SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SÍNTESIS DE LAS AUDITORÍAS DE CIBERSEGURIDAD DE LOS QUINCE MAYORES AYUNTAMIENTOS Y DE LAS TRES DIPUTACIONES DE LA COMUNITAT VALENCIANA

Ejercicio 2021

RESUMEN

Todas las Administraciones públicas desarrollan sus actividades en entornos de administración electrónica cada vez más avanzados tecnológicamente, cuyo funcionamiento se apoya en interconexiones mediante redes complejas, lo que origina un fuerte aumento de los riesgos provenientes del ciberespacio.

Atendiendo al escenario anterior y en sintonía con sus planes estratégicos, la Sindicatura de Comptes ha realizado auditorías sobre la situación en 2021 de los controles básicos de ciberseguridad (CBCS) en los quince mayores ayuntamientos de la Comunitat Valenciana y las tres diputaciones. Una parte importante del trabajo se ha dedicado a analizar la evolución de la situación de los CBCS y el seguimiento de las recomendaciones realizadas en los informes de 2019/2020 de los quince ayuntamientos.

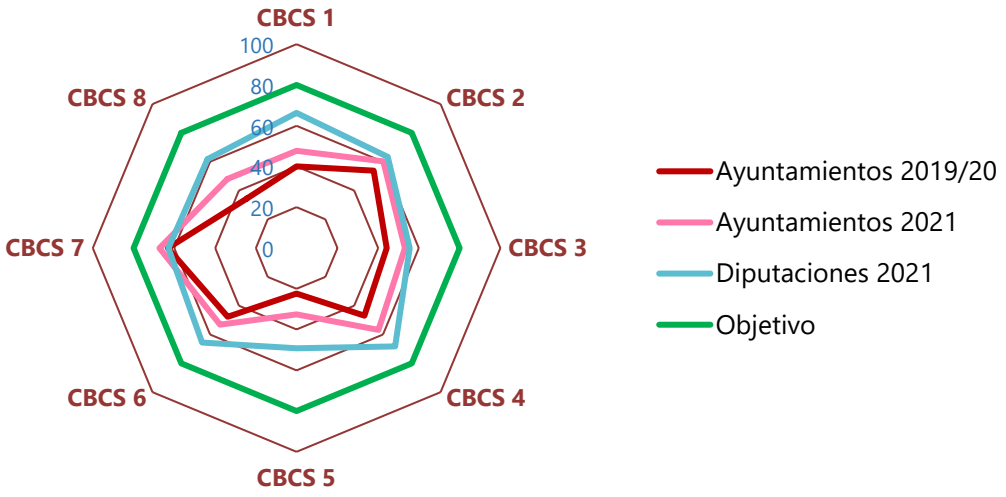
Tras la publicación de dieciocho informes individuales en nuestra página web, la Sindicatura ha realizado un informe de síntesis que ofrece una visión de conjunto, en el que se destacan las principales conclusiones y observaciones realizadas en los informes individuales.

Conclusiones

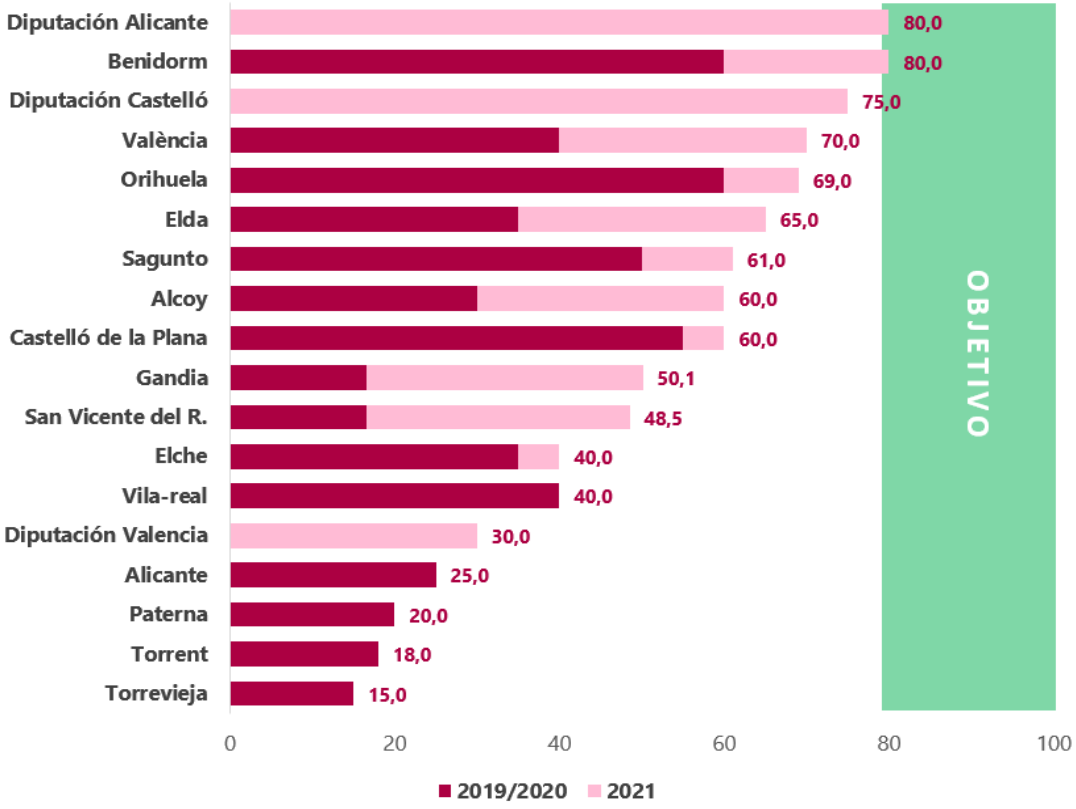
Aunque los ayuntamientos han realizado progresos desde nuestra anterior auditoría y han atendido parcialmente algunas de nuestras recomendaciones, el índice de madurez medio de los CBCS solo alcanza el 52,4% (44,1% en 2019/2020), que sigue siendo insuficiente y debe mejorar para alcanzar el 80% exigido por el ENS.

Respecto a las tres diputaciones, el índice de madurez medio de los CBCS alcanza el 61,6%, que tampoco cumple el objetivo establecido en el ENS.

En el siguiente gráfico puede observarse de forma visual el índice de madurez medio de los CBCS de las distintas entidades y su evolución desde la anterior auditoría en el caso de los ayuntamientos.



En el siguiente gráfico puede observarse de forma visual la situación del índice de madurez medio para cada una de las distintas entidades auditadas y su evolución desde la anterior auditoría en el caso de los ayuntamientos.



Aunque la mayoría de los ayuntamientos ha mejorado el cumplimiento de la normativa relacionada con la seguridad de la información, nuestra revisión ha puesto de manifiesto que el grado de cumplimiento es, en general, deficiente, existiendo incumplimientos significativos generalizados.

Hemos evaluado, además, el estado de su gobernanza de la ciberseguridad, entendida esta como el conjunto de responsabilidades y actividades llevadas a cabo por los órganos de gobierno de las entidades para proporcionar una dirección estratégica en materia de ciberseguridad, garantizando así que se logren los objetivos, que el riesgo se gestione adecuadamente y que los recursos de la entidad sean utilizados de manera responsable.

Los resultados del trabajo muestran que las entidades, en general, no tienen establecida una adecuada gobernanza de la ciberseguridad, tal como exigen tanto la normativa como un sistema de control interno bien establecido. Las organizaciones requieren el compromiso e implicación de sus órganos superiores. La alta dirección tiene la responsabilidad de establecer una adecuada gobernanza de la ciberseguridad.

Este liderazgo debe hacerse efectivo mediante la participación activa de los órganos superiores en la gestión de las TIC y en la gestión de riesgos, en la aprobación de políticas, normativas y procedimientos de seguridad de la información, estableciendo planes estratégicos, velando por el correcto funcionamiento de los órganos y roles designados en

materia de seguridad, dotando de recursos materiales y humanos e impulsando la implantación de controles sobre los sistemas de información y las comunicaciones. Únicamente de esta manera podrá establecerse con éxito un sistema eficaz de gestión continuada de seguridad de la información.

El grado de atención a nuestras recomendaciones ha sido muy bajo en algunos ayuntamientos. Siete de los quince ayuntamientos auditados no han atendido completamente a ninguna de nuestras recomendaciones. En contraposición, ocho entidades han atendido, al menos parcialmente, la mayoría de las recomendaciones efectuadas.

Hemos reformulado las recomendaciones de acuerdo con la situación observada, con el propósito de contribuir a subsanar las deficiencias observadas y mejorar los procedimientos de gestión en las organizaciones. Entre las recomendaciones realizadas con mayor frecuencia se encuentran: aprobar formalmente procedimientos que describan las acciones y controles implantados, el establecimiento de soluciones para monitorizar y detectar comportamientos anómalos en las redes corporativas, el despliegue de herramientas para gestionar vulnerabilidades, restringir el acceso de dispositivos físicos no autorizados a la red corporativa o actualizar los sistemas obsoletos.

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 la lectura del informe completo para conocer el verdadero alcance del trabajo realizado.

Informe de síntesis de las auditorías de ciberseguridad de los quince mayores ayuntamientos y de las tres diputaciones de la Comunitat Valenciana

Ejercicio 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Por qué realizamos esta auditoría

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

En la guía de auditoría GPF-OCEX 5311, "Ciberseguridad, seguridad de la información y auditoría externa", del *Manual de fiscalización* de la Sindicatura de Comptes, se destaca la importancia creciente que la ciberseguridad está 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, el **Plan Estratégico de la Sindicatura de Comptes para el periodo 2019-2022 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 auditorías sobre la situación de los controles básicos de ciberseguridad (CBCS) de los 15 ayuntamientos de la Comunitat Valenciana con una población superior a 50.000 habitantes. 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 CBCS de esos 15 ayuntamientos, de los que ya se han emitido los correspondientes informes. Además, se emitieron informes de auditoría de los CBCS del ejercicio 2021 de las tres diputaciones.

Tras publicar los dieciocho informes individuales indicados (accesibles en nuestra página web), la Sindicatura ha considerado conveniente realizar el trabajo de compilación y síntesis incluido en el presente informe. De este modo se ofrece una visión de conjunto en la que se destacan las principales conclusiones y observaciones realizadas en aquellos.

El entorno actual de administración electrónica y los riesgos tecnológicos

Las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, representan la consolidación desde el punto de vista jurídico de la administración electrónica en las entidades públicas, y establecen que la tramitación electrónica constituirá su actuación habitual, tanto en las relaciones con terceros, como entre Administraciones e intra-Administraciones, estableciendo el principio de "digital por defecto".

Como consecuencia de la aplicación de dichas leyes, todas las entidades locales están inmersas en procesos de transformación en la forma de prestación de los servicios a los ciudadanos y de la gestión pública, para un pleno despliegue de la administración electrónica sustentada en sistemas de información cada vez más complejos tecnológicamente e interconectados a través de internet.

Los riesgos para los sistemas de información que soportan los procesos de la administración electrónica aumentan a medida que las amenazas a la seguridad provenientes del ciberespacio evolucionan continuamente y aparecen ataques nuevos cada vez más sofisticados y destructivos que obligan a los entes públicos a hacerles frente de forma proactiva y sistemática, estableciendo mecanismos de defensa que en su fundamento están articulados mediante el **Esquema Nacional de Seguridad** (ENS), de aplicación obligatoria para todo el sector público.

En nuestro informe "Análisis y seguimiento del Plan de Transformación Digital de la Generalitat 2016-2019" señalábamos que "la total dependencia de los sistemas de información y de comunicaciones existente en la gestión pública hace que las Administraciones públicas sean más vulnerables frente a los ciberataques, de modo que la transformación digital debe ir inseparablemente unida a la ciberseguridad"[1].

La **total dependencia de los SIC** que actualmente existe en la gestión pública hace que nuestras Administraciones sean **muy vulnerables** frente a los ciberataques y que **mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos sea más necesario que nunca**. La generalización del trabajo en remoto provocada por la pandemia COVID-19, aunque actualmente haya disminuido parcialmente, tiene como contrapartida de su eficiencia un fuerte aumento de la superficie de exposición frente a las ciberamenazas, al que las entidades públicas deben hacer frente con la debida diligencia.

La gobernanza de la ciberseguridad como elemento articulador

A los efectos del presente informe, se entenderá por gobernanza de la ciberseguridad el conjunto de responsabilidades y actividades que tienen como objetivo 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. 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. Consideramos que una gobernanza adecuadamente establecida proporciona mecanismos que garantizan

[1] En términos muy similares se manifiesta el CCN en su publicación *Aproximación al marco de gobernanza de la ciberseguridad*, donde se afirma que el éxito de la transformación digital depende, en gran medida, de garantizar los requisitos mínimos de seguridad protegiendo la información tratada y los servicios prestados, elementos consustanciales al desarrollo de nuestra sociedad.

que la seguridad es entendida como un sistema integrado y continuado, con procesos de gestión que velan por la eficacia de las medidas y procesos de seguridad. La inexistencia de este marco de gobernanza impide asegurar su eficacia e idoneidad.

2. OBJETIVOS, ALCANCE Y METODOLOGÍA DE LAS AUDITORÍAS

Objetivos

El objetivo general de las auditorías realizadas sobre la situación de los controles básicos de ciberseguridad, en los quince mayores ayuntamientos y en las tres diputaciones de la Comunitat Valenciana, ha sido proporcionar una evaluación sobre su diseño y eficacia operativa, y sobre el cumplimiento de la normativa básica relativa a la seguridad de la información.

También hemos analizado la evolución de la situación de los controles y la atención a nuestras recomendaciones en los ayuntamientos desde nuestra anterior auditoría.

Así mismo hemos formulado recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control.

Con esta finalidad el trabajo de auditoría ha consistido en:

- El análisis del diseño y la eficacia operativa de los CBCS implantados en los ayuntamientos y diputaciones auditados.
- La identificación de deficiencias de control que puedan afectar negativamente a la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los datos, la información y los activos de los sistemas de información de esas entidades.
- La determinación del nivel de madurez existente en cada uno de los CBCS y a nivel general en las distintas entidades auditadas.
- La identificación de incumplimientos significativos de la normativa sobre seguridad de la información.
- La evaluación de la gobernanza de la ciberseguridad existente en cada entidad.

Dado el carácter limitado de la revisión, el objetivo no ha consistido en emitir una conclusión general sobre la confianza que merecen los controles de ciberseguridad existentes en el conjunto de los sistemas de información de los entes auditados. No obstante, la auditoría proporciona información relevante sobre el grado de ciberseguridad y ciberresiliencia de las entidades y sobre las posibles acciones de mejora, medidas de ciberhigiene, que deberían acometer para subsanar las deficiencias observadas y alcanzar los niveles de madurez establecidos como objetivo en el ENS.

Ámbito subjetivo

Hemos auditado los quince municipios de la Comunitat Valenciana con población superior a 50.000 habitantes. En el cuadro 1 pueden verse los ayuntamientos auditados con los datos de población y las obligaciones reconocidas netas (ORN) de 2021, en millones de euros.

Cuadro 1. Ayuntamientos auditados

Ayuntamiento	Población 2021	ORN 2021
València	789.744	956,5
Alicante/Alacant	337.304	263,8
Elche/Elx	234.205	202,9
Castelló de la Plana	172.589	178,7
Torrent	84.025	63,0
Torrevieja	82.842	108,7
Orihuela	78.940	81,1
Gandia	75.970	95,8
Paterna	71.361	63,6
Benidorm	69.118	103,5
Sagunto/Sagunt	67.043	75,3
Alcoy/Alcoi	59.128	58,5
San Vicente del Raspeig/Sant Vicent del Raspeig	58.912	41,1
Elda	52.551	42,7
Vila-real	51.130	53,8
Ayuntamientos auditados	**2.284.862**	**2.389,0**
Población de la Comunitat Valenciana	**5.058.138**	**5.288,4**
Cobertura de la auditoría	**45,2%**	**45,2%**

Fuente: Ministerio de Hacienda. Liquidaciones de los presupuestos del ejercicio 2018. Datos actualizados 31/07/2019 (<https://serviciostelematicosext.minhap.gob.es/SGCAL/CONPREL>).

Las ORN son información consolidada obtenida de la liquidación de cada entidad local.

También auditamos las tres diputaciones provinciales, cuyas obligaciones reconocidas netas (ORN) de 2021, en millones de euros, se muestran en el cuadro 2.

Cuadro 2. Diputaciones provinciales

Diputación	ORN 2021
Valencia	518,0
Alicante/Alacant	274,1
Castelló de la Plana	178,1

En total se han aprobado **dieciocho informes** de auditoría de los controles básicos de ciberseguridad que están publicados en la página web de la Sindicatura. El presente es un informe de síntesis que recoge las conclusiones de carácter general que han podido extraerse tras realizar esas auditorías.

Ámbito objetivo

La auditoría se ha centrado en el análisis de la situación de los ocho CBCS definidos en la GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad":

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

En el apéndice 3 se proporciona un mayor detalle sobre estos controles, sus objetivos de control y los subcontroles que los forman.

Ha sido necesario delimitar y concretar qué sistemas se iban a analizar, debido a la naturaleza del objeto material a revisar, que comprende los sistemas de información y comunicaciones de un ente local de tamaño grande, con su gran amplitud, complejidad y diversidad. En este sentido, de cada entidad hemos analizado las aplicaciones informáticas que soportan dos de los procesos de gestión más relevantes a efectos de la Sindicatura, como son la gestión contable y presupuestaria y la gestión tributaria y recaudatoria.

Además, por su importancia para el buen funcionamiento de los sistemas de información y la ciberseguridad, en cada ente hemos analizado también una selección de los siguientes tipos de elementos:

- controlador de dominio
- *software* de virtualización
- equipos de usuario
- elementos de la red de comunicaciones (*router, switches*, puntos de acceso *wifi*, etc.)
- elementos de seguridad (*firewall,* IPS, *proxy* de correo, *proxy* de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.)

Ámbito temporal

En cuanto al ámbito temporal del trabajo, las conclusiones sobre los ayuntamientos 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. En el caso de las diputaciones los indicadores se han calculado con referencia al 30 de septiembre de 2021.

Metodología

Hemos llevado a cabo las auditorías de conformidad con los *Principios fundamentales de fiscalización de las instituciones públicas de control externo* y con las normas técnicas de auditoría 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 y normas técnicas antedichas siempre detecte un incumplimiento significativo cuando exista.

Las auditorías de los controles básicos de ciberseguridad (CBCS) han sido realizadas 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", y en el resto de las secciones aplicables del *Manual de fiscalización* de la Sindicatura de Comptes.

Hemos evaluado la situación de los CBCS en las distintas entidades utilizando el modelo de nivel de madurez de los procesos, ya que es el sistema previsto en el ENS y permite establecer objetivos y realizar comparaciones de forma homogénea entre distintas entidades y también ver la evolución a lo largo del tiempo en una entidad.

Los sistemas de información revisados están clasificados como de categoría de seguridad MEDIA. Así, acorde con esta categoría, el nivel de madurez requerido por el ENS y que también hemos aplicado para los CBCS en las auditorías realizadas es *N3, proceso definido* y un índice de madurez del 80%. Este nivel exige que los procesos estén estandarizados, documentados y comunicados con acciones formativas. Esto implica que se debe disponer de un catálogo de procesos que se mantiene actualizado; que estos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general; que hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes, y que se ejerce un mantenimiento regular; que las oportunidades de sobrevivir a un ciberataque son altas, aunque siempre queda el factor de lo desconocido (o no planificado).

Como se ha señalado antes, los resultados obtenidos al aplicar esta metodología permiten formar una idea general de la situación de los controles de ciberseguridad en los entes auditados, de su ciberresiliencia y del grado de cumplimiento de una serie de disposiciones legales muy importantes en materia de seguridad de los sistemas de información.

Los hallazgos de la auditoría, las conclusiones y los borradores de informe individuales fueron discutidos con los responsables de las distintas entidades, de acuerdo con lo establecido en nuestro *Manual de fiscalización*. Los informes individuales fueron sometidos al procedimiento contradictorio mediante el correspondiente trámite de alegaciones tal como se recoge en aquellos. En el presente informe se muestran los resultados comparativos de todas las entidades de forma sintética.

En el apéndice 1 se proporciona un mayor detalle de la metodología utilizada.

