SINDICATURA DE COMPTES

Auditoría de los controles básicos de ciberseguridad de los mayores ayuntamientos de la Comunitat Valenciana

Los sistemas de información están en riesgo frente a las amenazas de ciberseguridad

Ejercicios 2019 y 2020

AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DE LOS MAYORES AYUNTAMIENTOS DE LA COMUNITAT VALENCIANA

Los sistemas de información están en riesgo frente a las amenazas de ciberseguridad

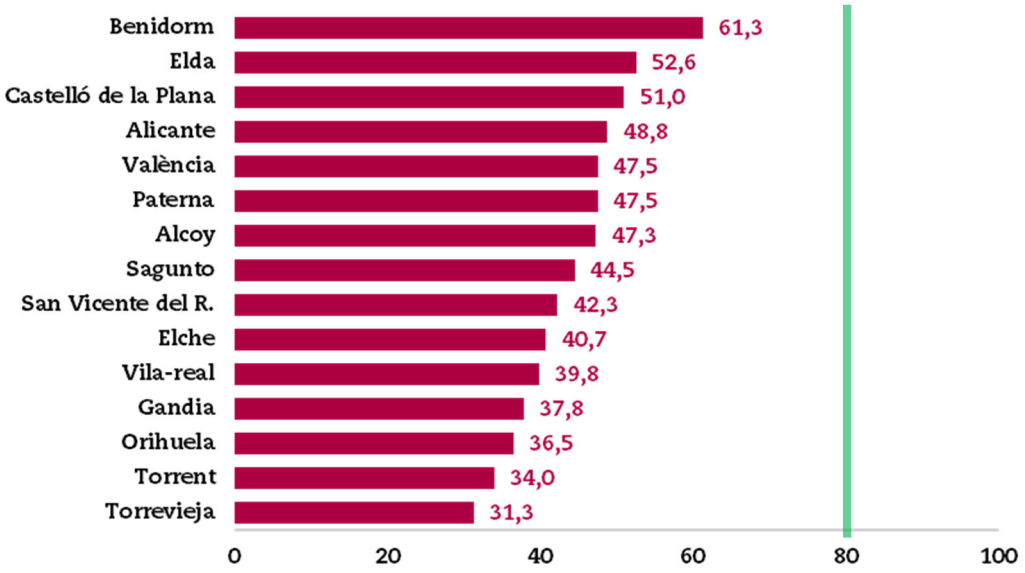
Ejercicios 2019 y 2020

RESUMEN

Los sistemas de información analizados están en riesgo frente a las amenazas de ciberseguridad

Ninguno de los ayuntamientos auditados alcanza el índice de madurez de los controles básicos de ciberseguridad del 80% requerido por el ENS (es decir, solo se puede considerar haber obtenido un "aprobado" en ciberseguridad alcanzando la línea verde del gráfico).

Bajo índice de madurez de los CBCS



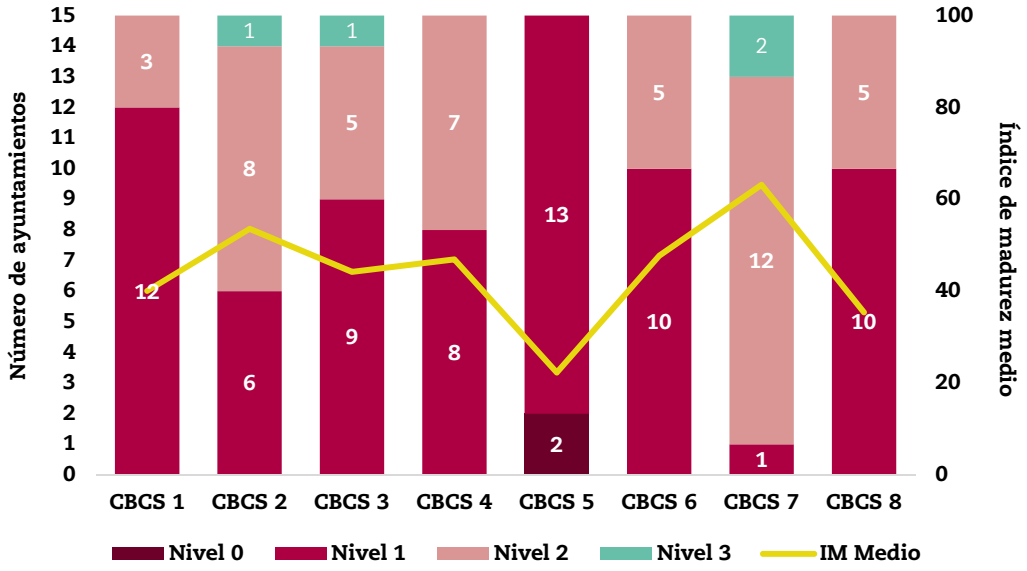
En general, el nivel de cumplimiento con la normativa relacionada con la seguridad de la información es bastante insatisfactorio

La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto que existen incumplimientos generalizados de esa normativa, siendo el índice medio de cumplimiento del CBCS 8 del 44,2%. Los máximos órganos de dirección de los ayuntamientos tienen la responsabilidad de garantizar un nivel adecuado de cumplimiento de las normas legales y deben impulsar las medidas necesarias para subsanar la deficiente situación existente.

Todos los ayuntamientos deben adoptar medidas para mejorar su ciberseguridad

De un total de 120 controles básicos revisados en los quince ayuntamientos, solo cuatro controles alcanzan el nivel de madurez N3 establecido como objetivo en el ENS. En el siguiente gráfico se muestra de forma resumida los niveles de madurez observados para los ocho controles básicos en el conjunto de los quince ayuntamientos, y el índice de madurez (IM) medio de cada CBCS observado en ellos.

Situación de los niveles de madurez en los quince ayuntamientos auditados



Mantener una adecuada ciberhigiene y un sólido sistema de protección frente a las ciberamenazas es más necesario que nunca

La situación provocada por la epidemia de COVID-19 ha mostrado con absoluta claridad la total dependencia de los sistemas de información y las comunicaciones que existe actualmente en la gestión pública, lo que hace que las administraciones públicas sean más vulnerables que nunca frente a los ciberataques y ha puesto de relieve que mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos es de vital importancia.

No existe coste cero en materia de seguridad de la información

Es necesario un mayor compromiso y concienciación de los órganos de gobierno de los ayuntamientos con la seguridad de los sistemas de información y las comunicaciones, lo que inevitablemente conlleva una mayor inversión económica y en recursos humanos cualificados.

En la fase final de discusión de los borradores de informe con los distintos responsables, nos han manifestado, en general, su voluntad de subsanar las deficiencias de control observadas. En algunos casos las han subsanado antes de la emisión del informe. En el Programa Anual de Actuación de 2020 está expresamente previsto realizar un informe de "Seguimiento de las 11 auditorías de los controles básicos de ciberseguridad cuyo trabajo de campo se ha realizado en 2019 (una vez transcurrido un año desde su finalización)". Razonablemente este seguimiento tendrá continuidad con los cuatro ayuntamientos auditados en 2020.

NOTA

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

ÍNDICE **Página**

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS:	Controles básicos de ciberseguridad
CCN:	Centro Criptológico Nacional
CGTI:	Controles generales de tecnologías de la información
DPD:	Delegado de protección de datos
ENISA:	European Union Agency for Cybersecurity
ENS:	Esquema Nacional de Seguridad
INES:	Informe Nacional del Estado de la Seguridad
LOPD:	Ley Orgánica de Protección de Datos de Carácter Personal
RGPD:	Reglamento General de Protección de Datos
SGSI:	Sistema de Gestión de Seguridad de la Información
SIC:	Sistemas de información y comunicaciones
SIEM:	Sistema de gestión de información y eventos de seguridad

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.

Declaración de aplicabilidad: En el ámbito del ENS es el documento en el que se formaliza la relación de medidas de seguridad que resultan de aplicación a un sistema de información, conforme a su categoría, y que se encuentran recogidas en el anexo 2 del Real Decreto 3/2010.

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

Política de seguridad de la información: es un documento de alto nivel que define lo que significa "seguridad de la información" en una organización de acuerdo con el artículo 11 del Real Decreto 3/2010 y articula la gestión continuada de la seguridad. Debe ser aprobada por la junta de gobierno del ayuntamiento. 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.

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 y 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*, se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las administraciones públicas, razón por la que los auditores públicos deben prestar cada vez más atención a dichas cuestiones. La Sindicatura no es indiferente ante esta problemática y en 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**.

Considerando que las entidades locales no son ajenas a la problemática planteada por la ciberseguridad, y su cercanía a los ciudadanos, el Consell de la Sindicatura de Comptes acordó incluir en los programas anuales de actuación de 2019 y 2020 la realización de un informe sobre los controles básicos de ciberseguridad (CBCS) de los quince mayores ayuntamientos de la Comunitat Valenciana para evaluar su preparación frente a la actual situación de crecientes ciberamenazas.

Tras publicar los quince informes individuales correspondientes a cada ayuntamiento, la Sindicatura ha considerado conveniente realizar el trabajo de compilación incluido en el presente documento. De este modo se ofrece una visión de conjunto en la que se destacan las principales observaciones realizadas.

El entorno actual de administración electrónica y los nuevos 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 todas las entidades públicas, y establecen que la tramitación electrónica debe

constituir la actuación habitual de las Administraciones, 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, de aplicación obligatoria para todo el sector público.

La necesidad de una adecuada ciberhigiene

Los actuales sistemas de información son más complejos y están más interconectados que nunca, pero una mayor interconexión origina mayores riesgos de ciberseguridad, ocasiona una mayor probabilidad de que se produzca una perturbación significativa en los sistemas de información de las entidades locales debida a un ciberataque y, en consecuencia, una interrupción en los servicios prestados a los ciudadanos. Por esta razón, es imperativo que los responsables de los entes públicos gestionen los riesgos asociados con el funcionamiento y uso de sistemas de información que utilizan para desarrollar y prestar los servicios públicos.

En el escenario general descrito, la realidad de nuestro entorno cercano y del resto de la sociedad española y mundial en el momento de elaborar este informe es la de una crisis sanitaria y socioeconómica sin precedentes provocada por la epidemia de COVID-19. Entre otras muchas cuestiones, esta crisis ha puesto de manifiesto que las administraciones públicas han sido capaces de mantener gran parte de su actividad confiando en el buen funcionamiento y la eficacia de los sistemas de información y comunicaciones (SIC). Obligados por el confinamiento decretado por el Gobierno de la nación para hacer frente a la epidemia, todas las administraciones han recurrido al **trabajo en remoto**, en sus distintas modalidades técnicas, para mantener su actividad en niveles razonables. Este importante salto cualitativo, impensable en condiciones normales, ha sido posible gracias a unos SIC ampliamente desarrollados.

