Recoger, gestionar y analizar los registros de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.

Situación del control

El Ayuntamiento no ha realizado cambios significativos en este control, aunque se tienen previstas acciones que, una vez implantadas, tendrán un impacto positivo en el nivel general del control.

La única acción llevada a cabo respecto a los *logs* de auditoría ha sido la ampliación del espacio de almacenamiento para los registros del servidor de correo, que además son revisados periódicamente, aunque de manera informal y no documentada.

No existe un procedimiento aprobado que describa los sistemas sobre los que se registran acciones, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs*. Tampoco se ha implantado un sistema centralizado para la revisión de registros de auditoría.

La valoración global del control existente sobre el registro de la actividad de los usuarios alcanza un **índice de madurez del 41,5%**, que se corresponde con un **nivel de madurez *N1, inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada. Esto representa un **índice de cumplimiento del CBCS 6 del 51,9%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 37,8%. Por tanto, se ha producido una leve mejora de 3,7 puntos en el índice de madurez del control.

CBCS 7. COPIA DE SEGURIDAD DE DATOS Y SISTEMAS

Objetivo del control

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

Situación del control

El Ayuntamiento ya disponía de un procedimiento aprobado para la gestión de copias de seguridad de los distintos dispositivos y sistemas, que además se completaba con anexos que describían la periodicidad de las copias, los sistemas afectados, etc.

Se han adoptado medidas destinadas a mejorar el control sobre las copias; sin embargo, los procedimientos asociados no se han actualizado con las acciones implantadas.

El Ayuntamiento ha añadido, a su sistema actual de copias, un dispositivo en el que se copian periódicamente algunos de los datos de la entidad, aunque no se incluyen todos los sistemas críticos. La copia se ejecuta mediante una tarea programada y el dispositivo se desconecta manualmente una vez finalizada esta.

No se realizan pruebas de recuperación planificadas, si bien hemos comprobado que se han realizado recuperaciones puntuales de datos.

La valoración global del control existente sobre las copias de seguridad es que el Ayuntamiento alcanza un **índice de madurez del 63,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente. Esto representa un **índice de cumplimiento del CBCS 7 del 78,8%**.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,0%. Por tanto, se ha producido una mejora de 3 puntos en el índice de madurez del control.

CBCS 8. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD

Objetivo del control

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

Situación del control

Cumplimiento del ENS

Desde la revisión realizada en el año 2019, el Ayuntamiento no ha realizado acciones que hayan mejorado el nivel de cumplimiento exigido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

El Ayuntamiento dispone de una política de seguridad de la información aprobada y de nombramiento del responsable de seguridad, si bien dicha política se aprobó en 2015, por lo que sería necesaria una revisión identificando los puntos a actualizar.

Siguen vigentes las carencias identificadas y las recomendaciones realizadas en el informe precedente. Dichas carencias son:

- Completar la implantación de las medidas de seguridad recogidas en su declaración de aplicabilidad.
- Realizar las auditorías de cumplimiento previstas en el artículo 34 del Real Decreto 3/2010.
- Publicar en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS del 13 de octubre de 2016.

Cumplimiento del RGPD

En cuanto al cumplimiento en materia de protección de datos personales, desde la revisión realizada en el año 2019 el Ayuntamiento ha realizado determinadas acciones que han mejorado el nivel de cumplimiento exigido por el RGPD.

El Ayuntamiento cambió de DPD en 2020 y lo notificó correctamente a la AEPD. Hemos podido verificar que la DPD, además de la resolución de incidencias en materia de datos de carácter personal, elabora actas periódicas que describen sus actuaciones, participando activamente en reuniones en el Ayuntamiento.

Cumplimiento de la legalidad del registro de facturas

El Ayuntamiento no ha realizado la auditoría del registro de facturas exigida para cumplir los requerimientos establecidos en la Ley 25/2013, de 27 de diciembre.

Indicadores

En resumen, la valoración global sobre el cumplimiento de los aspectos de legalidad ha puesto de manifiesto que existe un insuficiente grado de cumplimiento de la normativa, siendo el **índice de madurez del 69,0%**, que se corresponde con un **nivel de madurez N2**, que indica que existen incumplimientos significativos de la normativa, y hay aspectos que se deben mejorar.