Confidencialidad

Dado que la información utilizada en la auditoría y los resultados detallados de esta tienen un carácter sensible y pueden afectar a la seguridad de los sistemas de información de las entidades revisadas, las comunicaciones de información sensible entre la Sindicatura y las entidades se han realizado por medio de canales cifrados, garantizando así la integridad y confidencialidad de los datos. Adicionalmente, la Sindicatura dispone de las políticas, procedimientos y mecanismos necesarios para garantizar que dicha información únicamente es accesible por el personal encargado de la ejecución del presente trabajo.

3. CONCLUSIONES GENERALES

PRIMERA CONCLUSIÓN

Aunque, en general, los ayuntamientos han realizado progresos desde nuestra anterior auditoría y han atendido parcialmente algunas de nuestras recomendaciones, el índice de madurez medio de los controles básicos de ciberseguridad (52,4%) sigue siendo insuficiente y debe mejorar para alcanzar los niveles exigidos por el ENS. Solo un ayuntamiento (Benidorm) alcanza el 80% requerido por el ENS.

La situación de las diputaciones es ligeramente mejor, alcanzando un índice de madurez medio del 61,6%, pero también está por debajo del objetivo establecido en el ENS.

En el cuadro 3 se muestra la situación detallada en las distintas entidades auditadas.

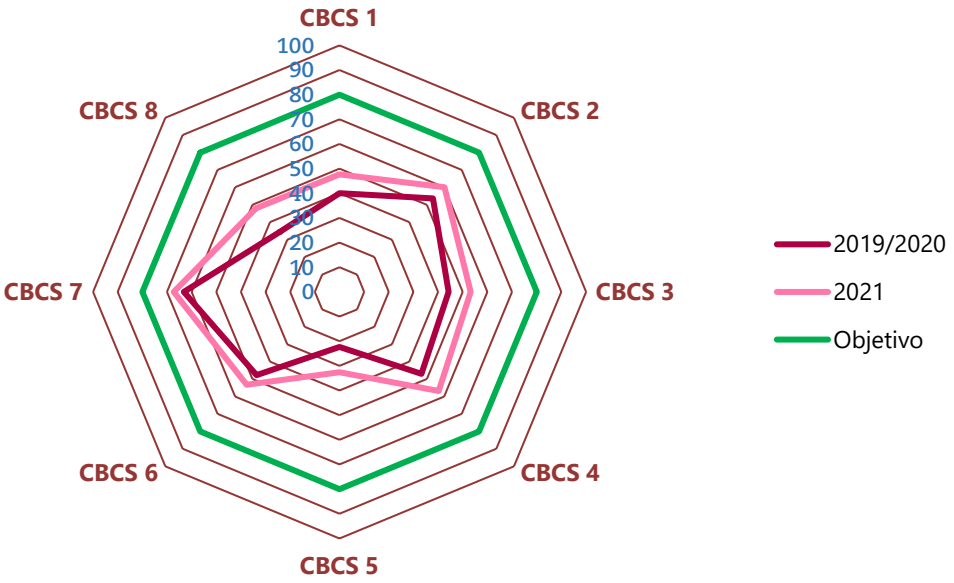
Cuadro 3. Índice de madurez medio de los controles básicos de ciberseguridad de los 15 ayuntamientos y de las tres diputaciones

		AYUNTAMIENTOS						DIPUTACIONES		
		2019/2020			31/12/2021			30/09/2021		
	Control	*Índice de madurez*	*Nivel de madurez*	*Índice de cumplimiento*	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	*40,1%*	***N1***	*50,1%*	47,7%	**N1**	59,6%	66,3%	N2	82,9%
CBCS 2	Inventario y control de *software* autorizado y no autorizado	*53,6%*	*N2*	*67,0%*	60,1%	N2	75,2%	63,3%	N2	79,2%
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	*44,2%*	***N1***	*55,3%*	53,2%	N2	66,5%	55,5%	N2	69,3%
CBCS 4	Uso controlado de privilegios administrativos	*47,0%*	***N1***	*58,7%*	56,8%	N2	71,0%	68,3%	N2	85,4%
CBCS 5	Configuraciones seguras del *software* y *hardware*	*22,3%*	***N1***	*27,9%*	32,6%	**N1**	40,7%	49,2%	**N1**	61,5%
CBCS 6	Registro de la actividad de los usuarios	*47,7%*	***N1***	*59,6%*	53,2%	N2	66,5%	65,6%	N2	82,0%
CBCS 7	Copias de seguridad de datos y sistemas	*63,2%*	*N2*	*79,0%*	67,3%	N2	84,1%	62,9%	N2	78,6%
CBCS 8	Cumplimiento normativo y gobernanza de ciberseguridad	*34,4%*	***N1***	*43,0%*	48,0%	**N1**	60,0%	61,7%	N2	77,1%
	General	***44,1%***	***N1***	***55,1%***	52,4%	*N2*	65,4%	61,6%	*N2*	77,0%

La comparación de los resultados detallados obtenidos en la auditoría de 2021 con los obtenidos en las auditorías de 2019/2020 muestra una mejora en todos los controles. No obstante, el nivel de efectividad medio en los controles analizados sigue siendo insuficiente, ya que ninguno alcanza el objetivo y existen claras posibilidades de mejora para alcanzar los niveles exigidos por el ENS, particularmente sobre los controles que presentan deficiencias significativas y no alcanzan el nivel de madurez N2 (CBCS 1, 5 y 8).

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

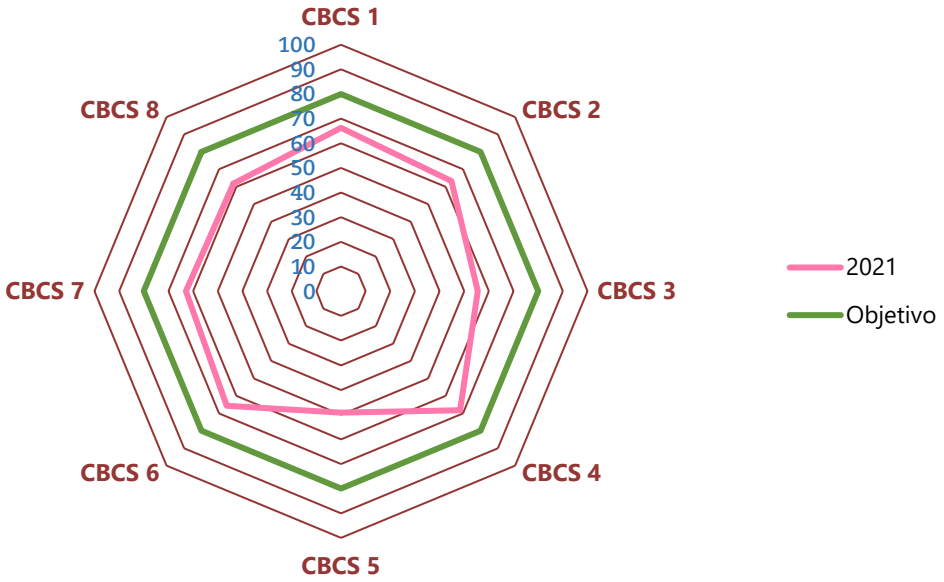
Gráfico 1. Índice de madurez medio de los CBCS de los quince ayuntamientos



En general, los ayuntamientos han realizado acciones encaminadas a mejorar sus sistemas, pero dichas acciones no son suficientes para alcanzar los requisitos del ENS.

Por otro lado, el gráfico 2 refleja el mismo indicador (índice de madurez medio de cada control) en las tres diputaciones provinciales.

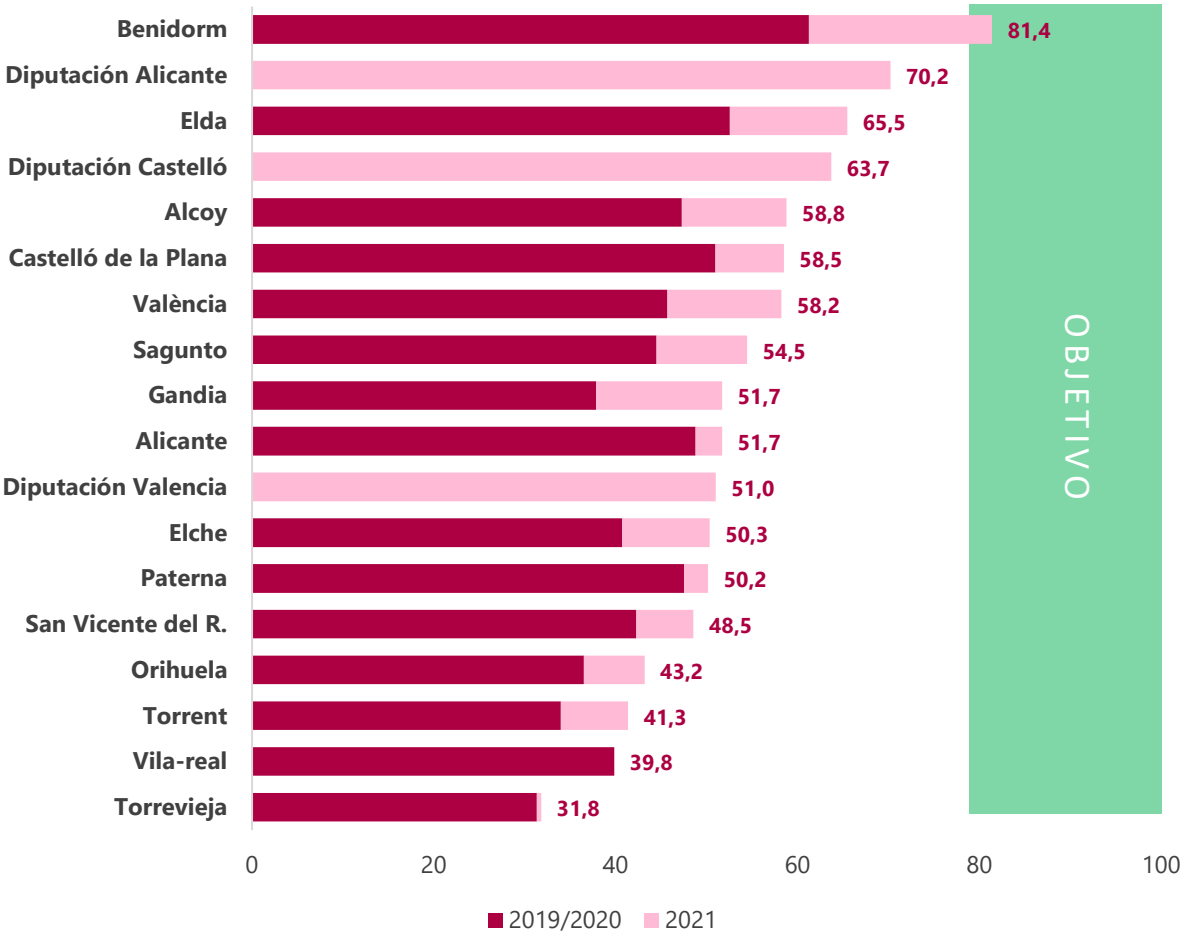
Gráfico 2. Índice de madurez medio de los CBCS de las diputaciones



Aunque los resultados se aproximan al objetivo en algunos de los controles revisados, ninguno alcanza, en promedio, el valor objetivo.

El gráfico 3 muestra la evolución del índice de madurez medio de cada una de las dieciocho entidades auditadas.

Gráfico 3. Situación del índice de madurez medio de los CBCS



Tal y como se observa en el gráfico anterior, **únicamente el índice de madurez medio del Ayuntamiento de Benidorm alcanza el objetivo establecido por el ENS.**

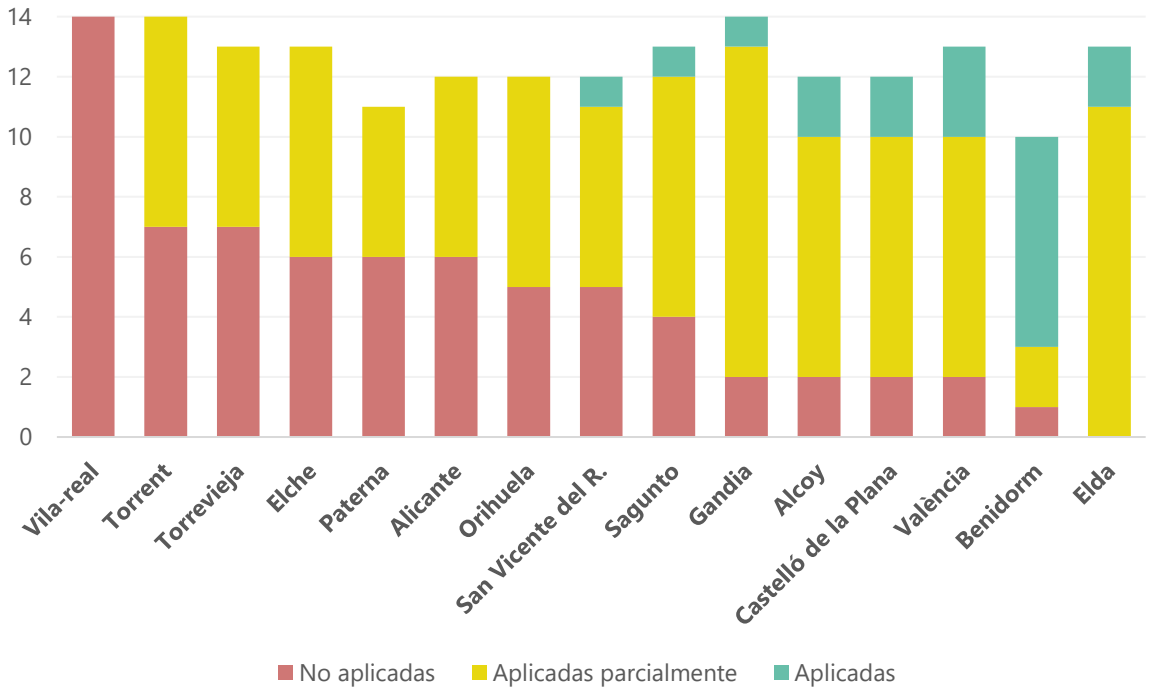
En el apéndice 3 se detallan las deficiencias observadas y se añade más información sobre cómo mejorar el funcionamiento de los controles.

SEGUNDA CONCLUSIÓN

El grado de atención a nuestras recomendaciones por parte de los ayuntamientos ha sido desigual. Es preciso que estos dediquen los esfuerzos y recursos necesarios para subsanar las deficiencias identificadas y alcanzar un razonable nivel de ciberseguridad.

En los 15 informes emitidos en 2019/2020 se efectuaron 188 recomendaciones, de las cuales únicamente 19 han sido atendidas por completo, 100 han sido atendidas parcialmente y 69 no han sido atendidas. El siguiente gráfico muestra el nivel de atención a nuestras recomendaciones por parte de cada una de las entidades auditadas.

Gráfico 4. Recomendaciones atendidas por entidad



Del gráfico anterior es destacable que siete entidades no han atendido completamente ninguna de las recomendaciones que realizamos en 2019/2020, existiendo una de ellas (Vila-real) que no ha atendido a ninguna de las recomendaciones realizadas ni siquiera parcialmente.

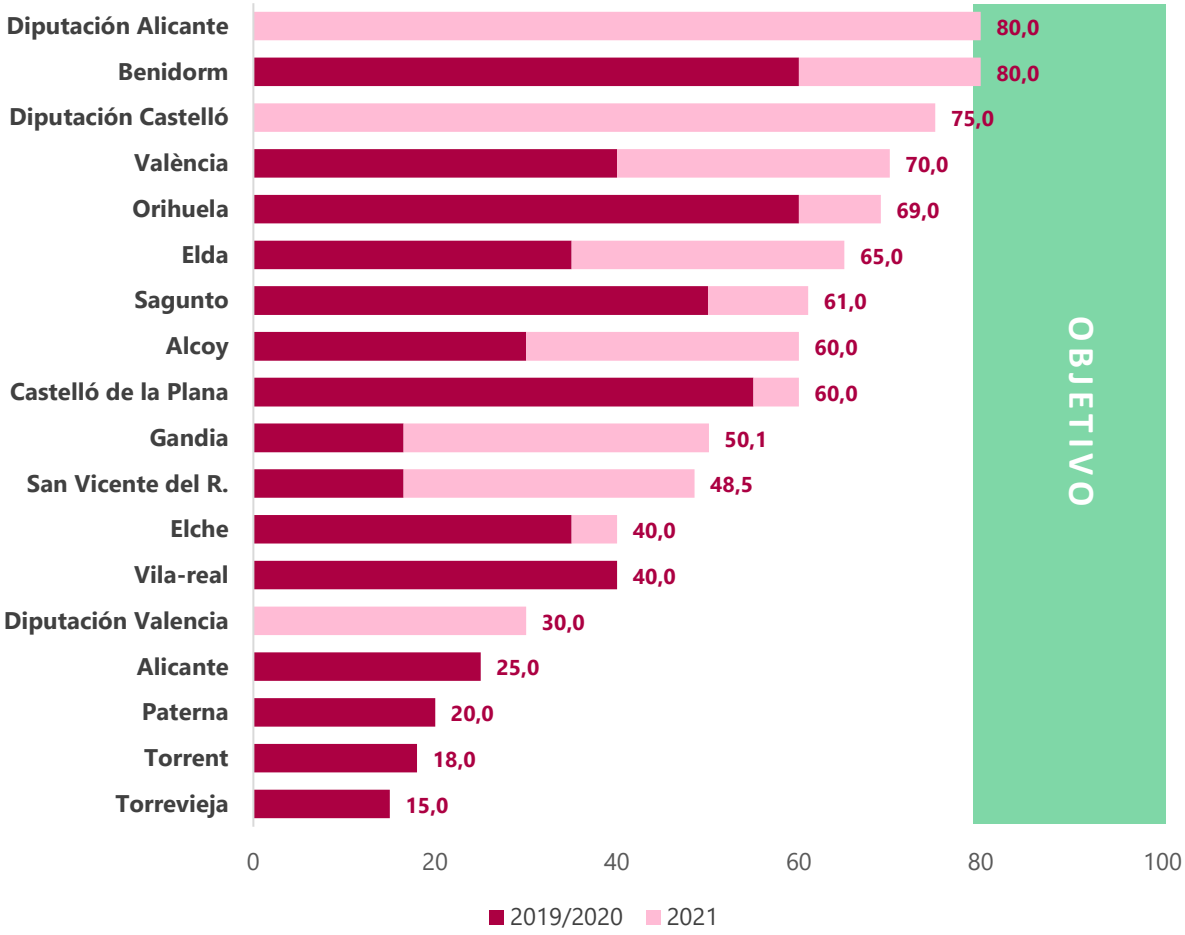
En contraposición a lo anterior, existen ocho entidades que han atendido completamente al menos una recomendación y de manera parcial la mayoría de las recomendaciones realizadas en 2019/2020.

TERCERA CONCLUSIÓN

El grado de cumplimiento de la normativa relativa a la seguridad de la información es, en general, deficiente, existiendo incumplimientos de la normativa significativos generalizados.

El siguiente gráfico muestra el índice de cumplimiento normativo obtenido por las entidades durante nuestro trabajo de revisión.

Gráfico 5. Índice de madurez del cumplimiento de la normativa (CBCS 8)



Como puede observarse en el gráfico, la mayoría de los ayuntamientos ha mejorado su grado de cumplimiento de la normativa desde nuestra anterior auditoría.

CUARTA CONCLUSIÓN

Las entidades auditadas, en general, no tienen establecida una adecuada gobernanza de la ciberseguridad, tal como exigen tanto la normativa como un sistema de control interno bien establecido.

Los órganos superiores de las entidades (alcalde o alcaldesa en el caso de los ayuntamientos; presidente o presidenta en el caso de las diputaciones) 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. Se debe actuar de manera urgente para solventar las carencias identificadas en esta materia en cada una de las entidades, ya que afectan de manera negativa al estado de su ciberseguridad.

Una adecuada gobernanza de ciberseguridad debe reflejarse, principalmente, en:

- Debe existir un claro **compromiso de los órganos de gobierno de la entidad con la ciberseguridad**. En ese sentido, los órganos de gobierno ostentan responsabilidad no solo en la formalización y adecuación legal, sino que deben ser ejemplarizantes en sus acciones y decisiones, como parte de un proceso de concienciación de la entidad.