Al mismo tiempo, esta circunstancia ha mostrado con absoluta claridad la **total dependencia de los SIC** que existe en la gestión pública, lo que hace

que nuestras administraciones sean más **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 tiene como contrapartida de su eficiencia un fuerte aumento de la superficie de exposición frente a las ciberamenazas, al que las entidades públicas tienen que hacer frente con las dificultades propias de un periodo de crisis.

En estos entornos actuales adquiere todo su sentido el concepto de ciberresilencia, que puede entenderse como la capacidad de una entidad para evitar o resistir y recuperarse de un ciberataque en un tiempo razonable para continuar prestando sus servicios.

Si el gran número de ciberataques exitosos que se produjo en 2019 en nuestro país se hubiera producido durante la actual crisis, las consecuencias hubieran sido nefastas en aquellos entes atacados, ya que no hubieran podido desarrollar ni actividad presencial ni de forma remota. **La ciberseguridad es hoy un elemento esencial en los SIC**.

2. OBJETIVOS, ALCANCE Y METODOLOGÍA DE LA AUDITORÍA

Objetivos

El objetivo general de la auditoría ha sido proporcionar una evaluación sobre el grado de ciberseguridad de los mayores ayuntamientos de la Comunitat Valenciana, sobre el cumplimiento de la normativa en materia de seguridad de los sistemas de información y efectuar recomendaciones para la adopción de medidas de ciberhigiene.

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 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 y sus respectivos índices de cumplimiento.

- La identificación de incumplimientos significativos de la normativa sobre seguridad de la información.

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 ayuntamientos 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 objetivos en las buenas prácticas y en el ENS.

Ámbito subjetivo

Se han auditado los quince municipios de mayor población (superior a los 50.000 habitantes) de la Comunitat Valenciana. En el cuadro 1 pueden verse los entes auditados con los datos de población y las obligaciones reconocidas netas (ORN) de 2018, en millones de euros.

Cuadro 1. Ayuntamientos auditados

Ayuntamiento	Población 2018	ORN 2018
València	791.413	1.046,1
Alicante	331.577	287,2
Elche	230.625	187,4
Castelló de la Plana	170.888	172,9
Torrevieja	82.599	64,8
Torrent	81.245	52,7
Orihuela	76.778	72,1
Gandia	73.829	92,9
Paterna	69.156	65,4
Benidorm	67.558	94,7
Sagunto	65.669	64,2
Alcoy	58.977	56,6
San Vicente del Raspeig	57.785	36,9
Elda	52.404	35,6
Vila-real	50.577	53,8
Ayuntamientos auditados	**2.261.080**	**2.383,3**
Total ayuntamientos CV	**4.963.703**	**4.917,0**
Cobertura de la auditoría	**45,6%**	**48,5%**

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 es información consolidada obtenida de la liquidación de cada entidad local.

Se han aprobado quince 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 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*, punto de acceso a red *wifi*, etc.)
- elementos de seguridad (*firewall, IPS, proxy* de correo, *proxy* de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.)

Ámbito temporal

El ámbito temporal analizado ha abarcado el segundo semestre de 2019 y el primer semestre de 2020. En el apartado 9 del apéndice se especifica cuándo se dieron por finalizados los trabajos en los distintos ayuntamientos y a qué fecha se refieren por tanto los indicadores y las situaciones descritas en este y en el conjunto de los quince informes individuales sobre los CBCS.

Metodología

Esta auditoría de los controles básicos de ciberseguridad (CBCS) ha sido realizada por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI), siguiendo la metodología establecida en la guía práctica de fiscalización *GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad* 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, además de ser un sistema ampliamente aceptado, 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. En este sentido la Sindicatura tiene previsto en su Programa Anual de Actuación de 2020 realizar un trabajo de seguimiento de la situación y de la implantación de las recomendaciones efectuadas en cuanto pase un año de la fecha de la auditoría realizada.

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 lo hemos aplicado para los CBCS en las auditorías de los quince ayuntamientos 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 dispone 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 son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.

La metodología utilizada está plenamente alineada con lo establecido por el Esquema Nacional de Seguridad (ENS) que es de aplicación obligatoria en todos los entes públicos. En el apéndice se proporciona un mayor detalle sobre esta.

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 ayuntamientos 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 quince informes individuales han sido 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.

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 los mecanismos necesarios para garantizar que dicha información únicamente es accesible por el personal encargado de la ejecución del presente trabajo.

Una vez elaborados los distintos informes, los resultados al máximo nivel de detalle se han comunicado con carácter confidencial a los responsables de cada entidad, con el objeto de que puedan adoptar las medidas correctoras que consideren precisas para reducir los riesgos de seguridad.

3. CONCLUSIONES GENERALES

Las conclusiones generales más relevantes que se deducen del trabajo realizado son las que se señalan a continuación:

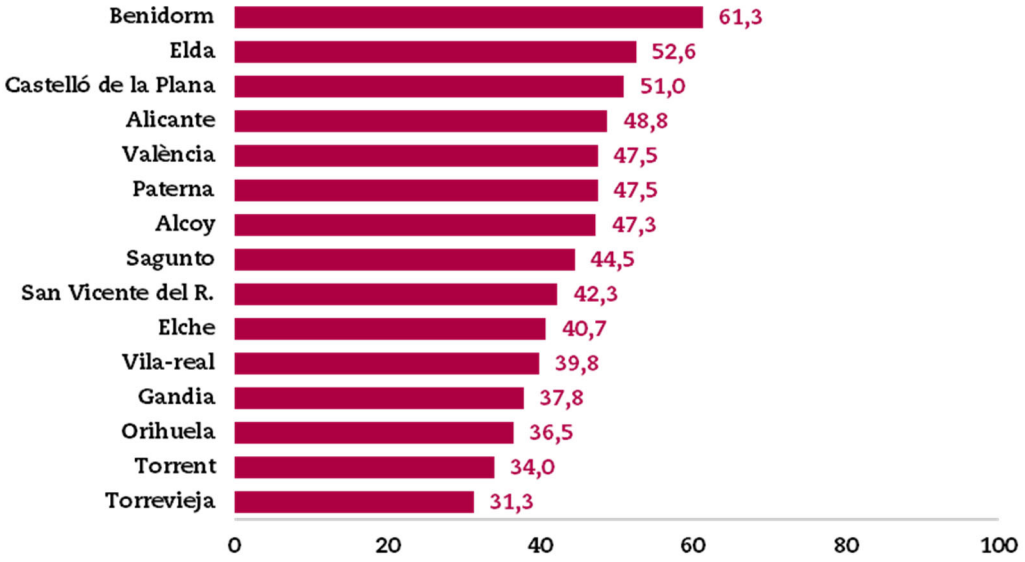
a) La principal conclusión general es que **ningún ayuntamiento auditado dispone de un conjunto de controles de ciberseguridad que permita proteger sus sistemas de información de forma satisfactoria**, esto es, al nivel exigido por el ENS, ni cumplen de forma razonable la normativa relacionada con la seguridad de los SIC.

   El índice de madurez medio de los quince ayuntamientos es el 44,2%, y en todos los ayuntamientos el índice de madurez global de los CBCS es inferior al objetivo requerido del 80%. Ninguno alcanza el nivel de madurez N3 requerido. Para interpretar correctamente los datos hay que tener en cuenta que el aprobado se corresponde con tener un índice de madurez del 80%.

   Los malos resultados obtenidos muestran que **los sistemas de información están en riesgo frente a las amenazas de ciberseguridad** y que los ayuntamientos deben mejorar los controles para gestionar la seguridad de la información, garantizar la

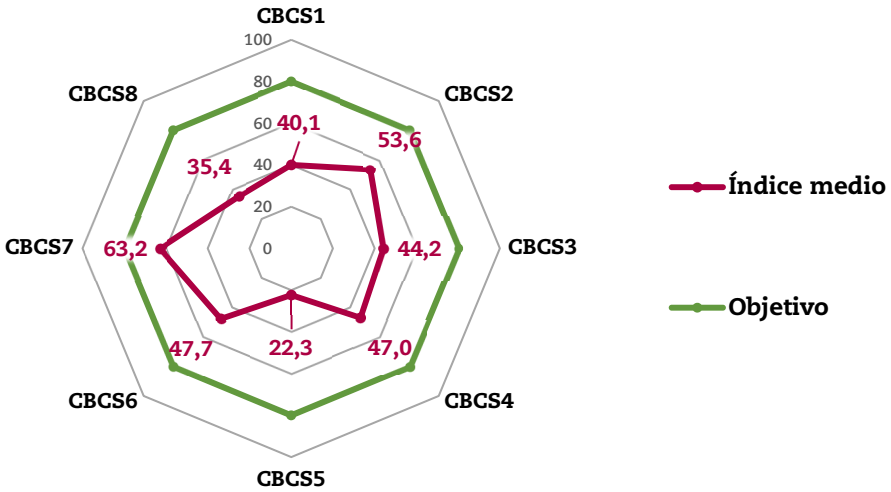
continuidad de la prestación de los servicios públicos y hacer frente a los ciberriesgos.

Gráfico 1. Índice de madurez general de los CBCS



b) El índice y el nivel de madurez medio de todos los CBCS, está por debajo del 80% o Nivel 3 requerido por el ENS. Tal como puede apreciarse en el siguiente gráfico:

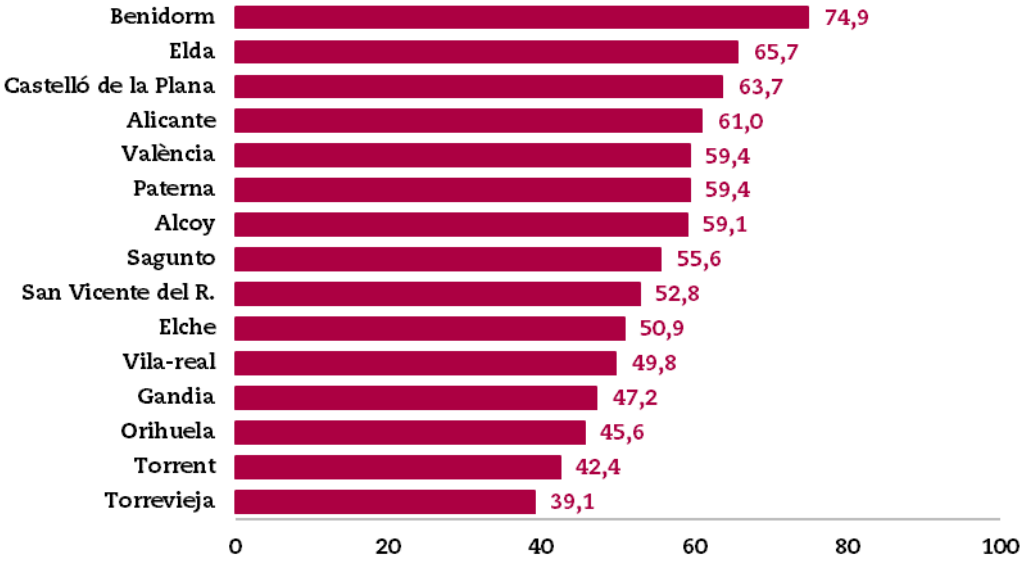
Gráfico 2. Índice medio de madurez de los CBCS



c) El índice de cumplimiento que resulta de comparar el índice medio de madurez de los CBCS (44,2%) con el objetivo del 80% es muy bajo,