La situación del control en el informe realizado en el año 2019 mostraba un índice de madurez del 60,0%, que se corresponde con un nivel de madurez N2. Por tanto, se ha producido una mejora de 9 puntos en el índice de madurez del control.

Gobernanza de ciberseguridad

El Ayuntamiento de Orihuela no tiene establecida una adecuada gobernanza de la seguridad de la información.

Aunque el Ayuntamiento aprobó en 2017 el documento "ENS 01 Política de Seguridad de la Información" y disponen del documento "ENS 02 Organización para la Seguridad" que define las funciones de cada uno de los roles en esta materia, que no está formalmente

aprobado, existen carencias que dificultan el establecimiento de un adecuado sistema de gestión de la seguridad de la información e impiden que la gobernanza en esta materia pueda considerarse efectiva. Las deficiencias más relevantes observadas son:

- La falta de liderazgo e implicación en materia de ciberseguridad de los órganos superiores del Ayuntamiento.

  La organización no dispone de planes ni estrategias elaboradas y aprobadas por los órganos superiores en relación con la seguridad de la información, ni impulsa las medidas de seguridad necesarias, incluyendo la formación y concienciación de sus trabajadores. Son los miembros del departamento TIC, según su iniciativa y sin el respaldo de un comité de seguridad, quienes implantan las medidas necesarias relacionadas con la ciberseguridad e impulsan el cumplimiento de la normativa en esta materia. Ejemplos de ello, además de las medidas ya implantadas, son aspectos como la elaboración de un plan de acción motivado por la concesión de las subvenciones Next Generation, que incluye actividades de formación y concienciación. Dicho plan debería ser aprobado e impulsado por el nivel más alto de la organización.

- La necesidad de constituir formalmente el comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas del Ayuntamiento, formalizar los nombramientos y establecer las responsabilidades de los roles en materia de seguridad de la información.

  Es en el comité de seguridad donde deben tomarse las decisiones concretas en materia de seguridad de la información, aprobando las medidas pertinentes e impulsando las acciones a llevar a cabo. Además, el comité debe reunirse periódicamente y, en una entidad del tamaño del Ayuntamiento de Orihuela y dada la complejidad de sus sistemas, recomendamos que se haga al menos mensualmente.

- La dedicación a la seguridad de la información es insuficiente.

  El departamento TIC debe dedicar los esfuerzos necesarios para implantar las medidas de seguridad requeridas para cumplir con el ENS, medidas que deben ser impulsadas desde el nivel más alto de la organización proporcionando recursos humanos y materiales suficientes.

  Aunque existen roles designados en materia de seguridad de la información (DPD y responsable de seguridad, asumidos por personal externo contratado), su dedicación es, de acuerdo con sus contratos, claramente insuficiente para las necesidades de un ayuntamiento del tamaño de Orihuela, aunque ejerzan sus funciones de manera acorde a lo contratado. Por otra parte, estos contratos son gestionados por el departamento TIC; para preservar formalmente la independencia de estos roles, los contratos deberían ser gestionados por otro departamento.

En resumen, los órganos superiores del Ayuntamiento deben reforzar el 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.

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

ENS: Esquema Nacional de Seguridad

INES: Informe Nacional del Estado de la Seguridad

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

PSI: Política de seguridad de la información

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de gestión de seguridad de la información

SIC: Sistemas de información y comunicaciones

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, un borrador previo del Informe de auditoría se discutió con el secretario general del Ayuntamiento, con la responsable del Área de Modernización y Nuevas Tecnologías, con el responsable de Seguridad del ENS, y con los responsables de redes y de sistemas, para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

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

Transcurrido dicho plazo no se han recibido alegaciones.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y del artículo 55.1.h) de su Reglamento de Régimen Interior y de los programas anuales de actuación de 2021 y 2022 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 15 de diciembre 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 seguimiento CBCS Oriola 2019_ejercicio 2023_cas - SEFYCU 3771883

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 3MUR U3UZ QRT4 NDVH

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 - 12/01/2023 7:46 VICENT CUCARELLA TORMO