- La aprobación por el presidente del ente local de las **políticas de seguridad de la información**.

- Debe existir una **planificación estratégica en materia de ciberseguridad**, que proporcione un marco de actuación a medio plazo que asegure la atención a las necesidades prioritarias con respecto a la seguridad, y se encuentre alineada con la estrategia corporativa. La planificación estratégica de la seguridad evita una gestión reactiva basada principalmente en necesidades sobrevenidas.

- La constitución, y funcionamiento efectivo, de un **comité de seguridad de la información**, órgano especializado y permanente para la ciberseguridad integrado por aquellas personas de la organización con responsabilidad en la toma de decisión en materia de seguridad y privacidad de la información, así como por aquellas designadas en representación de otros órganos o comités.

- El nombramiento de **roles de gestión de seguridad**, con objeto de concretar y personalizar las responsabilidades en materia de seguridad de la información.

- La elaboración de unos **presupuestos y la dotación de equipos humanos adecuados** a las exigencias de una eficaz ciberdefensa en los actuales entornos de administración electrónica avanzados e interconectados.

- Las normas y los procedimientos de seguridad **deben estar formalmente aprobados** por el órgano que se establezca en el documento de políticas de seguridad de la información y **deben ser de aplicación obligatoria en todos los sistemas de**

información del ayuntamiento o diputación, que deben estar gobernados por las mismas políticas y normas de seguridad.

Esta **normativa interna debe diseñarse para ser aplicada, no para cumplir una formalidad**. El contenido del conjunto de políticas, normas y procedimientos aprobados debe ser una representación fidedigna y precisa del sistema de seguridad implantado por el ente local. La aprobación de un marco normativo que no represente la realidad del ente deviene en un uso estéril de recursos por su carencia de efectividad y en una falsa percepción de cumplimiento que puede conllevar el abandono de otras medidas más adecuadas.

El apéndice 2 detalla las deficiencias observadas y se añade más información sobre cómo debe establecerse una adecuada gobernanza en las entidades para garantizar el funcionamiento eficaz de un sistema integral de gestión continuada de la seguridad de la información.

4. RECOMENDACIONES

Se incluye en este apartado un resumen de las recomendaciones realizadas en los 18 informes individuales de los controles básicos de ciberseguridad de ayuntamientos y diputaciones.

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

a) El inventario de dispositivos físicos se debe mantener sistemáticamente actualizado, utilizando un procedimiento de autorización para el alta de nuevo *hardware* y otro para actualizar las bajas.

   Si bien muchas de las entidades auditadas cuentan con un inventario de *hardware* actualizado, la principal recomendación ha sido que se debe aprobar un procedimiento que describa las acciones llevadas a cabo para inventariar los elementos y actualizar dicho inventario.

   Por otra parte, la principal carencia en este apartado ha sido la falta de controles de conexión de dispositivos físicos no autorizados a la red corporativa. Dicha carencia ha sido identificada como de riesgo y coste altos, lo que implica que las entidades han de realizar inversiones para implantar de manera efectiva dicho control.

Sobre el inventario y control de *software* autorizado y no autorizado (CBCS 2)

b) De manera similar al apartado anterior, se ha evidenciado la existencia de inventarios *software* actualizados en muchas de las entidades auditadas. La principal recomendación relacionada con este control ha sido que debe aprobarse formalmente un plan de mantenimiento para el *software* licenciado.

   Otra de las recomendaciones generalizadas ha sido que se debe identificar y actualizar todo el *software* que está fuera del período de soporte, que se ha considerado como deficiencia grave en casi todas las entidades auditadas.

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

c) Una de las principales recomendaciones relativas a este CBCS ha sido que las entidades deben dotarse de herramientas que faciliten la detección y aplicación de actualizaciones y parches de seguridad. Se ha recomendado a tal efecto el uso de herramientas centralizadas de gestión de parches.

   La no utilización de dichas herramientas implica un riesgo alto para la organización por carecer del control necesario sobre los dispositivos y sistemas. Su establecimiento puede suponer un coste moderado, pero el riesgo disminuye considerablemente.

   Adicionalmente, para alcanzar un control efectivo sobre las vulnerabilidades, se recomienda el uso de herramientas de escaneo y la realización de pruebas de *hacking* ético o de penetración.

Sobre el uso controlado de privilegios administrativos (CBCS 4)

d) En este apartado las entidades tienen un amplio margen de mejora mediante la implantación de ciertas medidas que suponen un coste bajo para la organización, pero que implican la disminución significativa del riesgo.

   Entre las recomendaciones realizadas destacamos la necesidad de eliminar el uso de usuarios genéricos, la utilización de permisos basados en la regla de mínimos privilegios, cambio de usuarios y contraseñas por defecto y la implantación de una política robusta de contraseñas que aplique a todos los sistemas de la entidad.

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

e) La recomendación más frecuente ha sido que se debe establecer y aprobar un procedimiento para el uso de guías de bastionado basadas en las recomendaciones de los fabricantes y del Centro Criptológico Nacional.

   Si bien la práctica totalidad de entidades revisadas dispone de guías informales de configuración de ciertos sistemas, su elaboración no considera como objeto la consecución de un determinado nivel de seguridad y la inclusión de medidas de seguridad en ellas no se encuentra formalizada. Además, en caso de incluir configuraciones específicas de seguridad, estas por lo general se basan únicamente en

la experiencia y conocimientos de los administradores e implantadores de los sistemas y no en las recomendaciones de fabricantes y organismos de referencia.

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

f) Las principales recomendaciones han sido la formalización y aprobación de un procedimiento de gestión de registros de actividad y su centralización en sistemas específicos para su tratamiento.

   La configuración por defecto de los sistemas incluye por lo general la habilitación de los registros de actividad de usuarios y administradores. No obstante, la falta de organización de su gestión y la dispersión en múltiples sistemas dificultan la explotación de la información y su aprovechamiento para la identificación de eventos y vulneraciones de seguridad.

Sobre las copias de seguridad de datos y sistemas (CBCS 7)

g) Hemos recomendado casi en la totalidad de auditorías la realización de pruebas planificadas de recuperación de las copias de seguridad de datos y sistemas, ya que su carencia impide garantizar la completa eficacia del proceso de gestión de copias de seguridad. Por lo general solo se realizan recuperaciones de datos de usuarios a demanda.

Sobre el cumplimiento normativo (CBCS 8)

h) Deben adoptarse las medidas necesarias para dar cumplimiento a los distintos requerimientos legales en materia de seguridad de la información.

APÉNDICE 1
Metodología aplicada

1. 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 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 no son ajenas a esta problemática de la ciberseguridad, por lo que deben implementar controles sobre la seguridad de la información y las comunicaciones de acuerdo con las directrices establecidas en el ENS, que es **de obligado cumplimiento**.

Por dichas razones, es imperativo que los responsables de las entidades gestionen este tipo de riesgos y establezcan los controles de ciberseguridad necesarios para mantener los sistemas de información protegidos frente a las amenazas de seguridad y evitar la interrupción en los servicios prestados a los ciudadanos.

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[2] 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 exigidas por el ENS– **constituye una medida básica de ciberhigiene** para las Administraciones públicas.

2. LA GUÍA PRÁCTICA DE FISCALIZACIÓN DE LOS OCEX 5313

La guía 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,

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

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), 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.

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

3. ALINEACIÓN DE LOS CBCS CON EL ESQUEMA NACIONAL DE SEGURIDAD

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

Cuadro 4. 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 y op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	mp.sw.2 y op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	op.acc.4 y op.acc.5
CBCS 5	Configuraciones seguras del *software* y *hardware*	op.exp.2 y op.exp.3
CBCS 6	Registro de la actividad de los usuarios	op.exp.8 y 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 de 2010 (vigente en el momento de las auditorías).

4. LOS CBCS COMO MEDIDAS DE CIBERHIGIENE

La European Union Agency for Cybersecurity (ENISA) señala[3] 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. 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[4].

En esa dirección, ENISA establece diez puntos de acción para una adecuada ciberhigiene. Como se observa en el cuadro 5, 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 5. 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.

5. CRITERIOS DE AUDITORÍA: LOS CBCS 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.

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

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

Cuadro 6. 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 o 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*	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.

6. 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 6 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 7. Evaluación de los subcontroles

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

Controles

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

Cuadro 8. 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 tiempos de respuesta y presupuestos. 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 fundamentalmente en la comprobación de su aplicación práctica.

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

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

7. NIVEL DE MADUREZ MÍNIMO REQUERIDO EN FUNCIÓN DE LA CATEGORÍA DE LOS SISTEMAS DE INFORMACIÓN AUDITADOS

A los sistemas de información y comunicaciones 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 ciberincidente 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[5]:

Cuadro 9. Categorías de seguridad

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%.

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

8. 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.

9. SEGUIMIENTO DE LAS RECOMENDACIONES

En las auditorías de los ayuntamientos se ha realizado el seguimiento de las recomendaciones efectuadas en los informes de auditoría de 2019/2020.

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

Cuadro 10. 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.

10. NUEVO ESQUEMA NACIONAL DE SEGURIDAD (RD 311/2022)

Durante los últimos años, el crecimiento de las TIC ha supuesto la aparición de numerosas y novedosas tecnologías relacionadas con el ciberespacio (inteligencias artificiales, *blockchain*, descentralización de servicios, *edge computing*, etc.), apareciendo con ello nuevos riesgos y amenazas, e incrementándose el número de ciberataques, cada vez más sofisticados.

En este complejo escenario, para abordar los riesgos y garantizar un uso seguro de las redes, comunicaciones y sistemas de información, deben adoptarse estrategias y medidas para prevenir, detectar y responder a ciberataques de manera proactiva, fomentando así el uso de un ciberespacio seguro y fiable. Al mismo tiempo deben adaptarse a las regulaciones europeas y nacionales en materia de seguridad.

El Real Decreto 3/2010, de 8 de enero, por el que se regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fijaba una serie de principios básicos, requisitos mínimos y medidas de seguridad para garantizar la seguridad de la información y los servicios prestados por los organismos públicos. Todas nuestras auditorías de los CBCS de las entidades locales, hasta 2022 inclusive, se han realizado tomando como base este ENS.

Las tecnologías emergentes y los nuevos riesgos que estas conllevan, junto a la experiencia y conocimiento adquiridos por el Centro Criptológico Nacional durante los últimos años, precisaban que el ENS fuera actualizado. Así, el nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, sustituye el anterior e incluye algunas novedades:

- Incorporación de la figura del perfil de cumplimiento, para ajustar los requisitos del ENS a necesidades específicas, como determinados colectivos (entidades locales, universidades, etc.) o determinados ámbitos tecnológicos (servicios *cloud*, por ejemplo).
- Establecimiento de un protocolo de actuación ante ciberincidentes.
- Nuevo sistema de codificación de los requisitos de las medidas de seguridad, añadiendo refuerzos a los requisitos básicos de seguridad.
- Se actualizan las medidas de seguridad con respecto al Real Decreto 3/2010.

APÉNDICE 2
La gobernanza de la ciberseguridad

1. QUÉ ES LA GOBERNANZA DE LA CIBERSEGURIDAD

A los efectos del presente informe, se entenderá por gobernanza de la seguridad de la información y las comunicaciones o de ciberseguridad (términos que utilizamos de forma indistinta) el conjunto de responsabilidades y actividades que tienen como objetivo 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.[6]

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[7]. Este liderazgo debe ser ejercido por la alta dirección/órganos superiores de la entidad. Su compromiso con la seguridad es el factor clave que habilita el establecimiento de un marco de gobernanza efectivo en las organizaciones.

2. POR QUÉ ES IMPORTANTE LA GOBERNANZA DE LA CIBERSEGURIDAD

La importancia de la gobernanza en la gestión de la ciberseguridad ha sido objeto de diversos documentos y guías del Centro Criptológico Nacional (CCN), entre los que destacan la "*Aproximación al Marco de Gobernanza de la Ciberseguridad. Año 2022*", la "*Guía de Seguridad de las TIC CCN-STIC 201. Organización y Gestión para la Seguridad de las TIC*" *y* la "*Guía de Seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad, Responsabilidades y Funciones*".

La existencia de un conjunto eficaz de procesos de gestión de la ciberseguridad y de responsabilidades definidas proporciona a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

Algunas de las ventajas que la existencia de un marco efectivo de gobernanza proporciona a las entidades serían:

- Posibilita la alineación de las actividades relativas a la seguridad de la información con los objetivos estratégicos de la entidad.

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

[7] 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.

- Facilita la coordinación entre distintas áreas de la organización y los implicados en materia de seguridad de la información.

- Posibilita que el conjunto de actividades realizadas y medidas de seguridad aplicadas constituyan un Sistema de Gestión de la Seguridad de la Información que trasciende las iniciativas individuales.

- Establece las responsabilidades del personal implicado, necesarias para garantizar que se cumplen los objetivos y se alcanza el nivel de seguridad requerido.

- Establece procesos que impiden que la eficacia de las actividades de seguridad dependa de roles concretos de la organización o solo de iniciativas personales, sino de un sistema bien establecido.

- Ayuda a fomentar una cultura en materia de ciberseguridad en las organizaciones.

Por el contrario, aquellas entidades que no disponen de un marco de gobernanza adecuadamente definido e implantado tienen una alta probabilidad de experimentar las siguientes carencias:

- El principal riesgo consiste en que la entidad sea vulnerable frente a ciberataques por carecer de un sistema de controles coherente y aceptado por toda la organización.

- Probable uso ineficiente de los recursos, dado que, independientemente de la idoneidad de dichos recursos con respecto a las necesidades identificadas, no existen mecanismos que aseguren que estos son utilizados de manera adecuada para responder a necesidades alineadas con los objetivos estratégicos.

- No asegura la existencia de mecanismos de coordinación interna entre las distintas áreas de la organización y los responsables de la seguridad, lo que impide garantizar que las necesidades sean adecuadamente identificadas en tiempo y forma. Además, posibilita que existan áreas que, de manera inadecuada, realicen una gestión no coordinada de la seguridad al margen de las políticas y normas de seguridad de la organización.

- No se asegura que el conjunto de medidas y procesos de seguridad implantados constituyan un Sistema de Gestión de la Seguridad de la Información, integrado y coherente, lo que implica un riesgo de que no existan mecanismos de control que velen por la eficacia de dichas medidas y procesos.

- En caso de no haberse definido responsabilidades al nivel directivo adecuado, existe un riesgo de que las necesidades, con respecto a la seguridad de la información identificadas por sus responsables, no sean debidamente atendidas por la organización.

- No se asegura que existan mecanismos que independicen las medidas y procesos de seguridad de las personas encargadas de gestionarlas, de modo que existe un riesgo de que, ante determinadas ausencias, las medidas de seguridad no sean aplicadas.

Por lo tanto, podemos concluir que una gobernanza adecuadamente establecida proporciona a las entidades mecanismos que garantizan que la seguridad es entendida como un sistema integrado y continuado, con procesos de gestión que velan por la eficacia de las medidas y procesos de seguridad. La inexistencia de este marco de gobernanza, independientemente de los esfuerzos y recursos dedicados a la seguridad, impide asegurar su eficacia e idoneidad.

3. RESPONSABLES DEL ESTABLECIMIENTO DE UNA ADECUADA GOBERNANZA DE CIBERSEGURIDAD

La estructura organizativa y las responsabilidades que habilitan la existencia de una adecuada gobernanza han sido descritas, además de en los documentos citados en el apartado anterior, en el *Prontuario de ciberseguridad para entidades locales*, elaborado de manera conjunta por el CCN y la Federación Española de Municipios y Provincias.

Aunque las responsabilidades relacionadas con la gobernanza se encuentran distribuidas entre distintos agentes implicados, con diferentes niveles de responsabilidad y atribuciones, **la responsabilidad de establecer una adecuada gobernanza de la ciberseguridad** mediante la aprobación de las políticas de seguridad de la información, 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 (ENS-2010), **es del titular del órgano superior correspondiente**.

En las entidades locales, esta responsabilidad principal recae en el presidente o presidenta. 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 información y las comunicaciones. Son los máximos responsables de la implantación del ENS.

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[8].

Sin embargo, en la práctica, de forma general, las Administraciones locales han asumido de manera errónea que la responsabilidad de la seguridad de la información y los servicios, materializada en el cumplimiento del Esquema Nacional de Seguridad, recae en exclusiva sobre los responsables de las áreas informáticas y tecnológicas, incurriendo en **un grave error de criterio** que menoscaba la ciberresiliencia de las instituciones.

Los responsables de las áreas informáticas ya asumen la responsabilidad de la gestión de los sistemas, que es **incompatible** con la responsabilidad sobre la seguridad de la información (artículo 10 del ENS-2010 y artículo 11 del ENS-2022).

[8] *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.

La responsabilidad de la ejecución de las actividades establecidas por la alta dirección corresponde a 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, al tesorero, a los funcionarios directores del departamento TIC y los jefes de área o servicio.

4. ELEMENTOS DE LA GOBERNANZA DE LA CIBERSEGURIDAD

Para lograr implantar un sistema de prevención proactiva de ciberseguridad, las organizaciones deben establecer un marco de gobernanza, en el que se designe a los responsables en la materia y sus funciones, y describir los procesos de gestión relacionados con la ciberseguridad[9].

De acuerdo con este marco y la experiencia de la Sindicatura en las auditorías de ciberseguridad, hay una serie de elementos que o bien son componentes esenciales de la gobernanza o son condiciones imprescindibles para su buen funcionamiento.

La relación de estos elementos esenciales es la siguiente:

- **Los órganos superiores de la entidad deben ejercer liderazgo y compromiso** con respecto a la seguridad de la información y deben velar por que sean satisfechas todas las necesidades y condiciones necesarias para el establecimiento de una gobernanza adecuada.

- 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 correspondiente**, es decir, por el presidente de la entidad. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización.

- Debe existir una **planificación estratégica en materia de ciberseguridad**, que proporcione un marco de actuación a medio plazo que asegure la atención a las necesidades prioritarias con respecto a la seguridad, y se encuentre alineada con la estrategia corporativa. La planificación estratégica de la seguridad evita una gestión reactiva basada principalmente en necesidades sobrevenidas.

- Debe existir un **comité de seguridad TIC** con un funcionamiento efectivo.

- Las entidades deben asignar **roles y responsabilidades en materia de seguridad de la información**.

- La entidad debe **disponer de los recursos materiales y humanos** adecuados para atender a las necesidades identificadas e implementar las medidas de seguridad necesarias.

[9] *Aproximación al marco de gobernanza de la ciberseguridad*, CCN 2022.

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.

- Deben existir **normas y procedimientos de seguridad formalizados y debidamente aprobados.**

- El conjunto de procesos implantados para la gestión de la seguridad debe constituir un **sistema de gestión de la seguridad de la información (SGSI)**, que trate la seguridad de manera continuada y proactiva, y que abarque todas las fases del proceso de seguridad: conocer, evaluar y tratar los riesgos y establecer las medidas de seguridad necesarias.

- Se debe establecer 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.

Aunque la ausencia de alguno de estos elementos no implica necesariamente la falta de efectividad de las medidas de seguridad que se encuentren implantadas en las entidades, la carencia de una correcta organización de la ciberseguridad impedirá asegurar que la efectividad se mantendrá a lo largo del tiempo, independientemente de las circunstancias y condicionantes existentes. En los siguientes apartados se desarrollan con mayor detalle estos aspectos.

5. EL COMITÉ DE SEGURIDAD TIC

Qué es el comité de seguridad TIC o comité de seguridad de la información

La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[10] o comité de seguridad de la información (CSI), que se constituye como un órgano colegiado, algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad. 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 estructura y composición debe constar en la PSI.

El CSI es el órgano especializado y permanente de una organización para la ciberseguridad y estará integrado por aquellas personas de la organización con responsabilidad en la toma de decisión en materia de seguridad y privacidad de la información, así como por aquellas designadas en representación de otros órganos o comités. Podrá integrar a vocales de otras áreas de la entidad que sean relevantes para la

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

finalidad del comité, tales como la persona designada como delegado de protección de datos o del departamento jurídico o de recursos humanos, entre otras.[11]

Consideraciones generales

De acuerdo con lo dispuesto en el ENS, con los criterios generales expuestos en las guías del CCN y con las distintas situaciones observadas en nuestras auditorías, consideramos que se deben tener en cuenta las siguientes consideraciones, tanto al definir la composición del CSI como en su funcionamiento:

- **No es un comité meramente técnico**, sino que debe integrar vocales de cualquier área significativa necesaria para llevar a cabo sus objetivos.