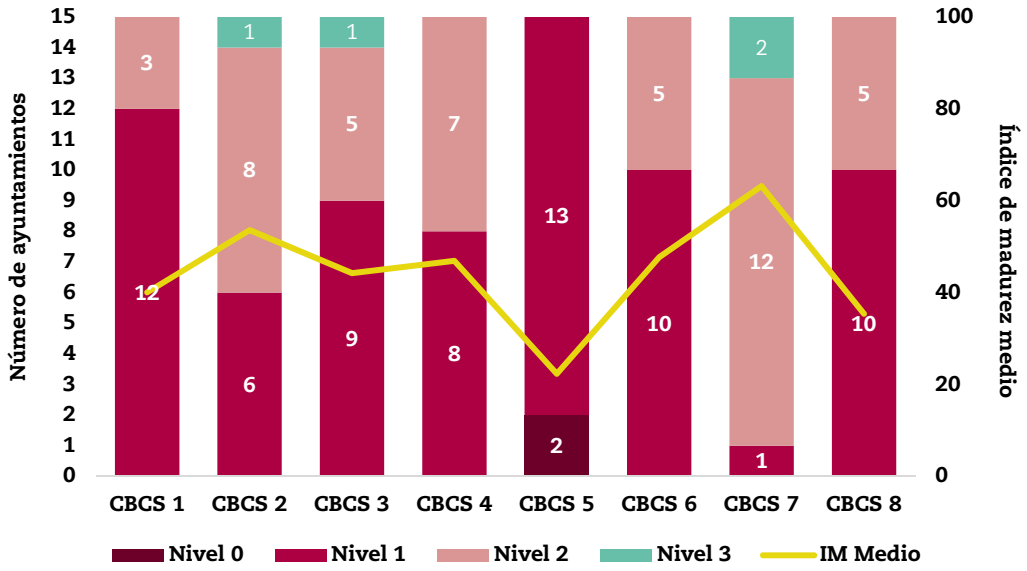
siendo un 55,1% la media general. En el siguiente gráfico puede verse el índice de cumplimiento de cada ayuntamiento respecto al objetivo exigido por el ENS.

Gráfico 3. Índice de cumplimiento de los CBCS



d) Existen deficiencias de control significativas y generalizadas en muchos de los subcontroles revisados.

Gráfico 4. Situación de los niveles de madurez en los quince ayuntamientos

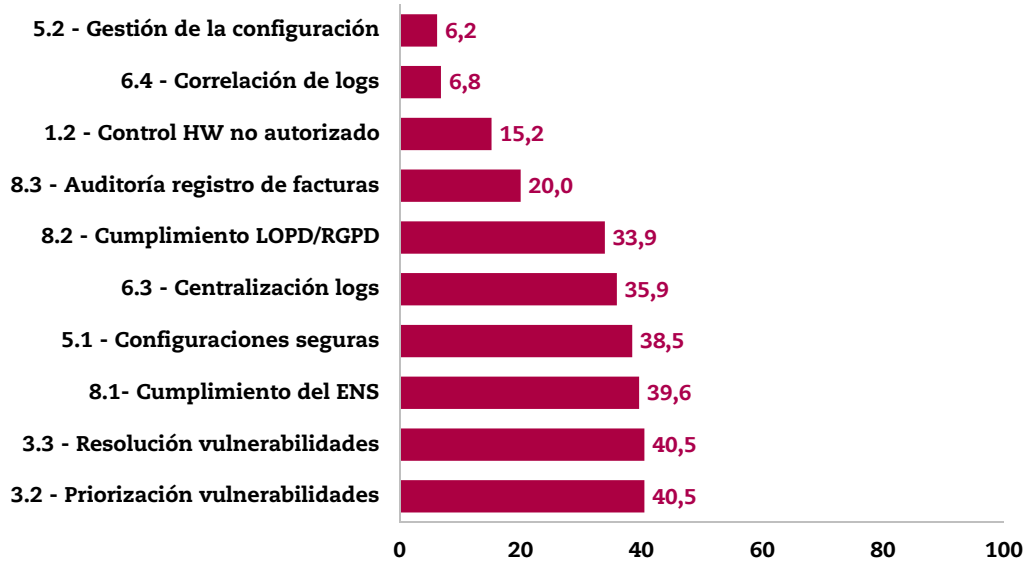


Solo cuatro de un total de 120 CBCS revisados en los quince ayuntamientos alcanzan el nivel de madurez mínimo N3 (o índice de madurez del 80%) establecido como objetivo en el ENS. En el gráfico 4 se muestra esta información de forma detallada.

Es preocupante la existencia de un número significativo de subcontroles cuya efectividad es muy limitada. En el apartado 5, "Resultados de la auditoría", se encuentra una descripción más detallada de las principales deficiencias observadas.

El siguiente gráfico muestra el índice de madurez de los diez subcontroles, de un total de 26 revisados, con los peores resultados obtenidos para el conjunto de los quince ayuntamientos auditados:

Gráfico 5. Los 10 peores resultados obtenidos



e) Hemos observado, **en general, un nivel de cumplimiento de la legalidad bastante insatisfactorio**, tal como refleja el índice medio de cumplimiento del CBCS 8 del 44,2%, que recoge el grado de cumplimiento de varias normas en materia de seguridad de los sistemas de información.

Los máximos órganos de dirección de las entidades locales tienen la responsabilidad de garantizar un nivel adecuado de cumplimiento de las normas legales y deben impulsar las medidas necesarias para subsanar la deficiente situación puesta de manifiesto.

f) Se requieren inversiones sostenidas y un mayor compromiso de los órganos de gobierno con la seguridad de los sistemas de información.

La necesaria mejora de los controles de ciberseguridad requiere de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas y sostenidas en el tiempo, puesto que cada vez más servicios se prestan utilizando sistemas de información y cada vez las amenazas provenientes del ciberespacio son más persistentes y dañinas.

Si no se priorizan presupuestariamente los controles de seguridad y se refuerza la capacidad de resiliencia de los sistemas de información, las entidades asumen riesgos importantes de perturbaciones en la prestación de servicios a su comunidad y se compromete la confidencialidad e integridad de la información que poseen.

4. RECOMENDACIONES GENERALES

Como resultado de las auditorías realizadas se han efectuado una serie de recomendaciones en los informes individuales. Además, las hemos clasificado en cada uno de ellos según criterios combinados del riesgo potencial a mitigar con cada una de las recomendaciones y el coste estimado de su implantación. De esta forma los responsables de los ayuntamientos tienen una orientación para establecer acciones correctoras basadas en criterios de coste/beneficio. También se señala en cada informe las medidas que deben adoptarse para el cumplimiento de la legalidad.

Para atender dichas recomendaciones los ayuntamientos deberán dedicar los esfuerzos y recursos necesarios.

Las recomendaciones generales más relevantes que se deducen del trabajo realizado son las que se señalan a continuación:

a) Todas las normas de seguridad y los procedimientos de seguridad de los sistemas de información y las comunicaciones **deben estar formalmente aprobados** por el órgano superior de dirección del ayuntamiento.

Además, **dicha 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 ayuntamiento.

Las políticas de seguridad deben sintetizar los objetivos y articular la gestión continuada de la seguridad. Las normas deben especificar el uso correcto y las responsabilidades de los usuarios de los sistemas.

Y los procedimientos deben detallar de manera precisa las acciones concretas a realizar.

La aprobación de un marco normativo que no satisfaga estas necesidades de contenido y que no represente la realidad del ayuntamiento 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.

b) Debe existir un **mayor compromiso de los órganos de gobierno del ayuntamiento con la ciberseguridad**. Esto debe reflejarse en:

- La constitución de órganos de gobierno de seguridad formados por miembros de todas las partes implicadas y que faciliten la toma de decisiones e instrumentalicen determinadas responsabilidades.

- El nombramiento de roles de gestión de seguridad, con objeto de concentrar y personalizar las responsabilidades existentes en las organizaciones.

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

- La asimilación de los nuevos retos y oportunidades que surgen de la administración electrónica, que modifican el paradigma tradicional de la gestión de servicios municipales, crean la necesidad de nuevos modos de organización y gestión de los servicios, y que permiten una mejora sustantiva en la aplicación de los principios de eficacia y eficiencia.

- La aceptación de que la ciberseguridad no se encuentra constituida únicamente por un componente tecnológico. **Es un modo de actuar**, de conducirse en el desempeño de las funciones dentro de la organización. 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.

c) Todos los sistemas de información del ayuntamiento deben estar gobernados por las mismas políticas y normas de seguridad. Con carácter general, deben tener un responsable de seguridad único y deben estar bajo el control y supervisión del departamento TIC.

d) Sobre el inventario y control de dispositivos físicos

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

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

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.

e) Sobre el inventario y control de *software* autorizado y no autorizado

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

Otra de las recomendaciones generalizadas ha sido 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. Esta recomendación implica riesgo y coste altos, por lo que se requieren inversiones para garantizar los sistemas actualizados.

f) Sobre el proceso continuo de identificación y remediación de vulnerabilidades

Una de las principales recomendaciones relativas a este CBCS ha sido que los ayuntamientos 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, que carece del control necesario sobre los dispositivos y sistemas. El establecimiento de este tipo de sistemas puede suponer un coste moderado, pero el riesgo disminuye considerablemente.

Adicionalmente, y 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.

g) Sobre el uso controlado de privilegios administrativos

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 del riesgo de manera significativa.