- Debe ser un **órgano con poder de decisión, ágil en su toma de decisiones**.

  Un comité sin poder de decisión puede resultar inefectivo. Por este motivo se requiere que el órgano cuente con integrantes del nivel más alto de las organizaciones, además de contar con el apoyo necesario para implantar cuantas decisiones y acuerdos se tomen en las reuniones.

- Debe **reunirse periódicamente** con objeto de conocer el estado de la seguridad de la información de la entidad y tomar las decisiones pertinentes de forma oportuna.

  En algunas de las entidades auditadas hemos observado una baja o nula actividad del comité, pese a estar constituido formalmente, lo cual es equivalente a su no existencia. En entidades de gran tamaño y dada la complejidad que presentan sus sistemas de información, el comité debería reunirse normalmente una vez al mes.

- **El personal con roles asignados en materia de seguridad de la información o protección de datos debe disponer del suficiente tiempo de dedicación a la seguridad** para desempeñar sus funciones de manera efectiva.

- **Debe abarcar todos los sistemas de información de la entidad.**

  En el curso de nuestras auditorías en los ayuntamientos hemos constatado que, en general, los **departamentos de policía municipal** gestionan de forma casi totalmente independiente sus propios sistemas de información, no integrándose en muchos casos en el marco general de ciberseguridad del ayuntamiento. Además, resulta habitual que, para determinados **sistemas críticos** de la entidad, la contratación, el desarrollo y el mantenimiento de estos sea efectuado por los **departamentos o servicios responsables de su explotación** y no por el departamento TIC.

  No es nuestra tarea definir cómo deben estar organizados en un ayuntamiento sus sistemas de información, ni si los sistemas policiales y otros sistemas críticos deben

[11] Apartado 5.1 de Aproximación al Marco de Gobernanza de la *Ciberseguridad. Año 2022*, CCN.

estar totalmente integrados con los sistemas corporativos o es mejor que estén totalmente separados. Esta es una decisión organizativa de la corporación.

Cualquiera que fuere la fórmula elegida, el marco de ciberseguridad debe ser único. Esto quiere decir que puede haber un único responsable de seguridad de la información con responsabilidades en el conjunto de sistemas de información del ayuntamiento. O puede haber un responsable de la seguridad de la información de los sistemas de información policiales y/o sistemas críticos, pero en este caso deberán estar integrados también en el CSI para que sean copartícipes y corresponsables de las decisiones que se adopten.

El comité de seguridad de la información debe ejercer sus competencias sobre todos los sistemas de la entidad sin excepciones, incluidos aquellos que por su naturaleza son gestionados directamente por los servicios que explotan dichos sistemas.

Componentes

La guía CCN-STIC 201 indica que será cada Administración la que establezca la composición de su CSI en función de sus competencias, estructura y circunstancias, dejando a las Administraciones la decisión de establecer los componentes de dicho órgano. No obstante, las guías del CCN establecen una serie de orientaciones sobre su composición y las responsabilidades de sus miembros.

Atendiendo a lo establecido por el CCN y la experiencia obtenida en nuestras auditorías, consideramos que los integrantes del CSI deberían ser, al menos, los siguientes:

- **El presidente** del comité debe ser el **concejal o diputado responsable** en materia TIC.
- Responsable de seguridad de la información, que ejercerá de secretario del CSI.
- Responsable de la información.
- Responsable del sistema.
- Responsable de seguridad física (RSF).
- Delegado de protección de datos (DPD).
- Responsable del cumplimiento legal.

Consideramos imprescindible la participación en el comité de seguridad de los **secretarios generales**, dado que sobre ellos recae la responsabilidad sobre la ejecución de muchas decisiones del comité. Puede ostentar el rol de responsable de seguridad.

El comité puede constituirse con miembros fijos y otros opcionales, por lo que además de los expuestos, podrá invitarse a intervenir en las reuniones a cuantas personas sean necesarias de acuerdo con los asuntos a tratar.

La composición del CSI debe constar en la PSI y sus miembros designados por el órgano superior de la entidad.

6. ROLES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

El ENS establece que la PSI deberá identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El **responsable de la información** determinará los requisitos de la información tratada.

b) El **responsable del servicio** determinará los requisitos de los servicios prestados.

c) El **responsable de la seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

d) El **responsable del sistema**, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria de este.

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

Las características de los roles y sus responsabilidades en materia de ciberseguridad se detallan en la *Guía de Seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad. Responsabilidades y Funciones*, además de ser una cuestión abordada por diversos documentos y guías del Centro Criptológico Nacional. El objeto de este apartado no es definir dichos roles y responsabilidades, sino exponer las buenas prácticas y errores que hemos visto durante nuestras auditorías.

Consideraciones generales

Para una correcta organización de la seguridad de la información, las entidades, tal y como establece la normativa y se ha señalado anteriormente, deben nombrar determinados roles y estos deben asumir ciertas responsabilidades. Al respecto y según nuestro criterio, son importantes las siguientes consideraciones:

- **Que los roles en materia de seguridad sean formalmente establecidos.**

  Los roles en materia de ciberseguridad deben ser formalmente asumidos por personas u órganos según se establezca en la política de seguridad de la información.

- **Que los roles establecidos ejerzan sus funciones de manera efectiva.**

  La mera designación de roles para cumplir con la normativa no es suficiente. Las organizaciones deben garantizar que las personas con roles establecidos en materia

de seguridad de la información y protección de datos de carácter personal **tengan la disponibilidad de tiempo necesaria para realizar sus tareas** de manera efectiva.

La dedicación compartida entre múltiples tareas y competencias o la existencia de múltiples tareas asignadas a una misma persona pueden originar riesgos como la falta de dedicación a la materia en cuestión o el conflicto entre prioridades de sus distintas responsabilidades.

- **Que los roles estén correctamente asignados, sin existir incompatibilidades con otras competencias.**

  Los documentos y guías del CCN nos describen algunas incompatibilidades legales para evitar conflictos de intereses. Adicionalmente, existen roles que han de realizar sus funciones con independencia, de manera transversal a toda la organización.

Responsable de seguridad de la información

El responsable de seguridad de la información puede ser un cargo unipersonal del nivel directivo de la organización o un órgano colegiado. **No requiere desarrollar funciones de carácter técnico, su función es básicamente supervisora** del cumplimiento efectivo de las decisiones del CSI y de la normativa de seguridad.

En una entidad local, la máxima figura que conoce los servicios que presta la entidad es el/la secretario/a general y, en consecuencia, está en mejores condiciones para asumir el rol de responsable de la información o nombrar a alguien que dependa directamente de este. Es quien conoce mejor todos los servicios ofrecidos por la organización y su importancia y, con ello el nivel de seguridad requerido. Puede apoyarse en todas las personas de la institución que considere oportuno.

La *Guía de Seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad Responsabilidades y Funciones* establece "*que la figura del Responsable de la Seguridad debe estar situada en una posición que le permita tener un acceso directo a los niveles directivos de la organización.*". Y además indica que "en el caso de entidades locales (Diputaciones, Cabildos o Ayuntamientos), debería depender del Secretario General".

De acuerdo con la guía CCN-STIC 201, el responsable de seguridad **será el secretario del Comité de Seguridad de la Información**, y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Responsable de seguridad física

Este rol asume la responsabilidad sobre la seguridad física de la organización y sería el enlace con el Comité de Seguridad Corporativa. Tanto este comité como el CSI deben estar debidamente coordinados.

7. NORMATIVA INTERNA DE CIBERSEGURIDAD

Un sistema de gestión continuada de la seguridad de la información requiere que la PSI se complete con normativa interna, desarrollada en documentos más precisos que materialicen los requisitos de la PSI (uso correcto de equipos, servicios, instalaciones, usos indebidos, responsabilidades del personal); y un conjunto de procedimientos de seguridad que describan, paso a paso, cómo deben realizarse tareas concretas (documentos que detallan cómo se realizan las tareas habituales, responsables, reporte de comportamientos anómalos).

Es importante diferenciar entre norma y procedimiento. Una norma o política (del inglés *policies)* indica "qué debe hacerse". Los procedimientos detallan las acciones a realizar, es decir, el "cómo debe hacerse" y, cuando procede, quiénes deben hacerlo.

Esta normativa interna debe diseñarse para ser aplicada, no para cumplir una mera formalidad. El contenido del conjunto de políticas, normas y procedimientos aprobados debe ser una representación fidedigna y precisa del sistema de seguridad implantado por el ente local. La aprobación de un marco normativo que no represente la realidad del ente deviene en un uso estéril de recursos por su carencia de efectividad y en una falsa percepción de cumplimiento que puede conllevar el abandono de otras medidas más adecuadas.

Cada entidad debe establecer y aprobar su propia organización de seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que deberá estar recogida en su política de seguridad de la información[12].

Es importante tener en cuenta que, independientemente del modelo organizativo existente en una entidad, toda la normativa de ciberseguridad afectará, sin excepción, a todos los departamentos y sistemas de información. La organización de la seguridad, sea la que sea, debe estar definida en la PSI aprobada por el órgano superior e incluirá todos los sistemas de información sin ninguna excepción.

Política de seguridad de la información

La política de seguridad de la información (PSI) es un documento de alto nivel que define, de acuerdo con el artículo 12 del ENS (2022), el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. Constituye la expresión formal del compromiso y liderazgo de la alta dirección con la seguridad.

[12] *CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones.*

El ENS indica los principios básicos y los requisitos mínimos de la PSI. Además, existen algunos aspectos que las organizaciones deben tener en cuenta, como son:

- Debe ser elaborada por el CSI y aprobada por el presidente del ente local.
- Que sea un documento breve, dejando detalles técnicos para las normas que la desarrollan.
- Debe ser revisada y actualizada periódicamente.
- Debe ser accesible (publicada y dada a conocer) a los empleados y colaboradores de la organización.

Normativa de seguridad

Se dispondrá de una serie de documentos que describan:

- El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Esta normativa deberá ser aprobada por quien se disponga en la PSI. Es de carácter obligatorio y deberá estar a disposición de todos los miembros de la organización (publicada en la intranet corporativa).

Procedimientos de seguridad

Las entidades deben disponer de un conjunto de procedimientos aprobados que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos anómalos.
- La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere,

Los procedimientos deberán ser aprobados por quien se disponga en la PSI.

8. OTROS ÓRGANOS DE GOBIERNO RELACIONADOS CON LA GESTIÓN DE LA CIBERSEGURIDAD

Las organizaciones, dependiendo de su tamaño y complejidad, pueden disponer, además del CSI, de diversos órganos de gobierno relacionados con la gestión de la ciberseguridad, que pueden administrar funciones a distintos niveles, incluyendo el operativo, el ejecutivo/supervisión o el de gobierno. Algunos de estos órganos pueden ser:

- El comité de seguridad corporativa.
- El comité de gobernanza TIC
- El comité de gestión de crisis.
- El comité de seguridad física.
- El comité de protección de datos.
- El centro de operaciones de seguridad.
- La oficina de gobernanza y cumplimiento normativo.

La existencia de estos órganos responde, en general, a las exigencias de la normativa básica de aplicación, el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos. No obstante, puede ser también de aplicación otra legislación sectorial y específica, como la de la Ley de Protección de Infraestructuras Críticas (Ley PIC8/2011), que establecen sus propios requisitos de seguridad adicionales, incluyendo medidas organizativas.

Aunque la existencia de estos órganos puede no ser obligatoria en todas las circunstancias, dependiendo de la legislación que sea de aplicación en cada caso, sí resulta **imprescindible que**, en caso de existir, el **conjunto de estos órganos coordine adecuadamente sus actividades y existan mecanismos de comunicación y colaboración** entre ellos.

Aunque la revisión de estos órganos no estaba incluida en el alcance de las auditorías de los CBCS, por su importante relación realizamos a continuación algunos comentarios sobre ellos.

Comité de gobernanza TIC

Es el órgano colegiado encargado de la definición y supervisión de la estrategia sobre las TIC en una entidad, que debería aprobar la Junta de Gobierno. La definición de la composición y funciones de este comité corresponde a este órgano superior; no obstante, debe haber algún miembro común con el CSI (como por ejemplo el responsable del sistema) de forma que sus actividades sean coherentes.

Se entiende por gobierno o gobernanza TIC el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. Constituye una parte esencial del gobierno de la entidad en su conjunto y aglutina la estructura

organizativa y directiva necesaria para asegurar que las TIC soportan y facilitan el desarrollo de los objetivos estratégicos definidos. Esto garantiza que:

- Las TIC están alineadas con la estrategia del negocio.
- Los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente.
- Todos los riesgos relacionados con TI son conocidos y administrados y los recursos de TI están seguros, incluyendo los relacionados con la ciberseguridad mediante la coordinación con el CSI.

En las entidades de pequeño tamaño el comité de gobernanza TIC y el de ciberseguridad pueden confluir en uno único.

Comité de gestión de crisis

Un ciberincidente grave provocará una crisis y esto implica la necesidad de tomar decisiones bajo mucha presión, en poco tiempo y con información probablemente incompleta.

Con independencia del tipo de ciberincidente que cause la crisis, se hace patente la componente de gestión que implica su resolución. Para ello, la organización afectada necesita haberse dotado de las capacidades y estructuras de gestión (comités/equipos) adecuadas que le han de permitir abordarla con garantías de éxito.

En resumen, la capacidad de gestionar una situación de crisis depende en gran medida de las estructuras o comités que se hayan establecido antes de que ocurra el desastre causado por un ciberincidente, suceso de "baja probabilidad y alto impacto".

El comité de crisis es el órgano encargado de la gestión de la crisis a alto nivel dentro de la organización, con una visión estratégica. Se encargará de tomar las decisiones y coordinar las acciones necesarias para la resolución de los incidentes que hayan sido calificados como crisis dentro de la entidad, determinando y/o validando las estrategias de análisis, de contención y mitigación que permitan recuperar las operaciones en el menor tiempo posible, minimizando los impactos sobre las partes interesadas.

Aunque la revisión de los diversos aspectos relacionados con la gestión y los comités de crisis han quedado fuera del alcance de nuestras auditorías, recomendamos que se analicen todos los aspectos relacionados con la gestión de las crisis provocadas por ciberincidentes de forma coordinada con el CSI.

Centros de operaciones de ciberseguridad

De acuerdo con la guía CCN-STIC 201, la gobernanza de la seguridad en una organización se articula a través de un comité de seguridad TIC y se implementa mediante centros de operaciones de ciberseguridad que velan por la operación y correcta implementación de la seguridad, mediante una vigilancia continua de los sistemas de información

Bajo la dirección del responsable de seguridad, el centro de operaciones de ciberseguridad presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, especialmente los que manejan información clasificada, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

En definitiva, los centros de operaciones de ciberseguridad articularán la respuesta a los incidentes de seguridad, sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración con competencias y de la función de coordinación del CSIRT-CV de referencia y del CCN-CERT, como coordinador nacional.

Asimismo, en función de la naturaleza y dimensiones de la organización, el centro de operaciones de ciberseguridad puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el responsable de seguridad.

Equipo de respuesta a incidentes de seguridad

Este equipo se encarga de gestionar los incidentes de seguridad bajo las directrices marcadas por el CSI y el responsable de seguridad y posibles alertas recibidas del centro de operaciones de ciberseguridad.

Está compuesto por un equipo con capacidades de atención inmediata denominado "primer nivel de atención" y por un grupo de especialistas para aquellos incidentes no resueltos por el primer nivel que requieran un mayor grado de especialización.

9. PRINCIPALES DEFICIENCIAS EN MATERIA DE GOBERNANZA OBSERVADAS EN NUESTRAS AUDITORÍAS

En cada uno de los dieciocho informes de auditoría de ciberseguridad individuales realizados hemos indicado la situación en cuanto a la gobernanza y hemos observado que las entidades, en general, no tienen establecida una adecuada gobernanza de la seguridad de la información. A continuación, señalamos las principales deficiencias observadas.

En materia de normativa de seguridad

Una de las carencias generalizadas detectadas es la falta de un marco normativo y procedimental de seguridad formalmente aprobado. De acuerdo con la definición de los niveles del modelo de madurez establecido por el CCN, para alcanzar un nivel 3 de madurez es requisito necesario la existencia de procedimientos formalmente aprobados. Las deficiencias en este aspecto impiden que los controles alcancen niveles superiores al nivel 2, siendo las más comunes:

- Inexistencia de PSI formalmente aprobada por la corporación, o desactualizada o no adaptada a la realidad de las entidades, lo que impide que los principios que deben regir las actuaciones en materia de seguridad sean conocidos por toda la corporación.

- Inexistencia de normativa y procedimientos formalizados, lo que puede originar el riesgo de no realización de tareas importantes por no estar asignadas a responsables, dependiendo su ejecución de la buena voluntad de quienes los llevan a cabo.

- El contenido de los procedimientos no detalla de manera clara y precisa las tareas a realizar ni quiénes son los responsables de ejecutarlas, especificando únicamente el deber de realizar la acción, aspecto que corresponde a las normas de seguridad de rango superior, lo que genera procedimientos ineficaces.

- Existencia de procedimientos escritos que, aunque están definidos de manera correcta, han sido realizados por consultoras externas y tienen poca o nula adaptación al entorno de la entidad, dado que no reflejaban la realidad de las acciones llevadas a cabo en la práctica.

- Los procedimientos existentes, incluidos aquellos formalmente aprobados, no se encuentran actualizados y no representan con fidelidad los procesos de seguridad que describen.

En relación con el comité de seguridad de la información

- Existen entidades que no disponen de comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad.

- En otros casos, aunque el comité de seguridad de la información está formalmente constituido, no se reúne o no lo hace con la periodicidad necesaria, lo que impide hacer un seguimiento del estado de la seguridad de la información y tomar las decisiones pertinentes de forma oportuna.

- El comité de seguridad no dispone de los miembros adecuados, estando compuesto únicamente de miembros con cargos relacionados con los sistemas de información y la seguridad. La carencia de miembros con el más alto poder de decisión en la organización y de vocales de las áreas significativas convierte al comité en un órgano meramente técnico e impide un gobierno eficiente y la toma de decisiones estratégicas a nivel corporativo.

En relación con los roles de seguridad

Además de establecer un marco normativo y procedimental, las entidades deben nombrar los distintos roles en materia de seguridad y asignar formalmente responsabilidades a dichos roles. Las principales deficiencias relacionadas que hemos advertido durante las auditorías han sido:

- Existen entidades que no han asignado los roles y responsabilidades en materia de seguridad de la información.

- Existen entidades que no disponen de un delegado de protección de datos formalmente nombrado.

- Algunos de los roles de seguridad no ejercen sus funciones de manera que se garantice la necesaria independencia y la ausencia de conflicto de intereses.

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

  - Hemos observado situaciones en las que los roles designados en materia de seguridad de la información (DPD y responsable de seguridad) están asumidos por personal externo que, aunque ejercen sus funciones de manera acorde a lo especificado en el contrato, estos contratos son licitados por el departamento TIC. Esta dependencia en la contratación del departamento TIC limita la capacidad operativa y de decisión de los servicios contratados, que deberían ser promovidos desde secretaría general.

  - El DPD coincide con el responsable de seguridad. La AEPD señala que "en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible [...] siempre que en la misma concurran los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas [...] que garanticen la necesaria independencia y la ausencia de conflicto de intereses [...]".

    Es decir, **con carácter general ambos roles son incompatibles**.

- Algunos roles en materia de seguridad no disponen de la dedicación suficiente para las necesidades de una entidad del tamaño de las auditadas. Los responsables de seguridad de manera general no ejercen sus funciones de manera exclusiva, incurriendo en una acumulación de competencias no directamente relacionadas con la seguridad de la información que impide que desarrollen sus funciones de forma efectiva.

En relación con el liderazgo y el compromiso con la ciberseguridad

Además de las cuestiones anteriores, para la implantación exitosa de un sistema de gestión de la seguridad de la información se requiere el liderazgo, implicación, compromiso e impulso de medidas por parte de los órganos superiores del ente local (en particular, el presidente y la junta de gobierno). De estos depende la existencia de unos controles adecuados sobre los sistemas de información y las comunicaciones. En este aspecto, las principales deficiencias que hemos observado han sido:

- Inexistencia de implicación de los máximos responsables de la organización.

  Tal y como se ha indicado anteriormente, los órganos superiores de las entidades son los **responsables** de la seguridad de los sistemas de información y las

comunicaciones, y su implicación, compromiso y liderazgo constituyen el factor más importante para la implantación exitosa de un SGSI. Este compromiso también debe extenderse a la dirección, que son los responsables de articular y facilitar la ejecución de las actividades en materia de ciberseguridad.

La ausencia de este liderazgo tiene un efecto generalizado sobre la organización y gestión de la seguridad en la organización.

- La ausencia de planes estratégicos desarrollados e impulsados por el más alto nivel de la corporación en los que se establezcan acciones, objetivos y medidas concretas para alcanzar los niveles de seguridad exigidos por la normativa.

- La falta de recursos, tanto económicos como de personal, en los departamentos TIC, indispensable para implantar las medidas de seguridad necesarias y llevar a cabo proyectos transversales que afecten a toda la organización.

- La falta de una cultura de ciberseguridad en la entidad, materializada en acciones formativas y campañas de concienciación dirigidas a los empleados.

10. COORDINACIÓN E INTEGRACIÓN CON ORGANISMOS DE REFERENCIA

La mayoría de las entidades auditadas han participado de las actividades incluidas en el Plan de Choque de Ciberseguridad para las Entidades Locales de la Comunitat Valenciana, promovido por la Dirección General de Tecnologías de la Información y las Comunicaciones (DGTIC) de la GVA.

Entre las actividades de dicho plan, se encuentra el despliegue de varias de las herramientas ofrecidas por el CSIRT-CV o el CCN, siendo esta una de las mejores prácticas observadas en las entidades auditadas.

Adherirse a los servicios que proporcionan los organismos referentes en materia de seguridad aporta muchas ventajas, entre las que destacamos:

- La gestión de incidentes: vigilancia, sistema de alertas y soporte para la detección y tratamiento de las amenazas detectadas.

- Participación en aquellas acciones propuestas por el plan de choque de ciberseguridad para las EELL, que la Generalitat Valenciana ha puesto a disposición de los ayuntamientos de mayor tamaño, que conllevan entre otras, monitorización y análisis de eventos, emisión de informes, soporte, etc.

- Asesoramiento técnico en la implantación de medidas de seguridad, materializado en acciones como las recomendaciones recibidas de parte del CSIRT-CV para la maquetación de puestos de trabajo durante la pandemia.

Además de las tareas de colaboración con los organismos de referencia, estos ponen a disposición de las entidades un conjunto de herramientas en materia de ciberseguridad que, de acuerdo con lo observado, han tenido una acogida muy positiva entre las entidades.

El siguiente listado muestra las herramientas que hemos observado desplegadas en algunas de las organizaciones auditadas:

- LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas), herramienta para la gestión de ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad.

- CARMEN, solución desarrollada con el objetivo de identificar el compromiso de la red de una organización por parte de amenazas persistentes avanzadas. Herramienta en fase de implantación a fecha 31 de diciembre de 2021 pero implantada en su totalidad a fecha de este informe.

- CLAUDIA, solución de *endpoint* integrada con la herramienta CARMEN que permite tener una visión más completa de lo que ocurre dentro de una red.

- GLORIA, plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos (SIEM).

- 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.

- microCLAUDIA, que proporciona protección contra código dañino de tipo *ransomware*.

- REYES, que permite realizar investigación y análisis sobre ciberincidentes de forma ágil y rápida. Consiste en un metabuscador de información de diversas fuentes especializadas en ciberamenazas, que está integrado con herramientas de análisis del CCN-CERT. Las entidades reciben informes periódicos del CSIRT-CV con incidentes de seguridad relacionados con los dominios y correos corporativos (vigilancia digital).

APÉNDICE 3

Situación de los controles básicos de ciberseguridad

1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS (CBCS 1)

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.

Por qué es importante este control de ciberseguridad

La finalidad del control es conocer lo que está conectado a la red para que pueda ser defendido y, posteriormente, impedir que dispositivos no autorizados se conecten a la red. Este control ayuda a las organizaciones a definir la base de lo que hay que defender, ya que, si se desconoce qué dispositivos están conectados, no pueden ser defendidos.

El órgano competente debe aprobar formalmente un procedimiento que especifique las acciones a realizar para mantener actualizado el inventario de todo el *hardware* de la entidad, que incluya también aspectos como la realización periódica de revisiones y la descripción de las medidas implantadas para impedir el acceso de dispositivos físicos no autorizados a la red corporativa.

El inventario debe ser tan completo como sea posible. En organizaciones con un nivel de madurez básico el inventario puede ser realizado y mantenido con procedimientos manuales y, en otras más maduras, utilizando herramientas de escaneo que detecten los dispositivos conectados a la red corporativa.

Debe existir en toda la red corporativa un control efectivo que impida el acceso a esta a cualquier dispositivo físico no autorizado. Es más probable que las máquinas no controladas estén ejecutando *software* que no sea necesario para los fines de la entidad (introduciendo posibles vulnerabilidades de seguridad), o ejecutando *malware* introducido por un atacante después de que un sistema ha sido comprometido.

Otros dispositivos que se conectan a la red corporativa (por ejemplo, sistemas para demostraciones, redes para invitados, etc.) deben ser gestionados con cuidado o aislados para prevenir accesos no autorizados que comprometan la seguridad.

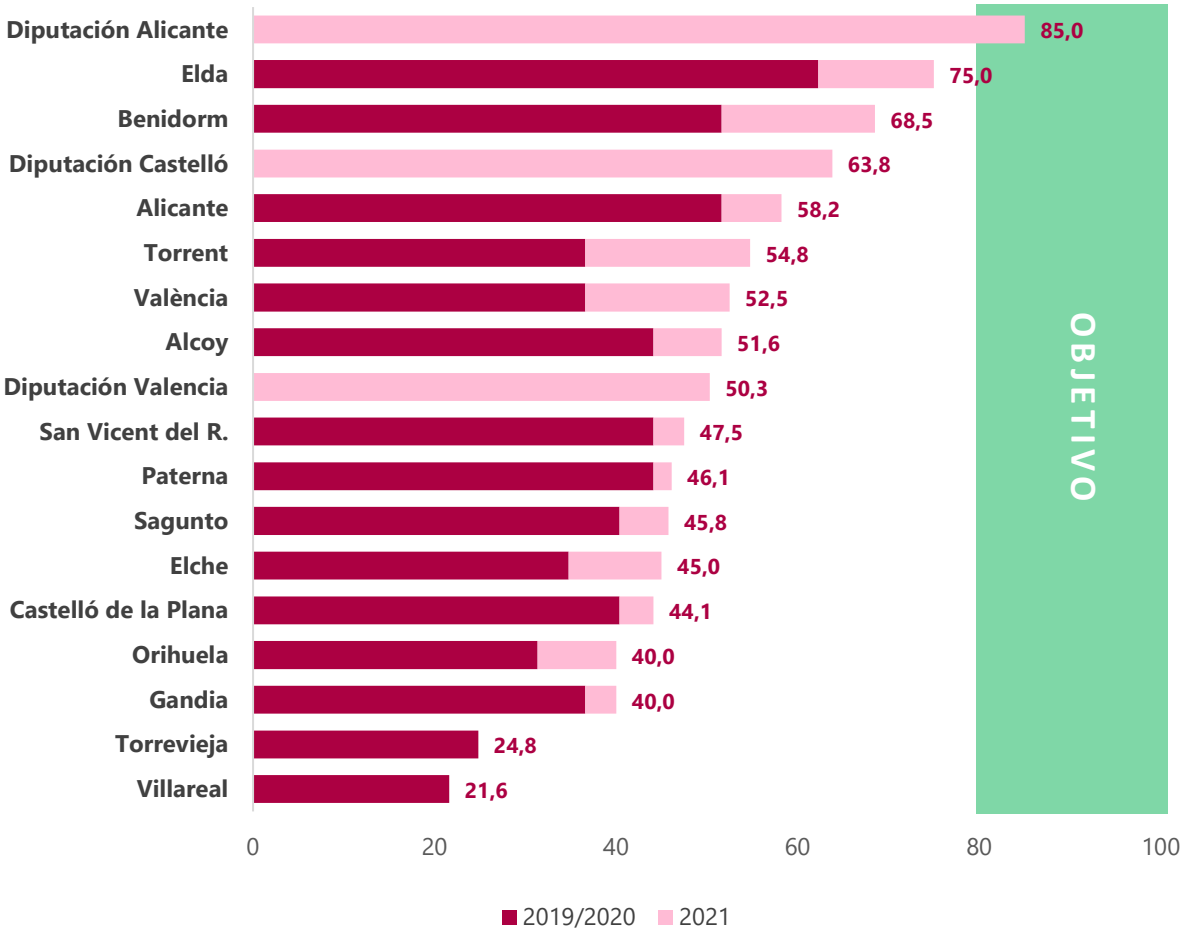
Los dispositivos personales de los empleados (portátiles, tabletas, móviles) que se conecten a la red corporativa también pueden verse comprometidos y ser usados para infectar los recursos internos.

Situación del índice de madurez del control

El siguiente gráfico 6 muestra el índice de madurez del CBCS 1 que los quince ayuntamientos obtuvieron en nuestras auditorías iniciales en 2019/2020 y la mejora que han experimentado hasta el 31 de diciembre de 2021, alcanzando una media del 47,7%.

También se incluye la situación del control en las diputaciones a 30 de septiembre de 2021, que obtienen un índice de madurez medio del 66,3%. Únicamente la Diputación de Alicante alcanza el nivel de madurez exigido en el ENS.

Gráfico 6. Índice de madurez del CBCS 1 por entidad



Se observa que casi todas las entidades, exceptuando dos ayuntamientos, han realizado acciones que mejoran los índices de madurez previos. Sin embargo, la mejora, en general, no es suficiente para alcanzar el nivel que exige el ENS.

Situación de los subcontroles revisados

El CBCS 1 consta de dos subcontroles:

- CBCS 1.1: Inventario de activos físicos autorizados
- CBCS 1.2: Control de dispositivos físicos no autorizados.

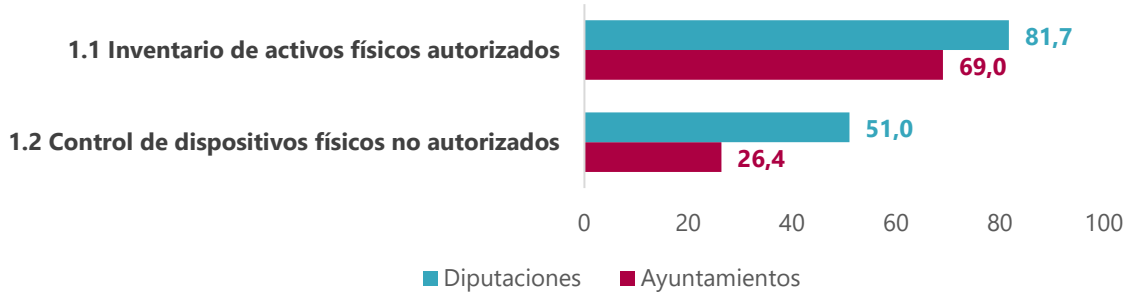
Si analizamos el índice de madurez medio para cada uno de estos subcontroles, se observa:

- Los ayuntamientos tienen cierto control sobre sus inventarios de *hardware* (69,0%), pero los mecanismos para controlar el acceso de dispositivos no autorizados a las redes corporativas son, en general, inexistentes o deficientes.

- Las diputaciones alcanzan, en promedio, el nivel exigido por el ENS para el control del inventario, pero no lo alcanzan para el control de dispositivos no autorizados, aunque la Diputación de Alicante sí que alcanza un índice de madurez del 90% en este subcontrol.

De forma gráfica:

Gráfico 7. Índice medio de madurez de los subcontroles del CBCS 1 en 2021



Para subsanar las deficiencias detectadas y alcanzar un nivel aceptable de efectividad del control, las entidades deben mantener el inventario de activos actualizado, realizar revisiones periódicas del *hardware* e implantar soluciones que permitan restringir el acceso de dispositivos físicos no autorizados a las redes corporativas.

2. INVENTARIO Y CONTROL DE "SOFTWARE" AUTORIZADO (CBCS 2)

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.

Por qué es importante este control básico de ciberseguridad

La finalidad de este control es asegurar que solo se ejecuta *software* autorizado en los sistemas de la organización, impidiendo la ejecución de *software* no autorizado o potencialmente vulnerable.

Mantener un inventario actualizado de *software* es importante, ya que permite conocer qué hay que proteger. Por ejemplo, el control de todo el *software* existente desempeña un papel fundamental en la planificación y ejecución de copias de seguridad y en la recuperación del sistema. Sin el conocimiento o el control apropiados de los programas desplegados en una organización, los defensores no pueden asegurar adecuadamente su protección. Las organizaciones que no tienen inventarios completos de *software* no pueden encontrar cuál es el vulnerable o malicioso para mitigar problemas o eliminar a los atacantes.

Por otra parte, disponer de una lista blanca de aplicaciones autorizadas limita la capacidad de ejecutar únicamente a aquellas que están expresamente autorizadas. Este control a menudo se considera uno de los más eficaces para la prevención y detección de ciberataques. La implementación del control a menudo requiere que las organizaciones reconsideren sus políticas y su cultura, puesto que los usuarios ya no podrán instalar el *software* que deseen.

La aplicación de parches y actualizaciones en el *software* inventariado y controlado permite a las entidades eliminar las vulnerabilidades o reducir los riesgos derivados de la materialización de las amenazas. Para que el proceso de actualización y parcheo sea posible, es necesario que la entidad cumpla con los siguientes requisitos: los programas utilizados deben de encontrarse en un estado de su ciclo de vida que permita la liberación de actualizaciones del fabricante, las licencias de *software* comercial deben encontrarse activas, y aquel que ha sido adaptado e implantado específicamente para la entidad debe encontrarse soportado por contratos de mantenimiento con las empresas correspondientes.

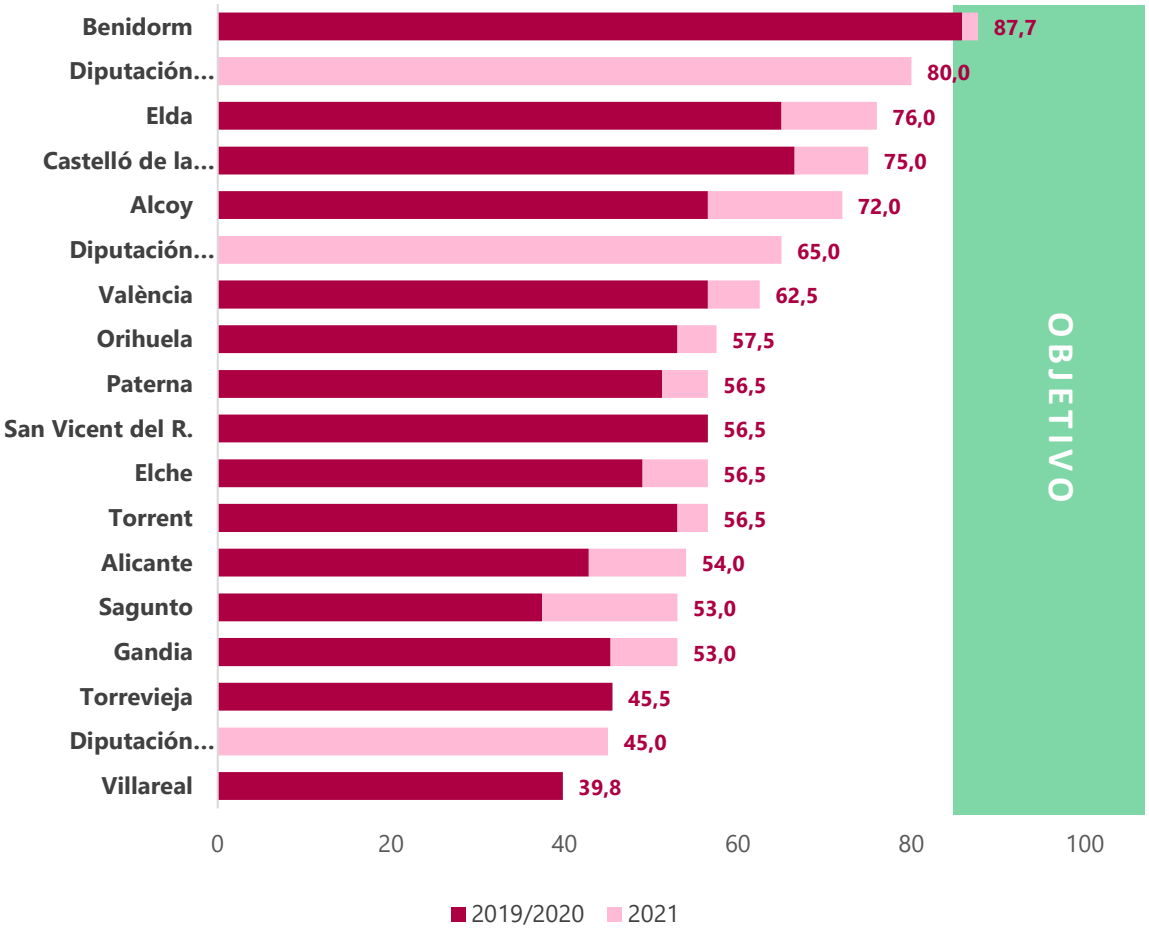
Las entidades deben disponer de un procedimiento que describa la gestión del inventario, que incluya todas las aplicaciones e identifique a sus responsables. Adicionalmente, se realizarán revisiones periódicas de los programas, que deberán ser documentadas. La efectividad del control es producto de un inventario de *software* actualizado, junto a una lista blanca de aplicaciones permitidas y la implantación de las medidas necesarias para bloquear cualquier aplicación no incluida dentro de esta lista.

Situación del índice de madurez del control

El siguiente gráfico muestra el índice de madurez del CBCS 2 que los quince ayuntamientos obtuvieron en nuestra revisión inicial y la mejora experimentada hasta el 31 de diciembre del 2021, que obtuvieron un índice medio del 60,1%.

Las tres diputaciones provinciales obtuvieron un índice de madurez medio del 63,3%.

Gráfico 8. Índice de madurez del CBCS 2 por entidad



Se observa que casi todos los ayuntamientos, exceptuando dos de ellos, han realizado acciones que mejoran los índices de madurez obtenidos en 2019/20. Únicamente uno de los ayuntamientos auditados y una de las diputaciones alcanzan el nivel que exige el ENS.

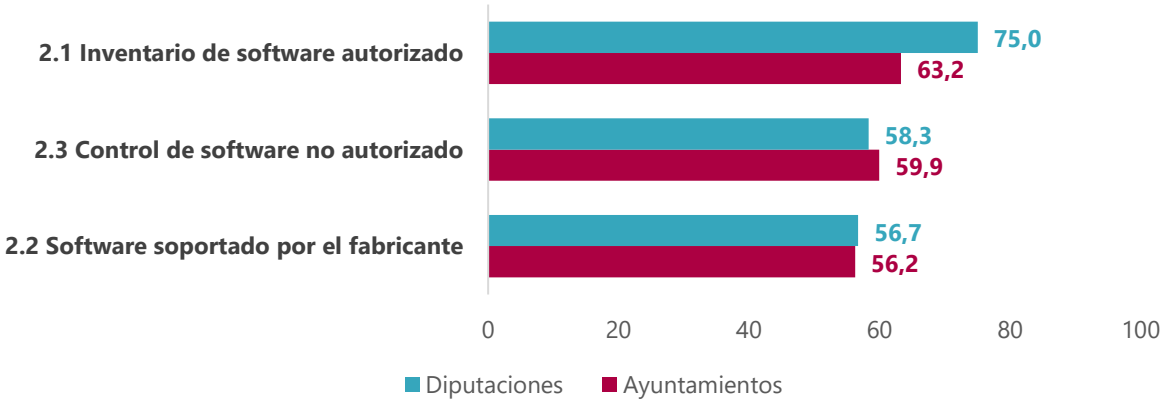
Situación de los subcontroles revisados

El CBCS 2 consta de tres subcontroles:

- CBCS 2.1: Inventario de *software* autorizado
- CBCS 2.2: *Software* soportado por el fabricante
- CBCS 2.3: Control de *software* no autorizado

Si analizamos el índice de madurez medio para cada uno de los subcontroles se observa que ninguno alcanza, en promedio, el nivel exigido por el ENS, tal como se ve en el siguiente gráfico.