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.

h) Sobre las configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores

La recomendación más frecuente ha sido que los ayuntamientos deben 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.

i) Sobre el registro de la actividad de los usuarios

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 identificación de eventos y vulneraciones de seguridad.

j) Sobre las copias de seguridad de datos y sistemas

Hemos recomendado casi en la totalidad de ayuntamientos la realización de pruebas planificadas de recuperación de las copias de seguridad de datos y sistemas. Carecer de ellas impide garantizar la

eficacia completa del proceso de gestión de copias de seguridad, dado que por lo general solo se realizan recuperaciones de datos de usuarios a demanda.

k) Sobre el cumplimiento normativo

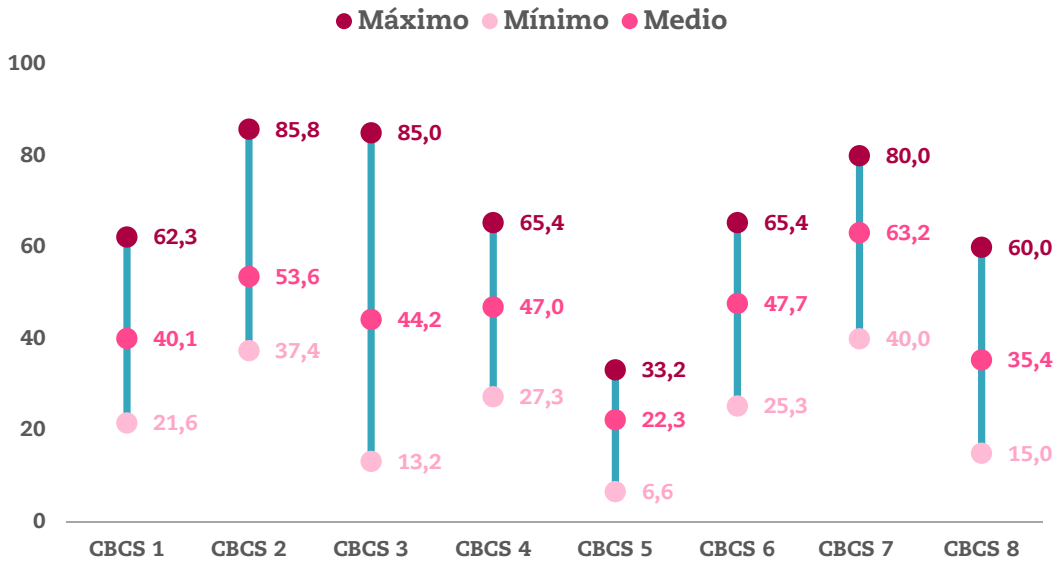
Deben adoptarse las medidas necesarias para dar cumplimiento a los distintos requerimientos legales en materia de seguridad de la información.

5. RESULTADOS DETALLADOS DE LA AUDITORÍA

5.1 Consideraciones generales

Hemos constatado una carencia generalizada de procedimientos de seguridad y control formalmente aprobados. De acuerdo con la definición de los niveles del *modelo de madurez*, para alcanzar un Nivel 3 de madurez de los CBCS es requisito necesario la existencia de procedimientos formalmente aprobados. En algunos casos hemos constatado que existen procedimientos escritos que, aunque son formalmente correctos, han sido realizados por empresas externas y tienen poca o nula adaptación al entorno del ayuntamiento y no reflejan la realidad de las acciones llevadas a cabo en la práctica. En otros casos, el contenido de los procedimientos no detalla de manera clara y precisa las tareas a realizar ni quién debe 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.

Gráfico 6. Dispersión de los resultados obtenidos de los índices de madurez de los CBCS



También hemos observado una situación muy dispar en los quince ayuntamientos auditados, con grandes diferencias en los resultados obtenidos, tal como puede observarse en el gráfico 6 que muestra la dispersión de los resultados obtenidos en los índices de madurez de los CBCS.

Esta disparidad de resultados se corresponde con la impresión recibida durante el trabajo de campo. Aunque es común el marco legal de obligado cumplimiento, el ENS, la realidad muestra que la percepción de la seguridad es muy dispar entre entidades, dependiendo de aspectos como:

a) Los conocimientos, experiencias y perfiles de los profesionales que componen los departamentos fiscalizados.

b) El mayor o menor compromiso de los máximos responsables de los ayuntamientos con la seguridad de la información.

Al analizar los datos es interesante observar cómo, en el caso del CBCS 3, "Proceso continuo de identificación y remediación de vulnerabilidades", hay algún ayuntamiento que ha cumplido sobradamente con los requerimientos y excede en cinco puntos el objetivo del 80%, y sin embargo hay algún ayuntamiento en una situación muy deficiente y solo ha obtenido una valoración de 13,2%.

Particularmente relevante, por los riesgos derivados de su deficiencia, es el insuficiente nivel del CBCS 4, "Uso controlado de privilegios administrativos", para el que únicamente un caso supera el índice de madurez del 60%, muy inferior al nivel requerido. En el curso del trabajo detallado hemos constatado que el control no solo ofrece una cierta dispersión entre ayuntamientos, sino también entre sistemas de un mismo ayuntamiento, ya que en los casos en los que existe un proceso de control adecuado, en general, este nunca es considerado de manera integral para todos los sistemas de la entidad, lo que limita su efectividad y nivel de madurez.

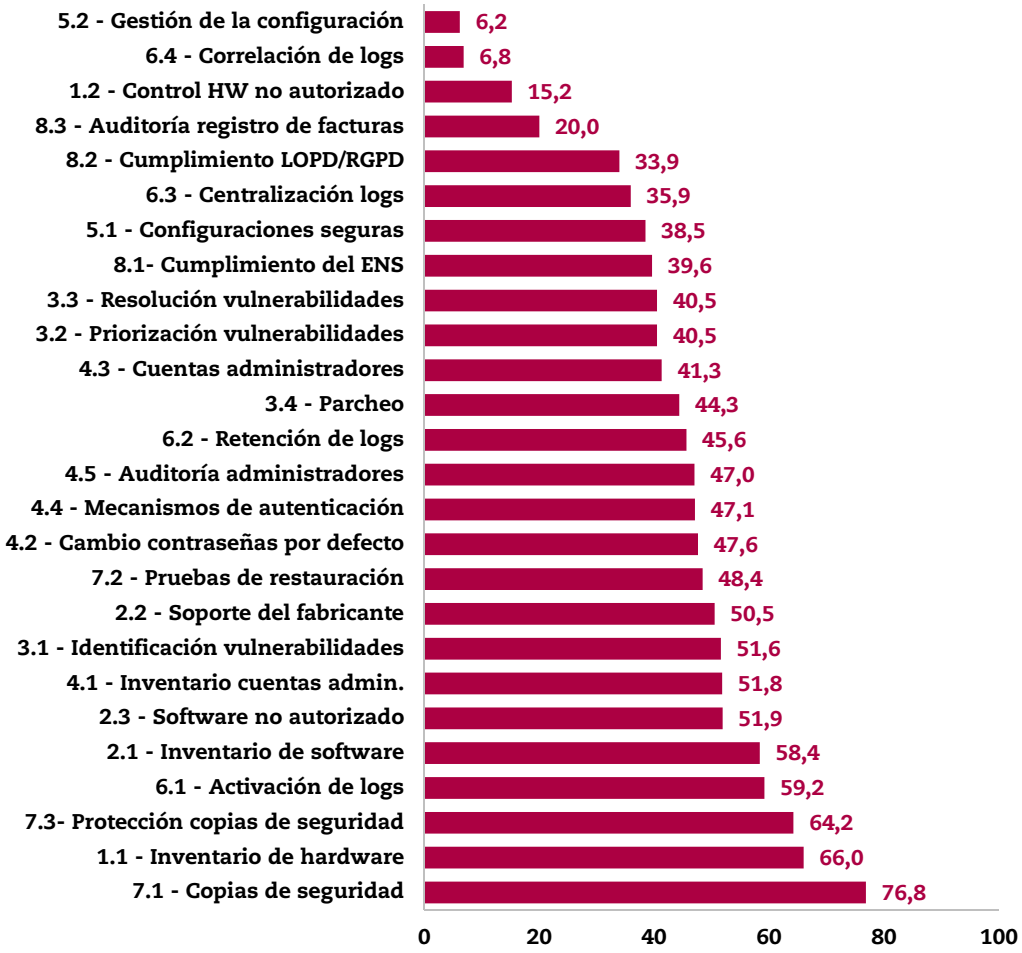
También se observa que en el caso del CBCS 5, "Configuraciones seguras del hardware y software", los resultados han sido muy deficientes en todos los casos. En general, no existen procedimientos específicos establecidos con el objeto de conferir a las configuraciones un nivel determinado de seguridad, y la limitada eficacia de los controles existentes depende casi exclusivamente de los conocimientos técnicos del personal del departamento.

Finalmente se observa que el CBCS 7, "Copias de seguridad de datos y sistemas", es el que ha obtenido la mejor valoración media de todos los CBCS analizados.

Analizando los resultados obtenidos con un mayor grado de detalle, podemos ver en el gráfico 7 el índice de madurez medio obtenido para

cada uno de los 26 subcontroles que se han analizado en los quince ayuntamientos.

Gráfico 7. Índices de madurez medios de los subcontroles



Se observa que en ningún subcontrol el índice medio de madurez alcanza el objetivo del 80%.

Del análisis de los subcontroles con mayores niveles de madurez podemos extraer las siguientes reflexiones:

- Dos de los subcontroles mejor valorados corresponden a procesos de inventariado de activos, tanto físicos como elementos *software*. En la mayor parte de los entes auditados se hace uso de una herramienta (GLPI/OCS Inventory) para la gestión automatizada de dichos inventarios, herramienta cuyo uso ha sido promovido y facilitado por las diputaciones provinciales. Los organismos de asistencia y coordinación externos como las diputaciones ejercen una acción positiva para alcanzar mayores niveles de eficacia sobre el cumplimiento de determinados controles.

- Dos subcontroles correspondientes a la gestión de copias de seguridad alcanzan los niveles de madurez más elevados. Este resultado nos permite evidenciar que las entidades priorizan la aplicación de medidas de recuperación, de coste de gestión medio/bajo, frente a controles preventivos y detectivos con mayor coste de implantación y gestión.

Por otra parte, hay tres subcontroles con un índice de madurez muy deficiente. Los tres presentan un perfil semejante, ya que son técnicamente complejos y requieren de un gran esfuerzo de recursos para alcanzar la efectividad. Por consiguiente, ofrecen una relación coste/beneficio muy reducida, lo que limita su implantación en entornos de escasos medios personales y presupuestarios. Además, dos de estos tres subcontroles son detectivos, más complejos que los preventivos. El único subcontrol preventivo (la gestión de la configuración) también es técnicamente complejo y suele estar reemplazado por compensatorios técnicamente simples, pero de limitada efectividad.

Otras observaciones generales sin impacto directo en los indicadores calculados

Además de las deficiencias específicas para cada CBCS que se señalan en los siguientes apartados, hay algunas consideraciones de carácter general, que no tienen un impacto directo en la cuantificación de los indicadores de madurez utilizados, pero que por su importancia interesa destacar:

- Hemos observado en varios ayuntamientos la existencia de departamentos/zonas de la red que realizan su propia gestión del sistema de información, de forma independiente del departamento TIC. Si bien dichas organizaciones descentralizadas se encontraban previstas en la normativa interna, la descentralización en la gestión dificulta la aplicación homogénea de medidas de seguridad, e impone al responsable de seguridad, si existe, un esfuerzo adicional de coordinación e incrementa los riesgos de control.

- Hemos constatado varios casos de aplicaciones certificadas en el ENS como de nivel de seguridad ALTO con deficiencias de control significativas (excesivo número de usuarios administradores, carencia de doble factor de autenticación, etc.).

- En muchos casos, pese a la aplicación de determinadas medidas de seguridad, no puede considerarse que exista un sistema de gestión de seguridad de la información (SGSI), dado que el conjunto de medidas, acciones y procedimientos implantados no se encuentran coordinados y gestionados con el objeto de alcanzar objetivos definidos.