Gráfico 9. Índice medio de madurez de los subcontroles del CBCS 2 en 2021



Además de elaborar y aprobar formalmente procedimientos que describan la gestión integral del *software* de la entidad y las medidas implantadas, se deben definir listas blancas de *software* autorizado, el proceso de autorización para la instalación de *software*, la implantación de las medidas técnicas que impidan la ejecución del *software* no autorizado y realizar revisiones periódicas. Adicionalmente, se deben definir planes de mantenimiento de *software* que consideren la totalidad de aplicaciones y revisar y actualizar todos los sistemas que se encuentran fuera de su período de soporte.

3. PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES (CBCS 3)

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.

Por qué es importante este control básico de ciberseguridad

La finalidad de este control es conocer y eliminar debilidades técnicas que existen en los sistemas de información de la organización, reduciendo la probabilidad de que los sistemas sigan siendo vulnerables.

Las entidades deben contar con un plan de mantenimiento del equipamiento físico y lógico, que detalle los componentes a revisar y los responsables. Se especificará el seguimiento continuo de anuncios de defectos publicados por los fabricantes y se documentarán las acciones llevadas a cabo para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones, teniendo en cuenta el riesgo que puede implicar dicho cambio.

Se deben implementar herramientas que centralicen y automaticen el proceso de gestión de vulnerabilidades, actualizaciones y parches, para dotarse de la capacidad de detectar y remediar debilidades de *software* explotables. Debe perseguirse la detección de vulnerabilidades de seguridad en los distintos sistemas de forma automática, continua y

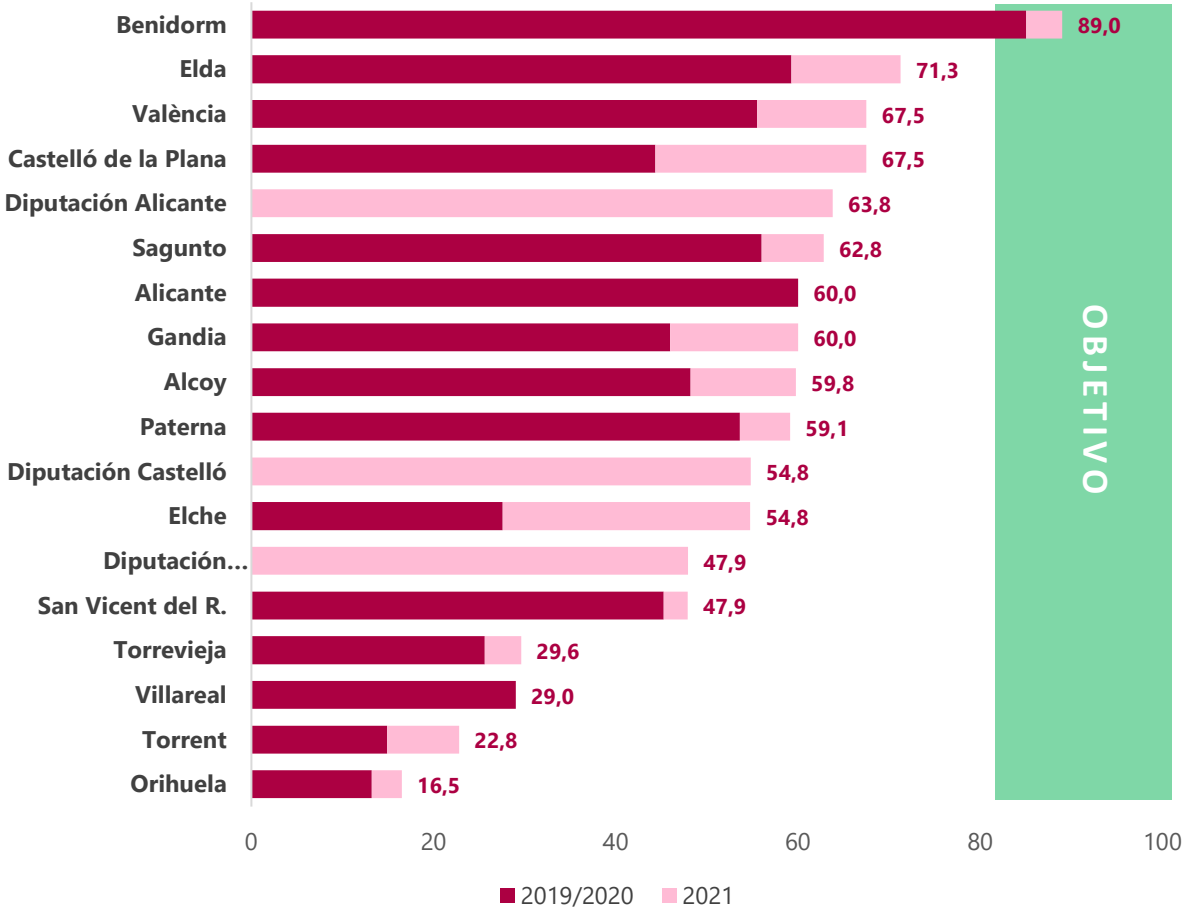
proactiva, y facilitar la instalación de actualizaciones y parches para solucionar las vulnerabilidades existentes. En otro caso existirá una alta probabilidad de que sus sistemas informáticos sean comprometidos.

Los ciberdefensores deben operar con un flujo constante de información: actualizaciones de programas, parches, avisos de seguridad, boletines de amenazas, etc. La comprensión y gestión de las vulnerabilidades es una actividad continua, que requiere tiempo, atención y recursos significativos. Los atacantes tienen acceso a la misma información y pueden aprovechar las brechas entre la aparición de nuevos conocimientos y su remediación. Por ejemplo, cuando los investigadores reportan nuevas vulnerabilidades, comienza una carrera entre todas las partes, incluyendo atacantes (para "armarse", desplegar un ataque y explotarlo), proveedores (para desarrollar, implementar parches o firmas y actualizaciones) y defensores (para evaluar riesgos, parches de prueba e instalarlos).

Situación del índice de madurez del control

El siguiente gráfico muestra el índice de madurez del CBCS 3 que las quince entidades obtuvieron en nuestra revisión inicial y la mejora que han experimentado hasta el 31 de diciembre del 2021. Se añade también el índice de madurez de las tres diputaciones.

Gráfico 10. Índice de madurez del CBCS 3 por entidad



El índice de madurez medio ha sido del 53,2% en los ayuntamientos y del 55,5% en las diputaciones.

Todos los ayuntamientos han realizado acciones que mejoran los índices de madurez obtenidos durante nuestro trabajo de 2019/20, pero dichas acciones no son suficientes para alcanzar el nivel que se exige en la normativa. Únicamente Benidorm alcanza el nivel exigido sobre el control de vulnerabilidades.

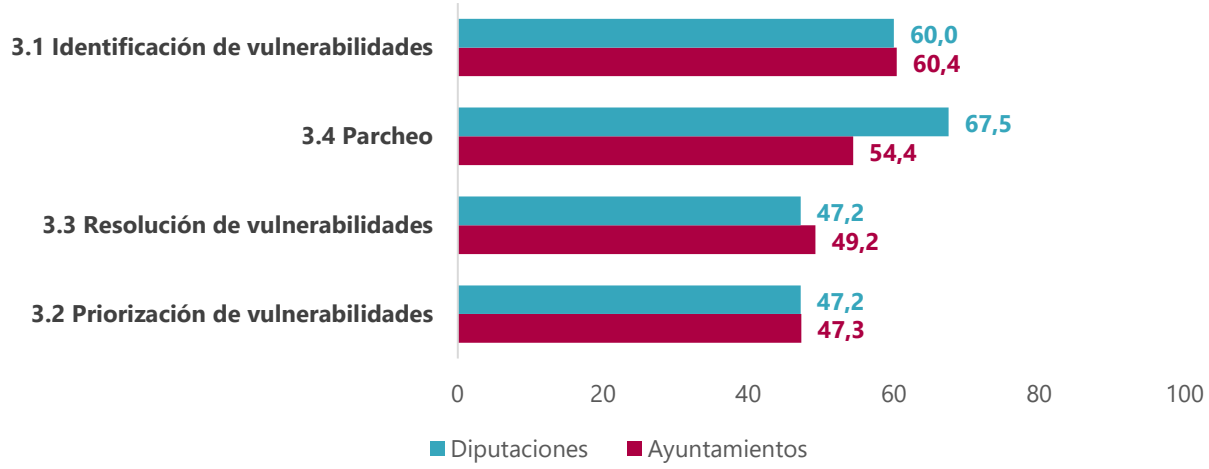
Situación de los subcontroles revisados

El CBCS 3 consta de cuatro subcontroles:

- CBCS 3.1: Identificación de vulnerabilidades
- CBCS 3.2: Priorización de vulnerabilidades
- CBCS 3.3: Resolución de vulnerabilidades
- CBCS 3.4: Parcheo

Si analizamos el índice de madurez medio para cada uno de los subcontroles se observa que, en general, los mecanismos de control implantados para la gestión de vulnerabilidades no alcanzan el nivel de eficacia necesario.

Gráfico 11. Índice medio de madurez de los subcontroles del CBCS 3 en 2021



Para implantar un control efectivo de identificación y remediación de vulnerabilidades, las entidades deben definir los sistemas a revisar, la periodicidad de las revisiones, el análisis de sistemas previo a la entrada en producción, el seguimiento de anuncios de fabricantes y boletines oficiales en materia de seguridad, la priorización de resoluciones basada en el análisis de riesgos y la documentación de las vulnerabilidades tratadas.

4. USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS (CBCS 4)

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.

Por qué es importante este control básico de ciberseguridad

Este control garantiza que los privilegios de administración de los sistemas estén asignados únicamente a los empleados que los necesitan, en base a las funciones que desempeñan (principio de mínimo privilegio) y que la entidad pueda atribuir las acciones administrativas a usuarios identificables (trazabilidad).

Desafortunadamente, para facilitar la agilidad y la comodidad, muchas organizaciones permiten que su personal tenga derechos de administrador tanto a nivel de una aplicación de gestión como en los sistemas que le dan soporte (sistema operativo, base de datos, etc.), así como en sus equipos. Esta situación deriva en la existencia del riesgo de acceso y de cambios no autorizados a los sistemas y datos, que puede materializarse utilizando los privilegios excesivos de un usuario como puerta de entrada para acceder desde fuera a la red interna de la entidad.

Este control conlleva que las cuentas de usuarios administradores de aplicaciones, bases de datos, sistemas operativos y equipos de usuario deben estar identificadas y su uso controlado, eliminando las que no se utilizan y cambiando las contraseñas que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

El uso inadecuado de privilegios administrativos es un método primario para que los atacantes se propaguen dentro de una entidad objetivo. Hay técnicas de ataque muy comunes que aprovechan los privilegios administrativos incontrolados. Por ejemplo, un usuario administrador de su equipo abre un adjunto de correo electrónico malicioso, descarga y abre un archivo de un sitio web malicioso, o simplemente navega en un sitio web que aloja contenido del atacante que puede explotar automáticamente navegadores. El archivo o *exploit* contiene código ejecutable que se activa en el equipo de la víctima, ya sea automáticamente o engañando al usuario para que ejecute su contenido. Si la víctima tiene privilegios administrativos, el atacante puede apoderarse completamente de su máquina e instalar los *keyloggers* (registradores de teclas), los *sniffers* y el *software* de control remoto para encontrar contraseñas administrativas y otros datos sensibles. Además, el atacante es capaz de acceder a todos los recursos compartidos de la víctima.

Si los privilegios administrativos se distribuyen de forma holgada, o las contraseñas son idénticas a las utilizadas en sistemas menos críticos, o a las que vienen de origen por defecto, al atacante le cuesta mucho menos tomar el control total de los sistemas, porque hay muchas más cuentas que pueden actuar como vectores de penetración.

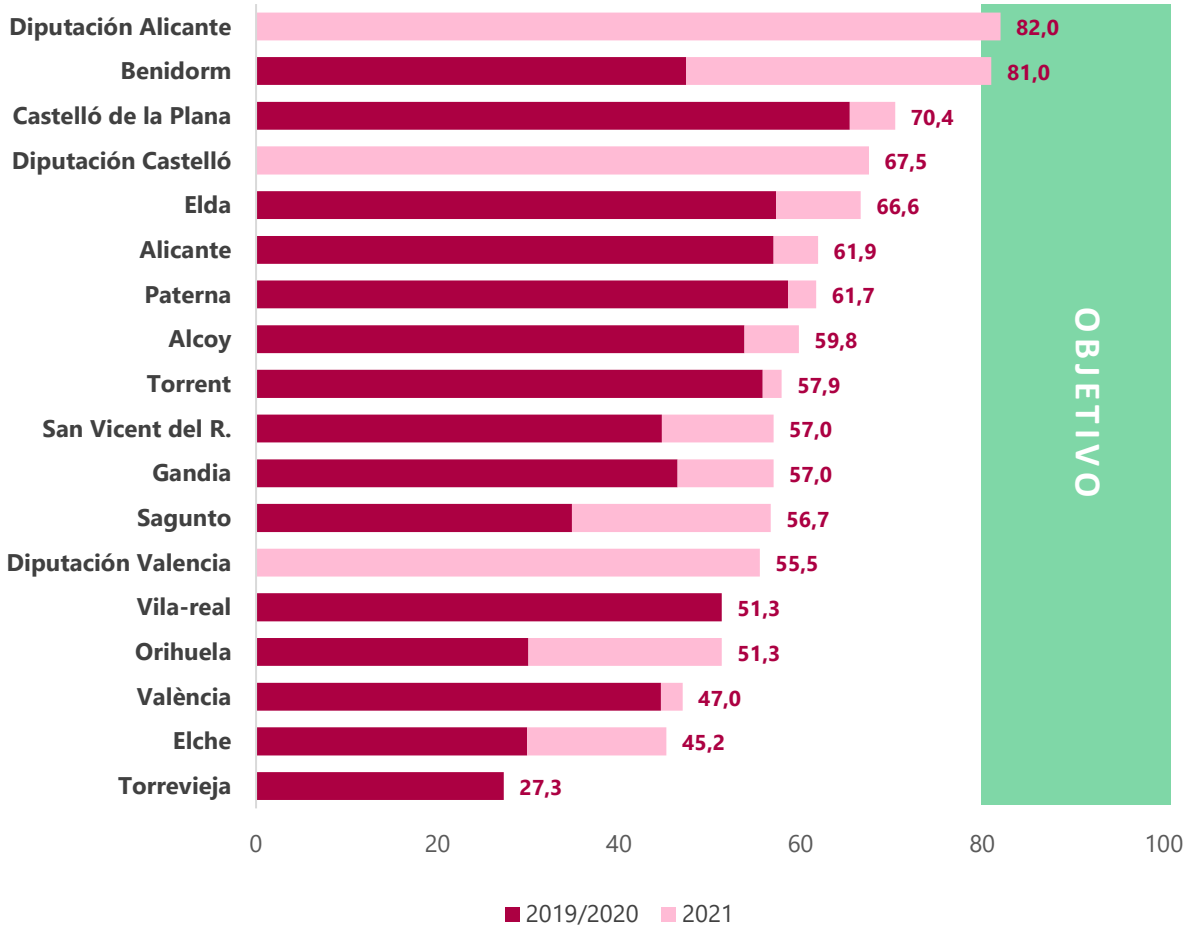
En consecuencia, las entidades deben disponer de un procedimiento formalmente aprobado que describa las acciones llevadas a cabo para la gestión de sus usuarios

administradores, que cumpla con una serie de buenas prácticas para garantizar la efectividad del control. Entre estas cabe destacar: asignación de usuarios nominativos; permitir la trazabilidad de las acciones; cambio de cuentas y contraseñas por defecto; y una política robusta de contraseñas que se aplique de manera homogénea a todos los dispositivos y sistemas que componen el sistema de información.

Situación del índice de madurez del control

El siguiente gráfico muestra los resultados obtenidos. Se aprecia que casi todos los ayuntamientos, exceptuando dos de ellos, han realizado acciones que mejoran los índices de madurez obtenidos en la anterior auditoría. Sin embargo, la mejora no es suficiente para alcanzar el nivel que se exige en el ENS. Únicamente un ayuntamiento y una diputación alcanzan el nivel exigido por el ENS.

Gráfico 12. Índice de madurez del CBCS 4 por entidad



El índice de madurez medio ha sido del 56,8% en los ayuntamientos y del 68,3% en las diputaciones.

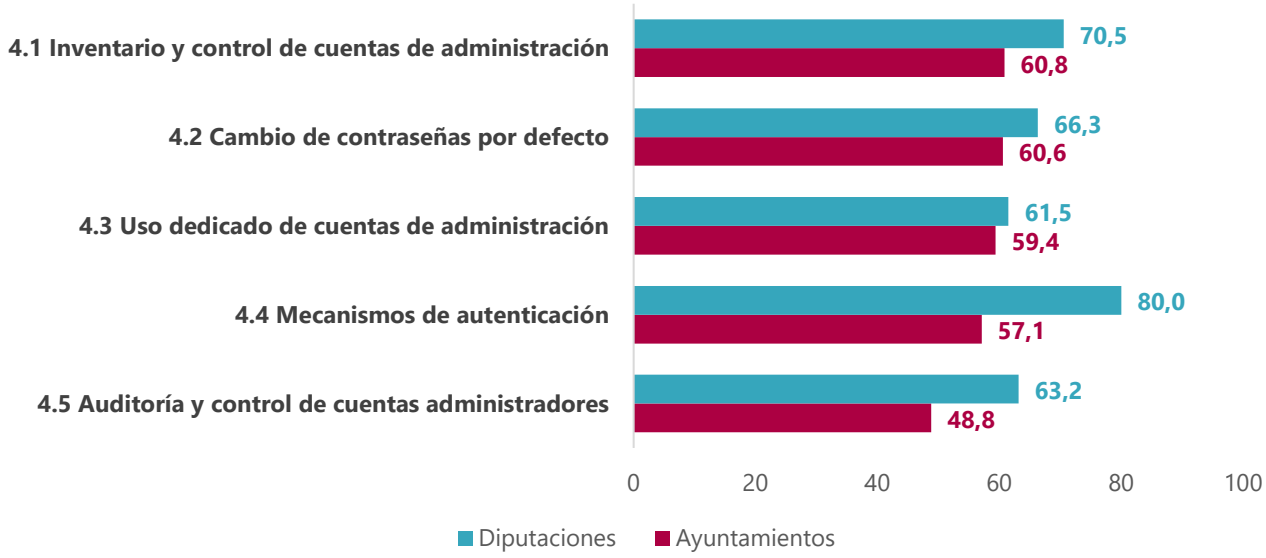
Situación de los subcontroles revisados

El CBCS 4 consta de cinco subcontroles:

- CBCS 4.1: Inventario y control de cuentas de administración
- CBCS 4.2: Cambio de contraseñas por defecto
- CBCS 4.3: Uso dedicado de cuentas de administración
- CBCS 4.4: Mecanismos de autenticación
- CBCS 4.5: Auditoría y control de cuentas administrativas

Si analizamos el índice de madurez medio de cada uno de los subcontroles del CBCS 4 se observa que, en general, las entidades no tienen implantadas medidas que supongan un control efectivo sobre sus usuarios administradores. No obstante, se observan mejoras que indican que, en general, las entidades son conscientes de sus carencias y realizan acciones encaminadas a establecer controles más eficaces.

Gráfico 13. Índice medio de madurez de los subcontroles del CBCS 4 en 2021



Las entidades deben aprobar procedimientos que describan la gestión de los usuarios administradores e incluyan las directrices que establece la normativa, como la eliminación de todos los usuarios no nominativos, la segregación de funciones en función de la tarea a desempeñar, la política de autenticación, el registro de acciones de estos usuarios, etc.

5. CONFIGURACIONES SEGURAS DEL "SOFTWARE" Y "HARDWARE" (CBCS 5)

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.