- Se aprecia en la mayoría de los casos una carencia en el uso de herramientas adecuadas para la gestión de los procedimientos de

seguridad implantados, que pueden ser adecuadamente soportados por herramientas de *workflow* y BPM (gestión de procesos de negocio). Esta insuficiencia dificulta la consideración de los controles implantados como gestionados e impide alcanzar un nivel de madurez N3.

- Hemos observado que pese a la existencia de normativa como el ENS que actúa como elemento normalizador de la seguridad, la percepción sobre los procesos críticos de seguridad que deben ser establecidos es muy dispar entre entidades, lo que conlleva una desigual implantación de determinados controles o medidas de seguridad relevantes.

- Se ha evidenciado el desconocimiento en muchas de las entidades sobre procesos de seguridad, controles, soluciones o herramientas que proporcionen respuesta a determinados problemas comunes a todos los entes. La existencia de casos de éxito en muchos de los subcontroles revisados evidencia la necesidad de coordinación entre entidades y el establecimiento de sinergias que permitan compartir soluciones efectivas a problemas colectivos. Esta tarea debería ser impulsada por las diputaciones provinciales.

En los siguientes apartados se detalla la situación de los controles básicos de ciberseguridad en los quince ayuntamientos auditados.

5.2 CBCS 1. Inventario y control de dispositivos físicos

Objetivo del control

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

Por qué es importante este control básico 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 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.

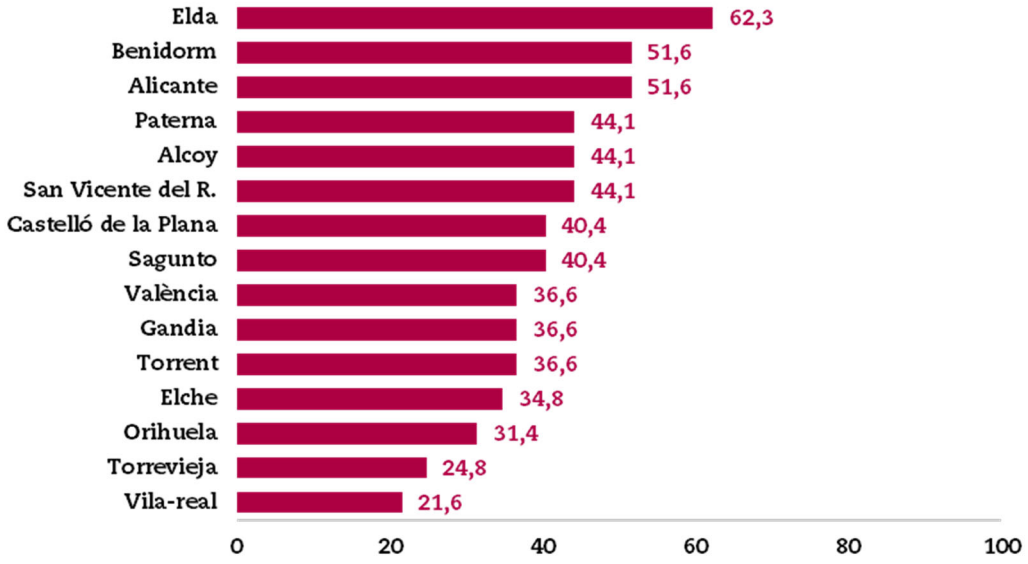
Otros dispositivos que se conectan a la red corporativa (por ejemplo, sistemas para demostraciones, redes para invitados, etc.) deben ser gestionados con cuidado o aislados para prevenir accesos no autorizados que comprometan la seguridad.

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 control en los ayuntamientos revisados

En el siguiente gráfico se muestran los índices de madurez del CBCS 1 en los quince ayuntamientos revisados. Solo tres ayuntamientos alcanzan el nivel de madurez *N2, repetible, pero intuitivo (50%)*, y ninguno el nivel *N3 (80%)* requerido por el ENS.

Gráfico 8. Índices de madurez del CBCS 1



Principales deficiencias observadas

Las principales deficiencias relacionadas con el inventario y el control de dispositivos físicos autorizados y no autorizados han sido:

- Ausencia de un procedimiento formalmente aprobado para la gestión del inventario y el control de activos físicos, que incluya las revisiones periódicas de *hardware* (trece casos).

- El inventario de *hardware* existente no está debidamente actualizado o no contempla todo el *hardware* de la entidad (tres casos).

- Los controles para restringir el acceso de dispositivos físicos no autorizados a la red corporativa son inefectivos o inexistentes (catorce casos).

5.3 CBCS 2. Inventario y control de *software* autorizado y no autorizado

Objetivo del control

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

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* 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 sus activos. 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.

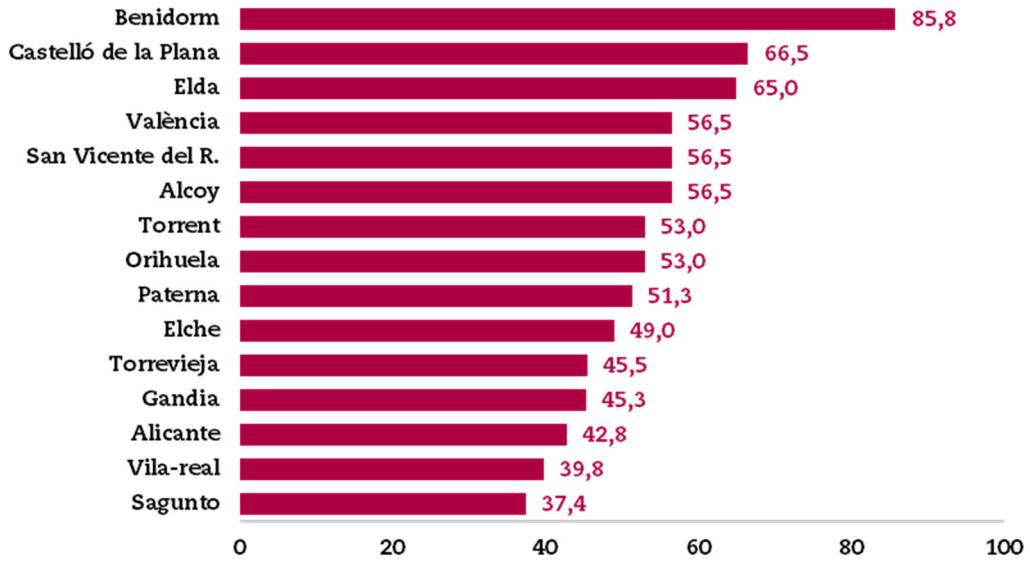
La aplicación de parches y actualizaciones en el *software* inventariado y controlado permite a las entidades eliminar las vulnerabilidades o reducir los riesgos derivados de la materialización de las amenazas. Para que el proceso de actualización y parcheo sea posible, es necesario que la entidad cumpla 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 control en los ayuntamientos revisados

En el siguiente gráfico se muestran los índices de madurez del CBCS 2 en los quince ayuntamientos revisados. Solo un ayuntamiento alcanza el nivel de madurez *N3 (80%)* requerido por el ENS.

Gráfico 9. Índices de madurez del CBCS 2



Principales deficiencias observadas

Las principales deficiencias relacionadas con el inventario y el control de *software* autorizado y no autorizado han sido:

- Ausencia de un procedimiento formalmente aprobado que considere de manera integral el control y la gestión de todo el *software*, aprobando una lista blanca de *software* autorizado, revisiones periódicas y que describa las medidas implantadas para impedir la ejecución del no autorizado (catorce casos).

- Inexistencia de planes de mantenimiento para la gestión del soporte de todo el *software* utilizado en la entidad (quince casos).

- Las medidas para impedir la ejecución de *software* no autorizado o son inexistentes o no son efectivas (tres casos).

- Existe un número significativo de equipos con *software* fuera del periodo de soporte por parte del fabricante (doce casos).

5.4 CBCS 3. Proceso continuo de identificación y remediación de vulnerabilidades

Objetivo del control

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

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.

Las organizaciones 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.

Las organizaciones punteras implementan herramientas especializadas

en el escaneo y gestión de vulnerabilidades de seguridad. Esto permite su detección en los distintos sistemas de forma automática, continua y proactiva, y facilita la instalación de actualizaciones y parches para solucionar las vulnerabilidades existentes.

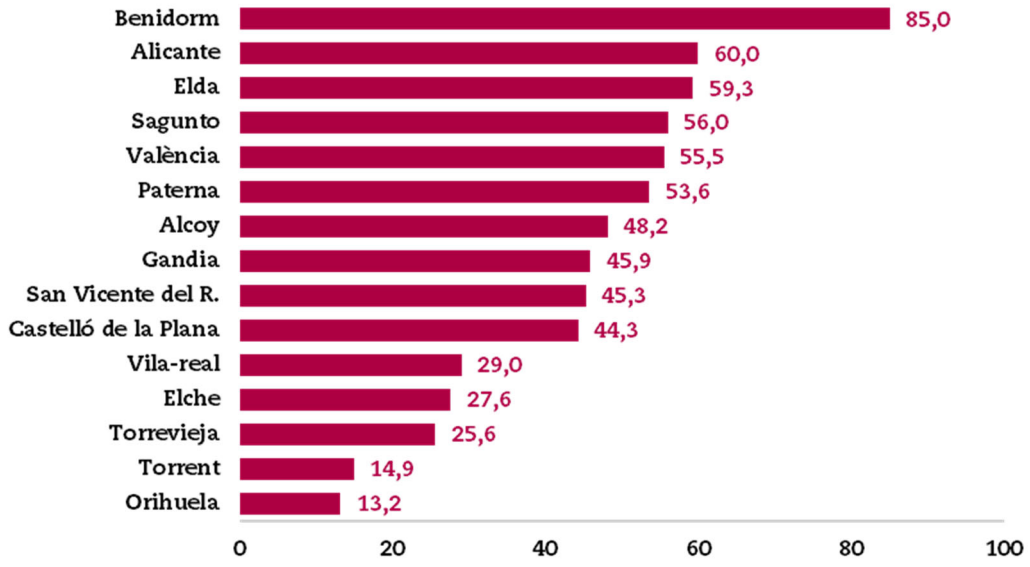
Los ciberdefensores deben operar con un flujo constante de información nueva: actualizaciones de programas, parches, avisos de seguridad, boletines de amenazas, etc. La comprensión y gestión de las vulnerabilidades se ha convertido en una actividad continua, que requiere tiempo, atención y recursos significativos. 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).

Las organizaciones que no escanean las vulnerabilidades y abordan de forma proactiva los defectos encontrados se enfrentan a una alta probabilidad de que sus sistemas informáticos sean comprometidos.

Situación del control en los ayuntamientos revisados

En el gráfico 10 se muestran los índices de madurez del CBCS 3 en los quince ayuntamientos revisados. Solo un ayuntamiento alcanza el nivel de madurez *N3 (80%)* requerido por el ENS.

Gráfico 10. Índices de madurez del CBCS 3



Principales deficiencias observadas

Las principales deficiencias relacionadas con el proceso de identificación y remediación de vulnerabilidades han sido:

- Ausencia de un procedimiento formalmente aprobado para la identificación, priorización, resolución y parcheo de las vulnerabilidades detectadas (trece casos).

- Los equipos de usuario no se actualizan ni reciben parches de seguridad (tres casos).

- No existe gestor de parches y actualizaciones de *software* o la gestión no está correctamente implantada (ocho casos).

- Ausencia de herramientas para realizar escaneos periódicos en busca de vulnerabilidades en la red (doce casos).

5.5 CBCS 4. Uso controlado de privilegios administrativos

Objetivo del control

Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso, asignación y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.

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, su uso controlado, eliminando las que no se utilizan y cambiando las 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 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

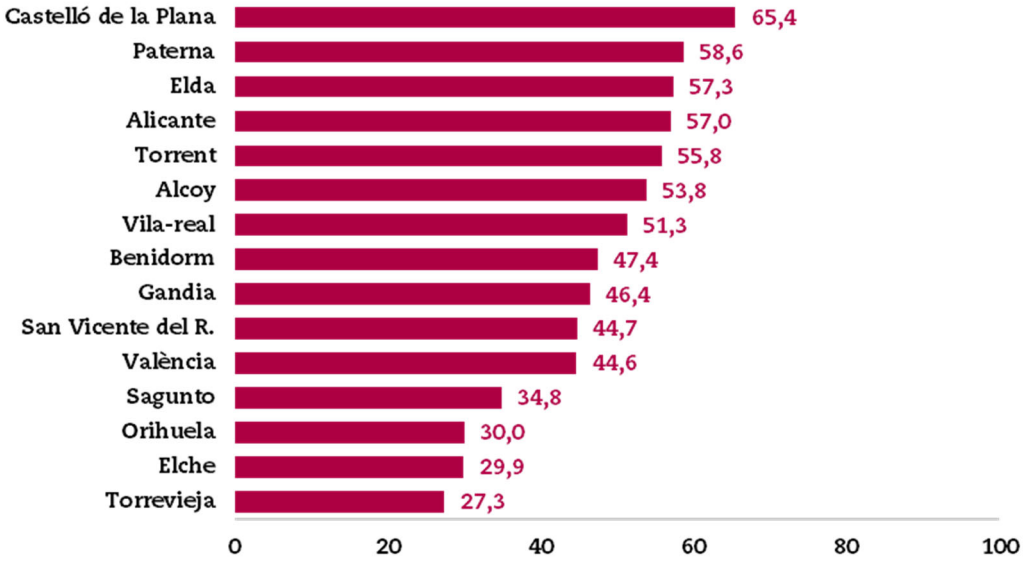
Si los privilegios administrativos se distribuyen de forma holgada, o son idénticos a las contraseñas utilizadas en sistemas menos críticos, o a las que vienen de origen por defecto, al atacante le cuesta mucho menos tomar el control total de los sistemas, porque hay muchas más cuentas que pueden actuar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

En el siguiente gráfico se muestran los índices de madurez del CBCS 4, "Uso controlado de privilegios administrativos", en los quince ayuntamientos revisados. Solo siete ayuntamientos alcanzan el nivel de madurez *N2, repetible, pero intuitivo (50%)*, y ninguno el nivel *N3 (80%)* requerido por el ENS.

Gráfico 11. Índices de madurez del CBCS 4



Principales deficiencias observadas

Las principales deficiencias relacionadas con el uso controlado de las cuentas de administración de los sistemas han sido:

- Ausencia de un procedimiento formalmente aprobado para la gestión de usuarios con privilegios de administración que se aplique a todos los sistemas de la entidad (doce casos).

- Existencia de usuarios no nominativos con privilegios de administración en los distintos sistemas, lo que impide la trazabilidad de las acciones en caso de incidentes de seguridad (diez casos).

- Sistemas y dispositivos con los usuarios y contraseñas por defecto (siete casos).

- Excesivo número de usuarios administradores o de usuarios con privilegios de administración sobre sus equipos (dos casos).

- Los administradores de sistemas no utilizan diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar (tareas de administración del sistema o tareas ofimáticas que no requieren privilegios administrativos), lo que incumple la regla de la mínima funcionalidad (nueve casos).

- Inexistencia de una política robusta de contraseñas que se aplique a todos los dispositivos y sistemas, o si existe no está aplicada correctamente (seis casos).

5.6 CBCS 5. Configuraciones seguras del *hardware* y *software* de dispositivos móviles, portátiles, equipos de sobremesa y servidores

Objetivo del control

Establecer una configuración base segura para 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.

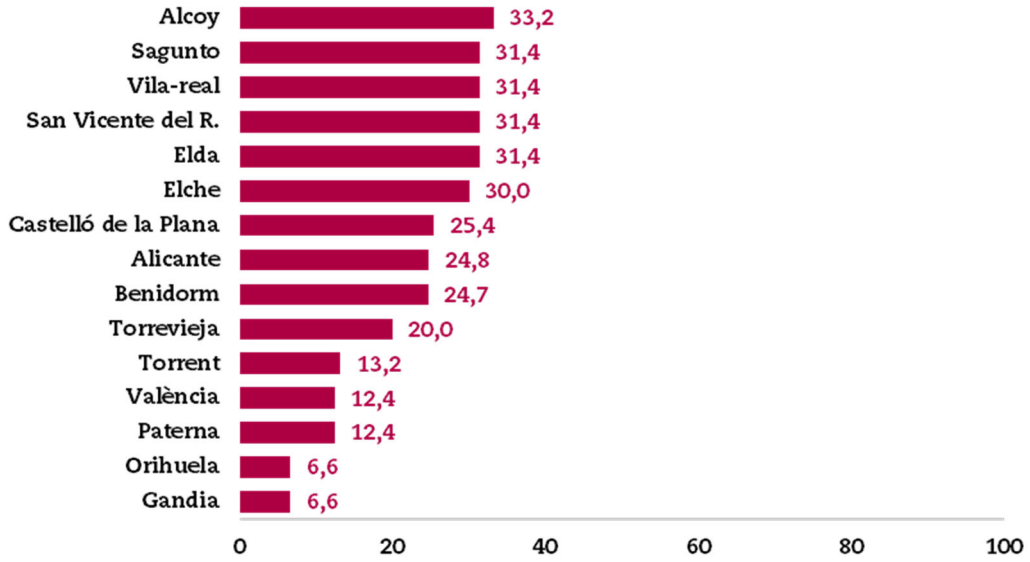
Para implantar de manera efectiva este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad. El desarrollo de opciones de configuración con buenas propiedades de seguridad no es una tarea sencilla y va más allá de la capacidad de los usuarios individuales, 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 control en los ayuntamientos revisados

En el siguiente gráfico se muestran los índices de madurez del CBCS 5 en los quince ayuntamientos revisados. Ningún ayuntamiento alcanza el nivel de madurez *N2, repetible, pero intuitivo (50%)*. Los resultados obtenidos en este importante CBCS son muy deficientes en todos los casos.

Gráfico 12. Índices de madurez del CBCS 5



Principales deficiencias observadas

Las principales deficiencias detectadas relacionadas con la configuración segura del *hardware* y del *software* han sido:

- Ausencia de procedimientos formalmente aprobados para la aplicación de configuraciones seguras a dispositivos y sistemas, considerando la seguridad por defecto y el criterio de mínima funcionalidad (catorce casos).

- En los casos en los que se dispone de plantillas para la configuración de determinados dispositivos y sistemas, estas no tienen carácter de bastionado, ni la configuración segura de estos dispositivos se encuentra formalmente establecida (siete casos).

- Ausencia de mecanismos que garanticen una monitorización efectiva de cambios no autorizados en la configuración en los sistemas críticos de la entidad (quince casos).

5.7 CBCS 6. Registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría)

Objetivo del control

Recoger, gestionar y analizar *logs* 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 del 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 manual, 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. Incluso con herramientas de análisis de registro automatizado, se requiere la intuición y experiencia humana para identificar y comprender los ataques.

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.

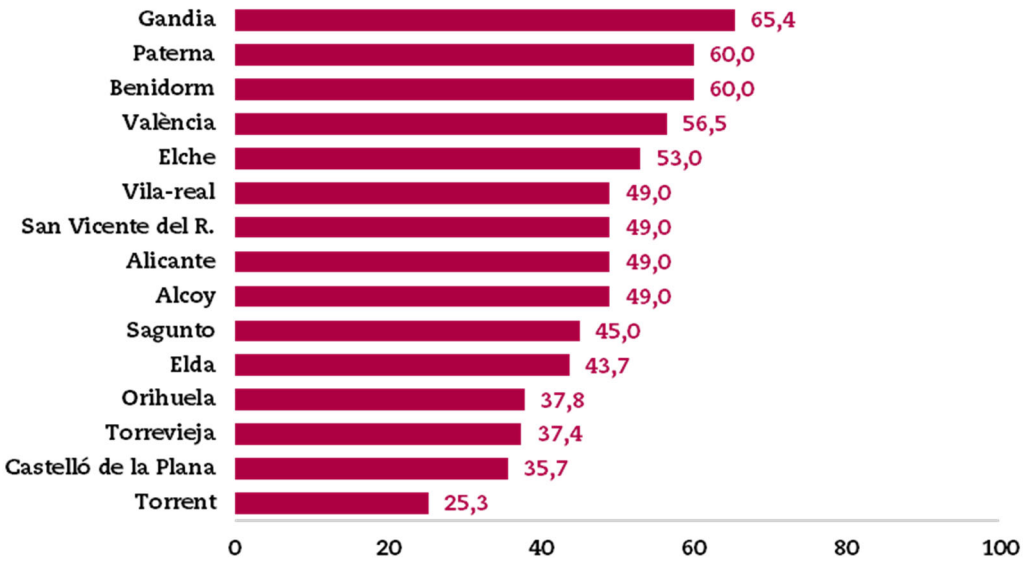
Por todo lo expuesto anteriormente, las organizaciones deben incluir entre sus procedimientos de seguridad la gestión de los registros de auditoría, en los que se definan los sistemas afectados, los tipos de eventos a registrar, el periodo de retención, los responsables y los mecanismos de protección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

Situación del control en los ayuntamientos revisados

En el siguiente gráfico se muestran los índices de madurez del CBCS 6 en los quince ayuntamientos revisados. Solo cinco de ellos alcanzan el nivel de madurez *N2, repetible, pero intuitivo (50%)*, y ninguno el nivel *N3 (80%)* requerido por el ENS.

Gráfico 13. Índices de madurez del CBCS 6



Principales deficiencias observadas

Las principales deficiencias relacionadas con el registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría) que hemos detectado han sido:

- Carencia de procedimientos formalmente aprobados por el órgano competente que describa la gestión de los registros de actividad de los usuarios, incluyendo los sistemas afectados, la información recabada, el periodo de retención y los mecanismos de protección de dichos registros (catorce casos).