Por qué es importante este control básico de ciberseguridad

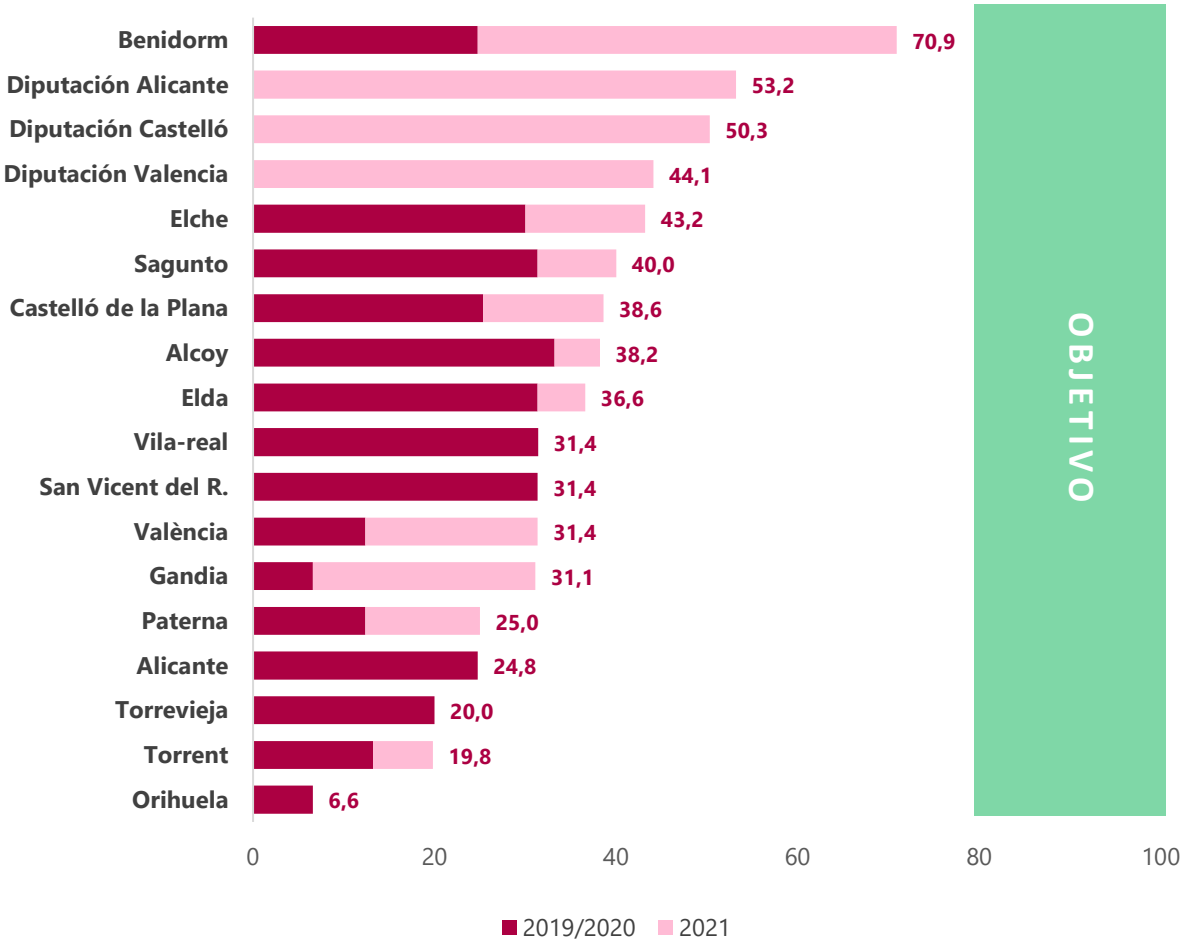
Por defecto, la mayoría de los sistemas están configurados para facilitar su uso y no necesariamente pensando en la seguridad. Tal como lo entregan los fabricantes y vendedores, cuando se recibe un equipo es habitual encontrarse con controles poco robustos, servicios y puertos abiertos, cuentas o contraseñas predeterminadas, protocolos antiguos, *software* preinstalado innecesario. Todos estos aspectos son vulnerables en su estado predeterminado.

Para implantar de manera efectiva este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad. El desarrollo de opciones de configuración con buenas propiedades de seguridad no es una tarea sencilla y va más allá de la capacidad de los usuarios individuales, requiriendo análisis a veces complejos y costosos para tomar buenas decisiones. Por esta razón, es altamente recomendable el seguimiento y aplicación de buenas prácticas que algunos organismos publican en materia de seguridad, aplicables a dispositivos y sistemas.

Incluso si se desarrolla e instala una configuración inicial fuerte, debe ser revisada y actualizada continuamente para evitar el deterioro de la seguridad, en particular, cuando el *software* se actualiza o parchea se divulgan las nuevas vulnerabilidades de la seguridad, o las configuraciones se "ajustan" para permitir la instalación de nuevos programas o para dar soporte a nuevos requerimientos operacionales. Si no se revisa y actualiza de forma continua, los atacantes encontrarán oportunidades para explotar tanto el *software* como los servicios accesibles a la red.

Situación del índice de madurez del control

Gráfico 14. Índice de madurez del CBCS 5 por entidad



Este gráfico muestra la situación de las entidades auditadas. Se observa que ninguna de ellas alcanza el 80% exigido por el ENS para sistemas de categoría media. No obstante, existen entidades que, conscientes de la inefectividad del control, han dedicado esfuerzos y medios para mejorar.

En la mayoría de las entidades este índice es preocupantemente bajo, por lo que deben destinar esfuerzos para mejorarlo.

El índice de madurez medio ha sido del 32,6% en los ayuntamientos y del 49,2% en las diputaciones.

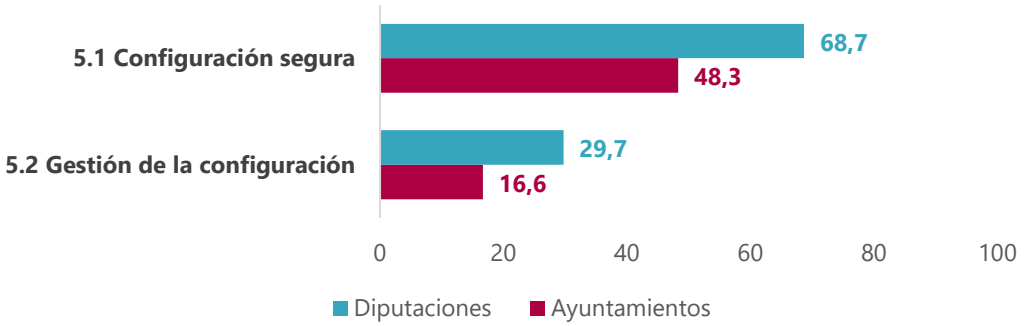
Situación de los subcontroles revisados

El CBCS 5 consta de dos subcontroles:

- CBCS 5.1: Configuración segura
- CBCS 5.2: Gestión de la configuración

Los resultados obtenidos para estos dos subcontroles son:

Gráfico 15. Índice medio de madurez de los subcontroles del CBCS 5 en 2021



Las entidades deben aprobar procedimientos que consideren la seguridad por defecto y el criterio de mínima funcionalidad, siguiendo las recomendaciones de los fabricantes en materia de seguridad o las recomendaciones de los organismos de referencia, tales como las guías STIC de las series 400, 500 y 600 del CCN.

Además, se ha aconsejado en todos los informes desarrollar procedimientos de gestión continuada de la configuración de los sistemas, particularmente de los sistemas críticos. Estos deben 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.

6. REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS (CBCS 6)

Objetivo del control

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

Por qué es importante este control básico de ciberseguridad

Implica que todos los sistemas y aplicaciones deberían tener habilitadas las trazas de auditoría, incluyendo respuestas a desde dónde, quién y cuándo se ha realizado una determinada acción, así como tener definidas actuaciones de alerta.

En organizaciones con presupuesto y personal suficiente se suele disponer de un SIEM (*security information and event management*), sistema que, además de centralizar registros

de auditoría y disponer en tiempo real de alertas de seguridad, es capaz de relacionar eventos de seguridad de los distintos dispositivos.

En la actualidad, todos los sistemas operativos, servicios y dispositivos de red ofrecen capacidades de *log*, pero tales registros deben ser correctamente configurados para almacenar toda la información disponible y permitir su análisis posterior. Un ejemplo son los servidores, que deben estar configurados para crear registros de control de acceso cuando un usuario intenta acceder a recursos sin los privilegios adecuados. Para evaluar si tal registro está operativo, la organización debe escanear periódicamente sus *logs* y compararlos con el inventario de activos instalado como parte de los CBCS 1 y 2 para asegurar que los elementos críticos de la red estén generando periódicamente *logs*.

Los programas analíticos para revisar registros pueden ser valiosos, pero los medios empleados para analizar los *logs* de auditoría son bastante diversos, incluso un rápido examen realizado por una persona es importante para esa finalidad. Las herramientas de correlación pueden hacer mucho más útiles los registros de auditoría para una posterior inspección, y pueden ser de gran ayuda en la identificación de ataques sutiles. Sin embargo, estas herramientas no son un reemplazo de los administradores de sistemas y personal experimentado de seguridad de la información.

Deficiencias en los registros de seguridad y en su análisis permiten a los atacantes ocultar su ubicación, el *software* malicioso introducido y las actividades ilícitas que realizan en las máquinas víctimas. Incluso si los entes atacados saben que sus sistemas han sido comprometidos, sin registros de *logs* completos y protegidos permanecen ciegos a los detalles del ataque y a las posteriores acciones de los atacantes.

Sin unos *logs* de auditoría sólidos, un ataque puede pasar desapercibido por tiempo indefinido y los daños infligidos pueden ser irreversibles. Debido a deficientes o inexistentes procesos de análisis de registros, a veces los atacantes controlan las máquinas víctima durante meses o años sin que nadie se percate en la organización de destino, a pesar de que la evidencia del ataque consta en dichos registros no examinados.

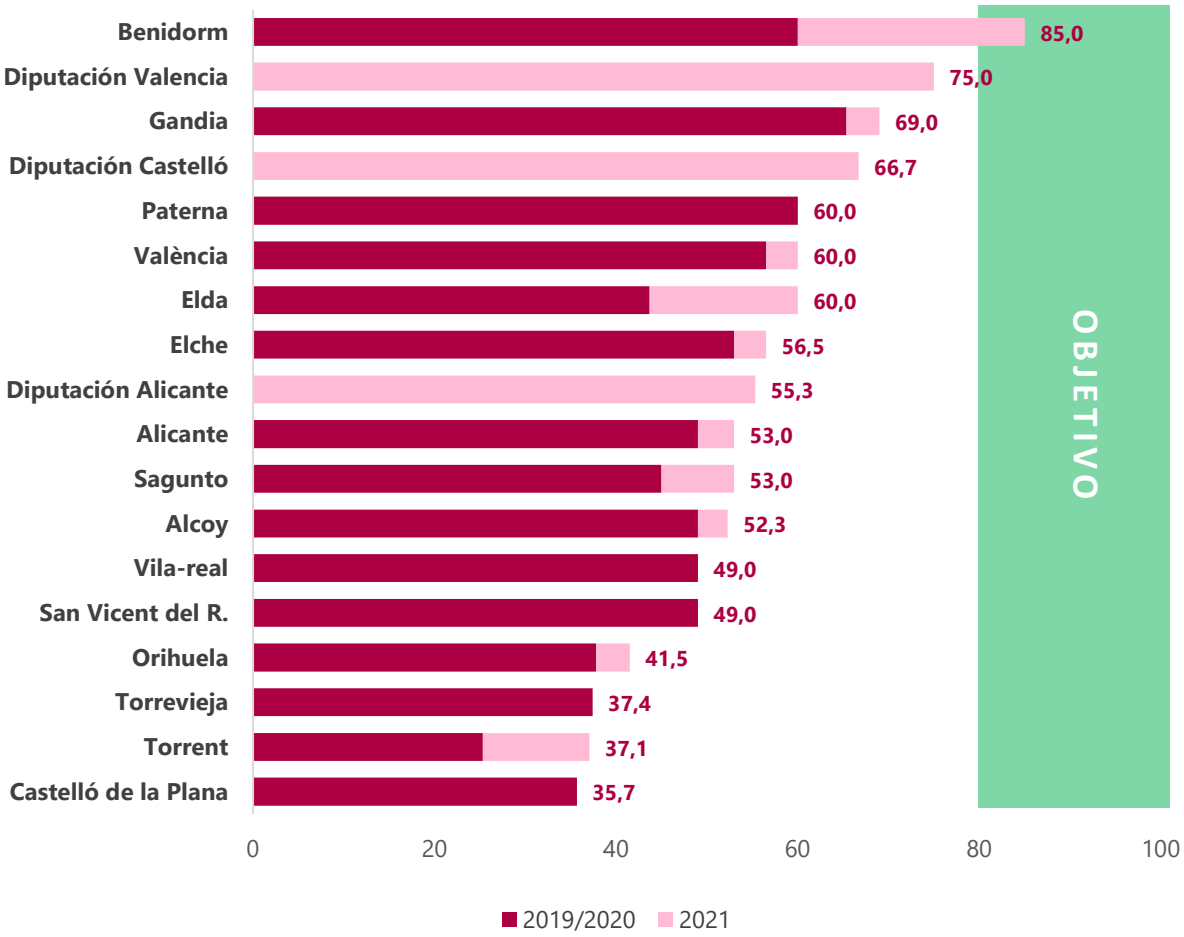
Por todo lo expuesto, las organizaciones deben incluir entre sus procedimientos de seguridad la gestión de los registros de auditoría, en los que se definan los sistemas afectados, los tipos de eventos a registrar, el periodo de retención, los responsables y los mecanismos de protección aplicados a estos.

Adicionalmente, y dado el amplio volumen de registros generados por los distintos dispositivos de un sistema de información actual, es conveniente el uso de herramientas para la centralización o correlación de eventos para gestionarlos de forma eficiente.

Situación del índice de madurez del control

El gráfico muestra el índice de madurez del CBCS 6 que los ayuntamientos obtuvieron en las auditorías precedentes y la mejora que han experimentado hasta el 31 de diciembre del 2021, e incorpora la revisión realizada a las tres diputaciones.

Gráfico 16. Índice de madurez del CBCS 6 por entidad



En general, los controles implantados por las entidades son insuficientes para alcanzar el nivel que se exige en el ENS, siendo el índice de madurez medio del 53,2% en los ayuntamientos y del 65,6% en las diputaciones.

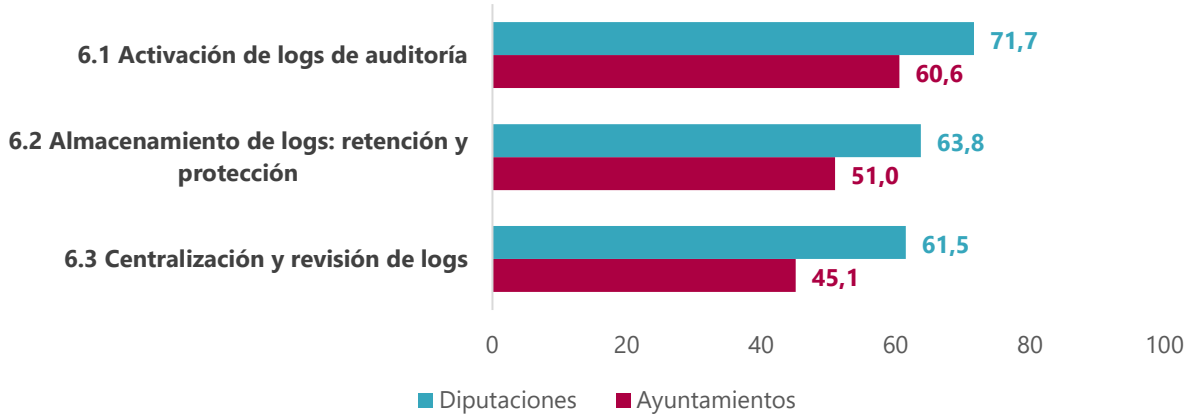
Situación de los subcontroles revisados

El CBCS 6 consta de tres subcontroles:

- CBCS 6.1: Activación de *logs* de auditoría
- CBCS 6.2: Almacenamiento de *logs*: retención y protección
- CBCS 6.3: Centralización y revisión de *logs*

Los índices de madurez medios para cada uno de los subcontroles se muestran en el siguiente gráfico.

Gráfico 17. Índice medio de madurez de los subcontroles del CBCS 6 en 2021



Las entidades deben aprobar formalmente un procedimiento para el tratamiento de *logs* de auditoría de actividad de los usuarios, que especifique los sistemas afectados, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro, proceso de revisión de los *logs*. Para la revisión de *logs* es aconsejable centralizarlos en sistemas dedicados a tal efecto.

7. COPIA DE SEGURIDAD DE DATOS Y SISTEMAS (CBCS 7)

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.

Por qué es importante este control básico de ciberseguridad

Cuando los atacantes comprometen los sistemas, a menudo realizan cambios significativos de las configuraciones y el *software*. En ocasiones, los atacantes también realizan alteraciones sutiles de los datos almacenados en los sistemas comprometidos, lo que puede poner en peligro la eficacia de la organización con información contaminada. Otras veces simplemente destruyen o invalidan todos o parte de los datos y *software* de una entidad.

Cuando se descubre a los atacantes, puede ser extremadamente difícil para las organizaciones eliminar todos los aspectos de la presencia del atacante en los sistemas. Los daños de ciberataques pueden ser mitigados si se dispone de copia de seguridad de los datos afectados.

Los ciberdelincuentes han evolucionado con el paso del tiempo, mejorando los métodos de cifrado o el acceso a los recursos del sistema. Este tipo de ataques "mejorados" ha tenido efectos devastadores en las últimas oleadas de *ransomware*. Por ello, contar con una copia de seguridad no accesible a nivel de red, es decir, que se encuentre aislada o desconectada, es una buena medida de protección adicional a las de cifrado y seguridad física.

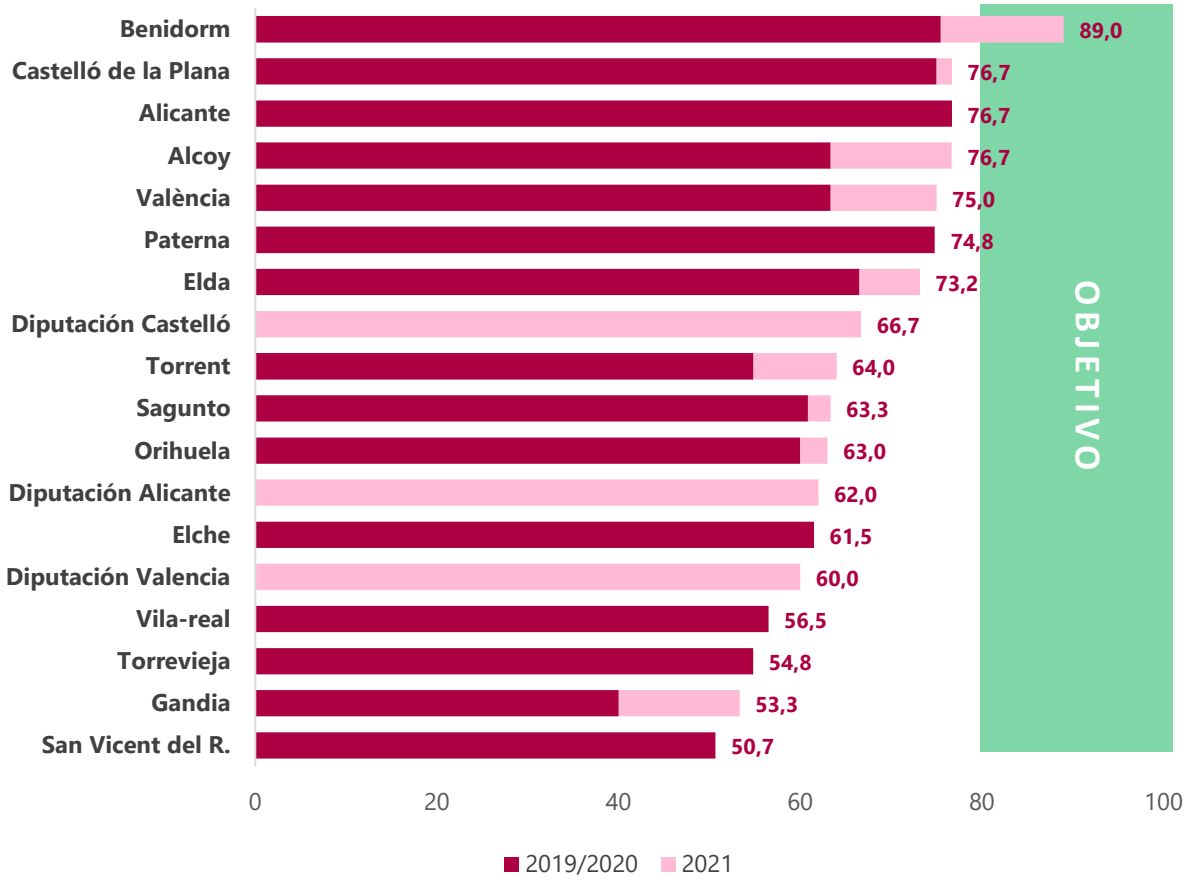
Las copias de seguridad deben ser verificadas. Para ello, periódicamente, un equipo de pruebas debe evaluar una muestra aleatoria de las copias de seguridad realizadas planificando restauraciones en entornos de pruebas. Las pruebas de restauración de sistemas deben incluir la verificación no solo del proceso de recuperación, sino también de su contenido, es decir, que el sistema operativo, la aplicación y los datos de la copia de seguridad estén intactos y sean funcionales.