- Aunque los registros de actividad se encuentran activados se mantiene la configuración por defecto definida por el fabricante, sin tener en cuenta aspectos como el periodo de retención, tipo de acciones a registrar, etc. (siete casos).

- Los registros de auditoría de los distintos dispositivos y sistemas no están centralizados en herramientas de recolección de *logs* que faciliten su revisión (quince casos).

5.8 CBCS 7. Copias de seguridad de datos y sistemas

Objetivo del control

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

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 mediante *ransomware* pueden ser minimizados si se dispone de copia de seguridad de los datos secuestrados.

Los ciberdelincuentes han ido evolucionando con el paso del tiempo, mejorando los métodos de cifrado o el acceso a los recursos del sistema. Este tipo de ataques "mejorados" ha sido utilizado con 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.

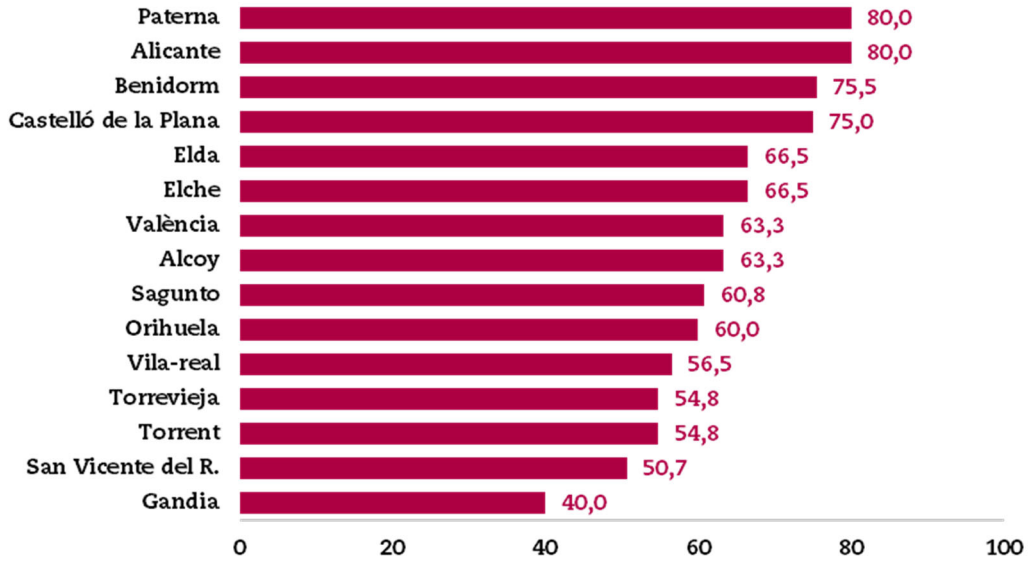
Con la evolución de la ciberdelincuencia y los métodos de ataque cada vez más sofisticados, es necesario que las organizaciones estén preparadas no solo para defenderse, sino también para reponerse ante ataques exitosos, es un elemento clave de la ciber-resiliencia de una entidad.

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 control en los ayuntamientos revisados

En el siguiente gráfico se muestran los índices de madurez del CBCS 7 en los quince ayuntamientos revisados. Solo dos ayuntamientos alcanzan el nivel *N3 (80%)* requerido por el ENS.

Gráfico 14. Índices de madurez del CBCS 7



Principales deficiencias observadas

Las principales deficiencias detectadas en este control han sido:

- Ausencia de procedimientos formalmente aprobados por el órgano competente que describa las acciones que deben llevarse a cabo para realizar copias de seguridad de datos y sistemas (diez casos).

- En general las políticas de copia de seguridad existentes han sido desarrolladas de acuerdo con criterios del departamento TIC, sin la

participación activa de los responsables funcionales de las aplicaciones señalando sus necesidades (cinco casos).

- No se realizan pruebas de recuperación planificadas de los sistemas críticos de la entidad (diez casos).

- Las medidas implantadas para la protección de las copias no son efectivas, existen copias no separadas físicamente del CPD principal, otras son accesibles a través de la red o bien no existen copias desconectadas (tres casos).

5.9 CBCS 8. Control de legalidad

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.

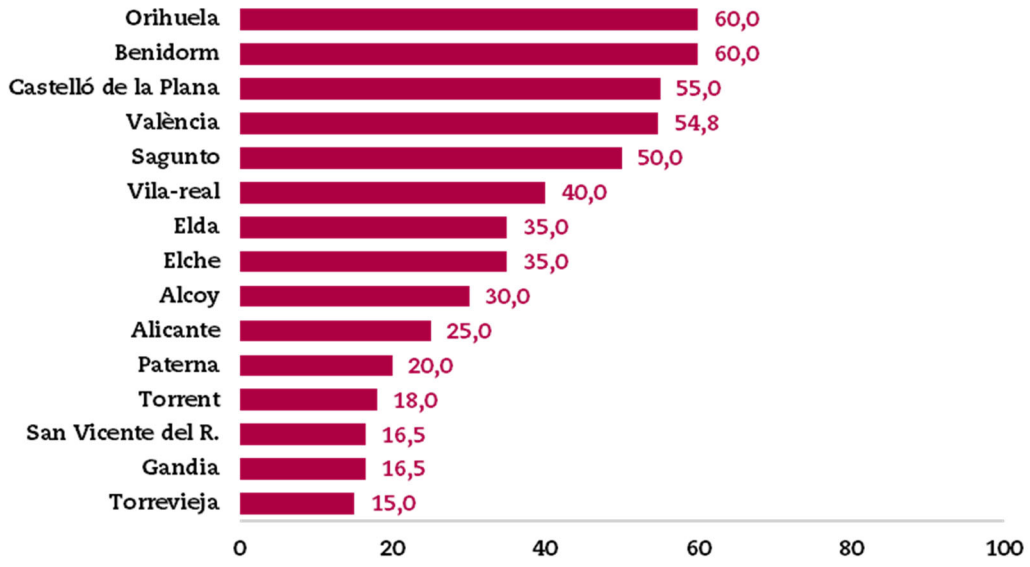
Por otra parte, las Administraciones públicas, en el desarrollo de sus actividades, actúan como responsables de tratar datos personales y deben garantizar el derecho de las personas a la protección de sus datos. Por tanto, deben adoptar las medidas necesarias para garantizar el nivel de seguridad requerido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

Madurez del control de cumplimiento en los ayuntamientos revisados

En el siguiente gráfico se muestran los índices de madurez del CBCS 8 referido al cumplimiento legal, en los quince ayuntamientos revisados. Solo cinco ayuntamientos alcanzan el nivel de madurez N2, *repetible, pero intuitivo (50%)*, y ninguno el nivel N3 *(80%)*.

Gráfico 15. Índices de madurez del CBCS 8



Principales deficiencias observadas

La revisión del cumplimiento de varias normas relacionadas con la seguridad de la información **ha puesto de manifiesto, en general, un nivel de cumplimiento bastante insatisfactorio**.

Dado el bajo nivel detectado en el cumplimiento de legalidad, la práctica totalidad de requisitos han sido frecuentemente incumplidos. Cabría pues destacar aquellos que suponen un mayor impacto a efectos de protección de datos de carácter personal y de consecución del requerido nivel de seguridad de los sistemas de información:

- La ausencia de Política de Seguridad aprobada y de cuerpo normativo y procedimental, evidenciando la falta de conciencia y de

compromiso de la entidad con la seguridad de la información y la protección de datos personales (cinco casos).

- La inexistencia de órganos de gobierno y de los perfiles requeridos por la normativa vigente, particularmente del DPD y del responsable de seguridad, carencias que dificultan la toma de decisiones, la unificación de criterios y la implantación homogénea de medidas de seguridad (seis casos).

- La falta de un registro de actividades del tratamiento, que implica la identificación y consideración de todos los usos de datos de carácter personal, requisito previo imprescindible para la implantación de medidas y el cumplimiento de obligaciones para con el uso de dichos datos (siete casos).

APÉNDICE. Metodología aplicada

1. Introducción

Los actuales sistemas de información son más complejos y están más interconectados que nunca, pero una mayor interconexión origina mayores riesgos de ciberseguridad, ocasiona una mayor probabilidad de que se produzca una perturbación significativa en los sistemas de información de las entidades locales debida a un ciberataque y, en consecuencia, una interrupción en los servicios prestados a los ciudadanos.

Por esta razón, es imperativo que los responsables de los entes públicos gestionen los riesgos asociados con el funcionamiento y uso de sistemas de información que utilizan para desarrollar y prestar los servicios públicos. Asimismo, es fundamental establecer controles de ciberseguridad adecuados para mantener los sistemas de información protegidos frente a las amenazas de seguridad.

La gestión de los riesgos de ciberseguridad comprende una amplia gama de actividades emprendidas para: proteger los sistemas de información y los datos de accesos no autorizados y otras amenazas cibernéticas; mantener la conciencia de las amenazas cibernéticas; detectar anomalías e incidentes que afecten negativamente a los sistemas de información y a los datos, y mitigar su impacto, responder y recuperarse de incidentes.

La existencia de unos eficaces CBCS es un elemento esencial para la prestación de servicios públicos de una forma tecnológicamente sostenible.

Aun cuando la adopción de medidas de seguridad adecuadas hace más resilientes a las organizaciones frente a los ciberataques, la descripción de los incidentes ocurridos en 2017 que se realiza en el Informe Nacional del Estado de Seguridad de los Sistemas de las TIC del CCN, revela que las organizaciones no siempre implementan, tan siquiera, las medidas más básicas que podrían haber prevenido o mitigado el daño causado. Se citan en ese informe un par de ejemplos: ataques como WannaCry o BadRabbit, explotaron vulnerabilidades conocidas. Las actualizaciones para estas vulnerabilidades habían estado disponibles durante meses, pero no se habían instalado en las organizaciones afectadas. En otros casos, aunque las vulnerabilidades eran desconocidas, la adopción de las medidas de seguridad más elementales habrían supuesto un impedimento para el ataque o habrían mitigado sus efectos.

Por otro lado, el hecho de que los ciberataques permanezcan sin ser detectados durante mucho tiempo puede ser evidencia de que las medidas básicas no están correctamente implementadas. Recientes investigaciones han revelado que las empresas, los gobiernos y las

organizaciones en Europa, frecuentemente, solo descubren que han sido víctimas de un ciberataque meses después.

2. La guía práctica de fiscalización de los OCEX 5313

La presente auditoría está basada en la guía práctica de fiscalización de los OCEX ***GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad*** aprobada por la Conferencia de Presidentes de los Órganos de Control Externo el 12 de noviembre de 2018, que forma parte del *Manual de fiscalización* de la Sindicatura de Comptes y 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, que es de obligado cumplimiento para todos los entes públicos. 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 seleccionar los más relevantes se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security (CIS[1]), que prioriza y clasifica los controles según su importancia para hacer frente a las ciberamenazas.

Los veinte controles de seguridad críticos del CIS son un conjunto conciso y priorizado de acciones de ciberdefensa, y su ventaja principal es que están orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. Según el CIS, con carácter general, las organizaciones que apliquen solo los cinco primeros controles pueden reducir su riesgo ante ciberataques alrededor del 85%. Si se implementan los veinte controles el riesgo se puede reducir un 94%.

La versión 7 de los controles CIS clasifica los seis primeros controles como básicos y son los que se han utilizado como referencia en la GPF-OCEX 5313 para establecer los controles básicos de ciberseguridad (CBCS) de los OCEX. A ellos se añadió el relativo a las copias de seguridad de datos y sistemas (décimo control CIS) por su importancia para la recuperación frente a un desastre o ataque exitoso y por tanto para garantizar una razonable ciber-resiliencia. Si todos los controles preventivos fallan y un ciberataque traspasa todas las líneas de defensa y tiene éxito, el último recurso de la entidad atacada es restaurar sus sistemas y datos en un plazo predeterminado para poder continuar prestando sus servicios.

A los siete CBCS se añadió un octavo relacionado con el cumplimiento normativo, por su importancia en una administración pública.

---

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

3. Los CBCS como medidas de ciberhigiene

La European Union Agency for Cybersecurity (ENISA) señala[2] que "la ciberhigiene es un principio fundamental relativo a la seguridad de la información y, como la 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 utiliza para hacer referencia 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.

En esa dirección, ENISA establece diez puntos de acción para una adecuada ciberhigiene. Como se observa en la siguiente tabla, los siete primeros son en buena medida coincidentes con los CBCS:

Cuadro 2. 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 dentro y fuera de su 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

De los siete CBCS, sin contar el cumplimiento normativo, cinco son coincidentes con los puntos de acción prioritarios recomendados por ENISA como buenas prácticas de ciberhigiene. A los efectos de este trabajo, consideramos que los CBCS constituyen un conjunto de prácticas y acciones básicas para mantener una adecuada ciberhigiene.

[2] *Review of Cyber Hygiene Practices*, ENISA, diciembre de 2016.

4. Alineación con el Esquema Nacional de Seguridad

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

Los ocho controles básicos de ciberseguridad debidamente referenciados con el ENS son:

Cuadro 3. Los CBCS y el ENS

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

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

Cuando una auditoría se realice en entidades que hayan pasado la auditoría de seguridad obligatoria establecida en el artículo 34 del Real Decreto 3/2010 por el que se aprueba el ENS, la revisión de la Sindicatura podrá basarse, en la medida de lo posible, en los resultados de dicha auditoría y determinadas comprobaciones podrán darse por cumplidas.

Para depositar confianza en dichas auditorías externas de seguridad, deberán cumplir con los requisitos legalmente establecidos como son, entre otros, que las entidades certificadoras estén acreditadas y constar en la sección "Entidades de certificación acreditadas" de la página web del CCN (es necesaria su acreditación si se pretende certificar el cumplimiento

del ENS). Además, el equipo de auditoría deberá obtener alguna evidencia de que el trabajo realizado ha sido adecuado para soportar las conclusiones de ese informe. Cuando se haya depositado confianza en estas auditorías se señalará expresamente en el informe.

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

Los CBCS son controles globales formados por varios subcontroles detallados que se muestran en la siguiente tabla. Todas nuestras comprobaciones tienen por finalidad contrastar su situación real en la entidad con las buenas prácticas recogidas en la GPF-OCEX 5313, que se resumen en el siguiente cuadro.

Los aspectos que se comprueban en cada CBCS se especifican con el máximo detalle en la GPF-OCEX 5313.

En cuanto a los índices o niveles objetivo que deben alcanzarse en cada CBCS y subcontrol, véase el apartado 6 siguiente.

Cuadro 4. Los CBCS y sus subcontroles

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

Control	Objetivo del control	Subcontrol	
CBCS 5 Configuraciones seguras del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Establecer, implantar y gestionar la configuración de seguridad de los dispositivos móviles, portátiles, servidores y de sobremesa, 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 de legalidad	La entidad cumple con los requisitos legales y reglamentarios que le son de aplicación.	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 (CBCS).

Subcontroles

Los CBCS son controles globales compuestos por varios subcontroles detallados (tal como puede verse en el apartado 2 anterior), cuyo diseño y eficacia operativa hemos revisado.

El trabajo de auditoría consiste básicamente en evaluar cada subcontrol en función de los resultados de las pruebas realizadas y las evidencias obtenidas, o bien de la información proporcionada en el informe de auditoría del ENS, si existe y si confiamos en él. Cada subcontrol se evalúa según la escala mostrada en el siguiente cuadro:

Cuadro 5. Evaluación de los subcontroles

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

De acuerdo con los resultados obtenidos en cada subcontrol se establece una correspondencia con el nivel de madurez descrito en el siguiente cuadro.

Nivel de madurez de los CBCS

Para determinar la situación global de cada CBCS 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 Centro Criptológico Nacional, usando una escala, según se resume en el siguiente cuadro.

Cuadro 6. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	El CBCS no está siendo aplicado en este momento.
N1 Inicial / *ad hoc*	10	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado. *La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.*
N2 Repetible, pero intuitivo	50	Los procesos siguen una pauta regular cuando los 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 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 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, era solamente cualitativa.*

Nivel	Índice	Descripción
N5 Optimizado	100	Se siguen buenas prácticas en un ciclo de mejora continua. *El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras.* *Se establecen objetivos cuantitativos de mejora, y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.* *En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.*

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

Para evaluar el nivel de madurez de cada CBCS se han tenido en cuenta los resultados obtenidos en la revisión de los subcontroles que lo forman y considerando la ponderación o importancia relativa que les asignamos para el cumplimiento del objetivo de control del CBCS.

Este modelo proporciona una base sólida para formarse una idea general de la situación en la entidad revisada de 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 las tecnologías de la información y la comunicación de los organismos del sector público obligados al cumplimiento del ENS se les asigna una categoría en función de la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.

b) Proteger los activos a su cargo.

c) Cumplir sus obligaciones diarias de servicio.

d) Respetar la legalidad vigente.

e) Respetar los derechos de las personas.

La categoría de un sistema será de aplicación a todos los sistemas empleados para la prestación de los servicios de la administración electrónica y soporte del procedimiento administrativo general.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se deben tener en cuenta las cinco dimensiones de la seguridad:

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 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[3]:

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 clasificados como de categoría MEDIA.

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%.

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 tanto un resumen del estado de las medidas de seguridad de cada ayuntamiento a los efectos del ENS, como de los CBCS:

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

- 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.

[3] Informe Nacional del Estado de Seguridad de los Sistemas de las Tecnologías de la Información y la Comunicación, de 2018, apartado 3.1. En los diferentes perfiles se evalúan los controles mediante un nivel de exigencia, también conocido como *nivel de madurez*, y se fija el nivel mínimo de exigencia requerido.

9. Fechas del examen

Los trabajos de auditoría de los quince ayuntamientos se iniciaron progresivamente en la primavera de 2019 y finalizaron en la de 2020. Los informes recogen e informan sobre la situación de los CBCS al finalizar el trabajo de campo y emitir el informe de auditoría.

Consideramos como fin del trabajo de campo la fecha en la que los hallazgos de la auditoría, las conclusiones y el borrador previo del informe son discutidos con los responsables de la entidad auditada, de acuerdo con lo establecido en nuestro *Manual de fiscalización*. Es admitida cualquier evidencia adicional disponible en ese momento y corroborados los hechos puestos de manifiesto en el informe. **El informe con carácter general refleja la situación en ese momento**, ya que es frecuente que, desde que se inicia el trabajo de campo, determinadas deficiencias observadas y señaladas a los gestores sean subsanadas y recogidas de esta forma en las conclusiones y en los indicadores.

Para conocer las fechas a las que se refieren los distintos informes señalamos los dos momentos clave para ello en el siguiente cuadro.

Cuadro 7. Momento que refleja la situación de los CBCS en los distintos ayuntamientos

Ayuntamiento	Fin del trabajo de campo	Plazo para remisión de alegaciones
Benidorm	04/10/2019	20/12/2019
Gandia	24/10/2019	10/01/2020
Alicante	23/10/2019	20/12/2019
Paterna	25/10/2019	28/02/2020
València	30/10/2019	20/12/2019
Orihuela	13/11/2019	10/01/2020
Torrent	25/11/2019	03/02/2020
Torrevieja	11/12/2019	13/02/2020
Elche	26/12/2019	03/02/2020
Castelló de la Plana	16/01/2020	28/02/2020
Sagunto	23/01/2020	28/02/2020
San Vicente del Raspeig	24/04/2020	12/06/2020
Elda	20/04/2020	12/06/2020
Alcoy	30/04/2020	12/06/2020
Vila-real	05/06/2020	06/07/2020

La tramitación formal de los informes incluye el trámite de alegaciones, en el que las entidades pueden aportar evidencias adicionales sobre la situación de los CBCS a la fecha del fin del trabajo de campo. Si es así se analizan, consideran y si se admiten se pueden modificar conclusiones e indicadores. Si se aportan evidencias con efecto posterior a la fecha señalada para la remisión de alegaciones a la Sindicatura, podrían recogerse en el informe, pero en este caso no alterarían las conclusiones ni los indicadores. En todo caso, tanto las alegaciones como el análisis de estas y el efecto en los informes son publicados como un anexo de los informes.

Además, es importante saber a qué fecha se refiere el informe, ya que en el Programa Anual de Actuación de 2020 está expresamente previsto realizar un informe de "Seguimiento de las 11 auditorías de los controles básicos de ciberseguridad cuyo trabajo de campo se ha realizado en 2019 (una vez transcurrido un año desde su finalización)". Razonablemente este seguimiento tendrá continuidad con los cuatro ayuntamientos auditados en 2020.

La finalidad del seguimiento de las auditorías será verificar si los ayuntamientos han introducido medidas correctoras a las deficiencias señaladas en los informes.

Con ánimo de facilitar esa tarea, en los informes hemos clasificado nuestras recomendaciones según criterios combinados de riesgo potencial a mitigar y coste de su implantación; de esta forma pueden establecerse acciones basadas en criterios de coste/beneficio, y las hemos reflejado en un gráfico.

Además de las recomendaciones señaladas en los informes, junto con el detalle al máximo nivel de las deficiencias de seguridad observadas, se ha comunicado a los responsables de cada ayuntamiento otras recomendaciones con una relación de riesgo potencial a mitigar y coste de su implantación menos favorable que las anteriores.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes de acuerdo con la redacción dada por la Ley de la Generalitat Valenciana 16/2017, de 10 de noviembre y del artículo 55.1.h) de su Reglamento de Régimen Interior y, en el Programa Anual de Actuación de 2020 de esta Institución, el Consell de la Sindicatura de Comptes, en reunión del día 9 de julio de 2020, aprobó este informe de auditoría.