Con la evolución de la ciberdelincuencia y los métodos de ataque cada vez más sofisticados, es necesario que las organizaciones estén preparadas no solo para defenderse, sino también para reponerse ante ataques exitosos, es un elemento clave de la ciberresiliencia de una entidad.

Las organizaciones deben decidir qué información proteger de acuerdo con los responsables funcionales de los sistemas, y deben documentar el proceso de copias de seguridad en un procedimiento formalmente aprobado que defina su ubicación, el periodo de retención, el tipo de copias y la periodicidad. Adicionalmente, las copias deben de ser provistas de las medidas de seguridad necesarias para su protección y deben realizarse pruebas de restauración planificadas, que garanticen que los sistemas pueden ser restaurados de manera efectiva.

Situación del índice de madurez del control

Gráfico 18. Índice de madurez del CBCS 7 por entidad



De acuerdo con los resultados obtenidos en las auditorías, el control sobre las copias es uno de los controles cuyo índice de madurez es, en promedio, más alto, aunque sin alcanzar el objetivo. Se observa que seis entidades tienen un índice cercano al objetivo, y únicamente una lo alcanza. Los índices de madurez de las demás entidades, aunque no son particularmente bajos, no alcanzan el nivel exigido.

El índice de madurez medio ha sido del 67,3% en los ayuntamientos y del 62,9% en las diputaciones.

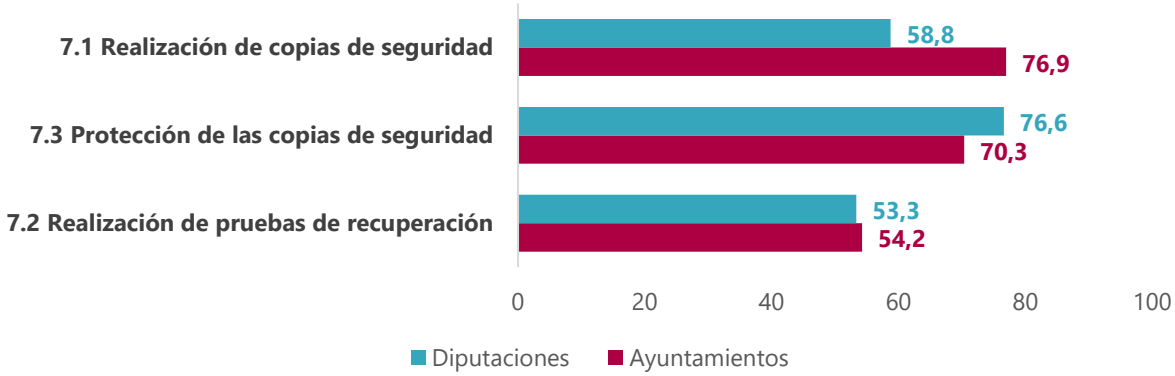
Situación de los subcontroles revisados

El CBCS 7 consta de tres subcontroles:

- CBCS 7.1: Realización de copias de seguridad
- CBCS 7.2: Realización de pruebas de recuperación
- CBCS 7.3: Protección de las copias de seguridad

Si analizamos los resultados por subcontrol, se observa que:

Gráfico 19. Índice medio de madurez de los subcontroles del CBCS 7 en 2021



Las entidades deben aprobar formalmente un procedimiento para la gestión de copias de seguridad de datos y sistemas que defina, como mínimo, los datos y sistemas afectados, la periodicidad de las copias, ubicaciones, responsables, las pruebas de restauración a realizar y los requisitos de protección de las copias.

8. CUMPLIMIENTO NORMATIVO (CBCS 8)

Objetivo del control

Asegurar el cumplimiento de la normativa básica en materia de seguridad de la información.

Por qué es importante este control básico de ciberseguridad

Con la inclusión de este control se pretende asegurar que se cumplen diversas normas relacionadas con la seguridad de la información que consideramos relevantes para mantener un adecuado control sobre la seguridad de los sistemas de información y las comunicaciones y la privacidad de la información.

Consideramos muy importante dar el debido cumplimiento a lo dispuesto por el Esquema Nacional de Seguridad, ya que su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. El ENS establece una serie de medidas de seguridad que deben implantar las entidades públicas con carácter obligatorio con la finalidad de fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Por otra parte, las administraciones públicas, en el desarrollo de sus actividades, actúan como responsables de tratar datos personales y deben garantizar el derecho de las personas a la protección de sus datos. Por tanto, deben adoptar las medidas necesarias para garantizar el nivel de seguridad requerido por la normativa vigente en materia de protección de datos personales.

Finalmente consideramos que, dentro del ámbito de la gestión económica, es importante disponer del informe de auditoría de sistemas anual del Registro Contable de Facturas en cumplimiento de lo que exige la Ley 25/2013, de 27 de diciembre, de Impulso de la Factura Electrónica y Creación del Registro Contable de Facturas, ya que uno de los objetivos de dichas auditorías es la "revisión de la gestión de la seguridad en aspectos relacionados con la confidencialidad, autenticidad, integridad, trazabilidad y disponibilidad de los datos y servicios de gestión".

Situación del índice de madurez del control

El gráfico 5, "Índice de madurez del cumplimiento de la normativa (CBCS 8)", muestra, al inicio de este informe, que, aunque la mayoría de entidades se encuentran realizando acciones encaminadas a subsanar los incumplimientos en esta materia, el grado de cumplimiento de la normativa relativa a la seguridad de la información es, en general, deficiente, existiendo incumplimientos significativos generalizados.

Únicamente uno de los ayuntamientos alcanza el nivel de madurez exigido por el ENS. Seis de los catorce restantes alcanzan un nivel de cumplimiento cercano al que exige la normativa y existen cinco ayuntamientos que no han mejorado el índice de cumplimiento desde nuestro trabajo de auditoría de 2019.

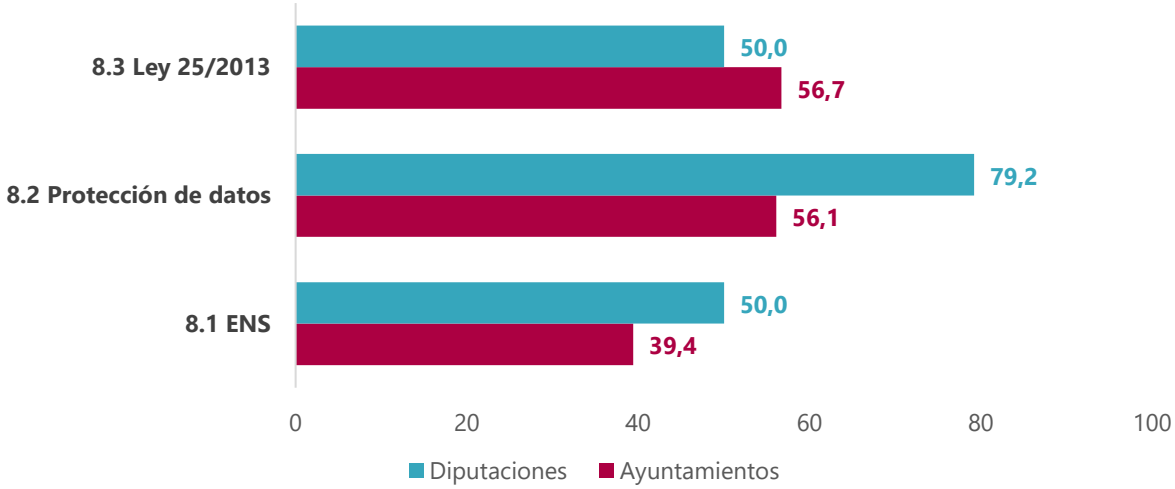
Subcontroles revisados e indicadores de la situación del control

El CBCS 8 consta de tres subcontroles:

- CBCS 8.1: Esquema Nacional de Seguridad
- CBCS 8.2: LOPD/RGPD
- CBCS 8.3: Ley 25/2013, de Impulso de la Factura Electrónica

El siguiente gráfico muestra el índice medio de madurez de los tres aspectos normativos evaluados (cumplimiento del ENS, materia de protección de datos de carácter personal y factura electrónica).

Gráfico 20. Índice medio de madurez por materia revisada

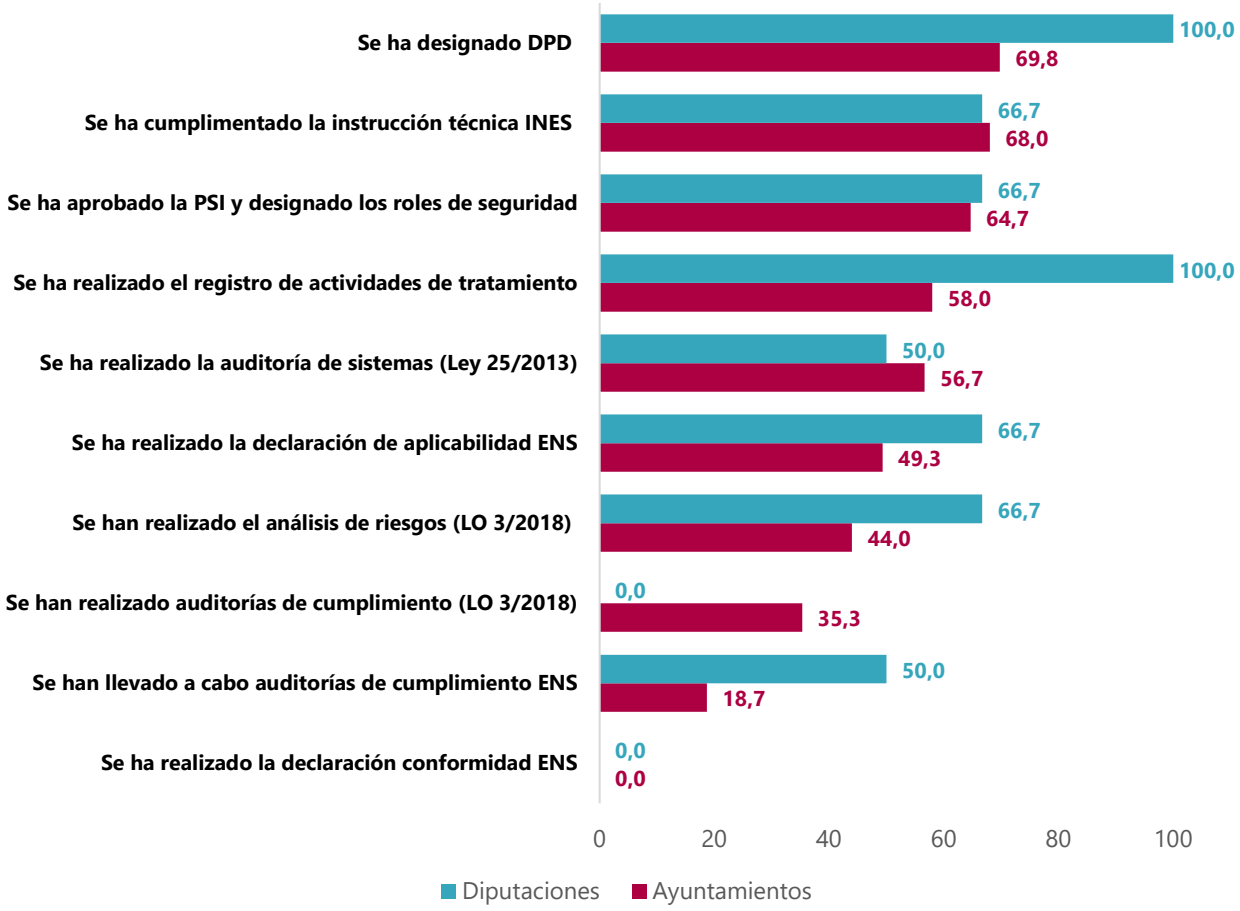


El gráfico 21 muestra el índice de madurez medio obtenido por las entidades para cada uno de los aspectos revisados en este CBCS. Dichos aspectos son:

- Respecto al cumplimiento del ENS:
  - Se ha aprobado la PSI y designado los roles de seguridad.
  - Se ha cumplimentado la instrucción técnica INES.
  - Se ha realizado la declaración de aplicabilidad.
  - Se han llevado a cabo auditorías de cumplimiento.
  - Se ha realizado la declaración de conformidad y se han publicado los distintivos en sede.
- Respecto al cumplimiento de la normativa en materia de protección de datos de carácter personal (LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y RGPD):
  - Se ha designado DPD.
  - Se ha realizado el registro de actividades de tratamiento de datos de carácter personal.
  - Se ha llevado a cabo el análisis de riesgos de los tratamientos de datos personales.
  - Se han llevado a cabo auditorías de cumplimiento en dicha materia.
- Respecto al cumplimiento de la Ley 25/2013, de 27 de diciembre, de Impulso de la Factura Electrónica y Creación del Registro Contable de Facturas:

- Se ha llevado a cabo la auditoría de sistemas exigida por la citada ley.

Gráfico 21. Índice medio de madurez de cada uno de los aspectos evaluados en el CBCS8

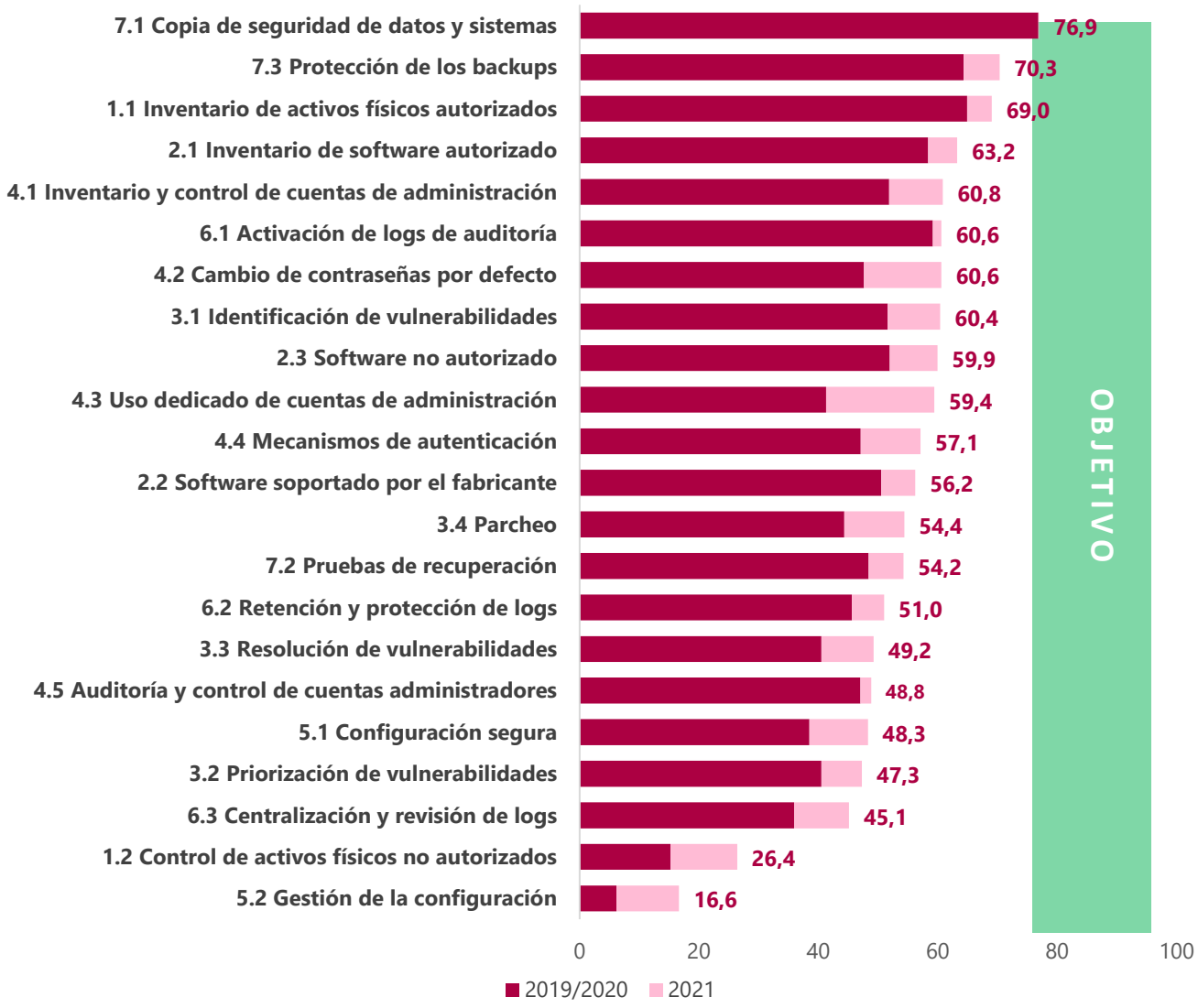


Se observa que la mayoría de entidades han designado un DPD o emitido el informe INES. Sin embargo, ninguna de las entidades cumple con el ENS ni ha publicado en sede los distintivos correspondientes.

9. EVOLUCIÓN DEL ÍNDICE DE MADUREZ DE LOS SUBCONTROLES EN LOS AYUNTAMIENTOS AUDITADOS

El gráfico 22 representa el conjunto de los subcontroles analizados ordenados de mayor a menor índice de madurez y su evolución desde la anterior auditoría.

Gráfico 22. Índice de madurez medio por subcontrol



De los resultados observados en la gráfica extraemos las siguientes reflexiones:

- Ninguno de los subcontroles alcanza, en promedio, el nivel exigido por el ENS.
- Los subcontroles relacionados con las copias de seguridad y los inventarios, tanto *hardware* como *software*, siguen siendo los controles con mayor índice de madurez obtenido.
- Existen controles cuyo índice de mejora se ha visto incrementado en mayor medida que en otros, como en los subcontroles relacionados con la gestión de perfiles de administración sobre los sistemas, contraseñas, dispositivos no autorizados o configuraciones por defecto.

- Existen subcontroles cuyo índice de madurez sigue siendo muy deficiente, aunque este se haya incrementado desde nuestro anterior trabajo de revisión. Entre estos subcontroles está la gestión de las configuraciones seguras, el control de activos físicos no autorizados o el uso de herramientas para la revisión de registros de auditoría.

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

ENS: Esquema Nacional de Seguridad

INES: Informe Nacional del Estado de la Seguridad

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

PSI: Política de seguridad de la información

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de gestión de seguridad de la información

SIC: Sistemas de información y comunicaciones

Alta dirección: A los efectos de este trabajo, nos referimos a los órganos superiores de la entidad (en particular, el presidente 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, y a los funcionarios directores del departamento TIC y los jefes de área o servicio.

EDR[13]: Un sistema EDR, acrónimo 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 corporativa: Es el sistema por el cual se dirigen y controlan las organizaciones (UNE-ISO/IEC 38500).

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*.

Gobernanza sobre las TI: Es un componente clave de la gobernanza corporativa en general. Es el sistema mediante el que se dirige y controla el uso actual y futuro de las tecnologías de la información y las comunicaciones. Implica evaluar y dirigir la utilización de las TI para dar soporte a la organización y la monitorización de ese uso para lograr la consecución de los planes. Incluye la estrategia y políticas para la utilización de las TI en la organización (UNE-ISO/IEC 38500).

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

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

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 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.

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 19 de abril de 2023, 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 de síntesis CBCS 2021_cas - SEFYCU 4095156

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 93QH EV2N J42D KNUU

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 - 09/05/2023 10:02 VICENT CUCARELLA TORMO