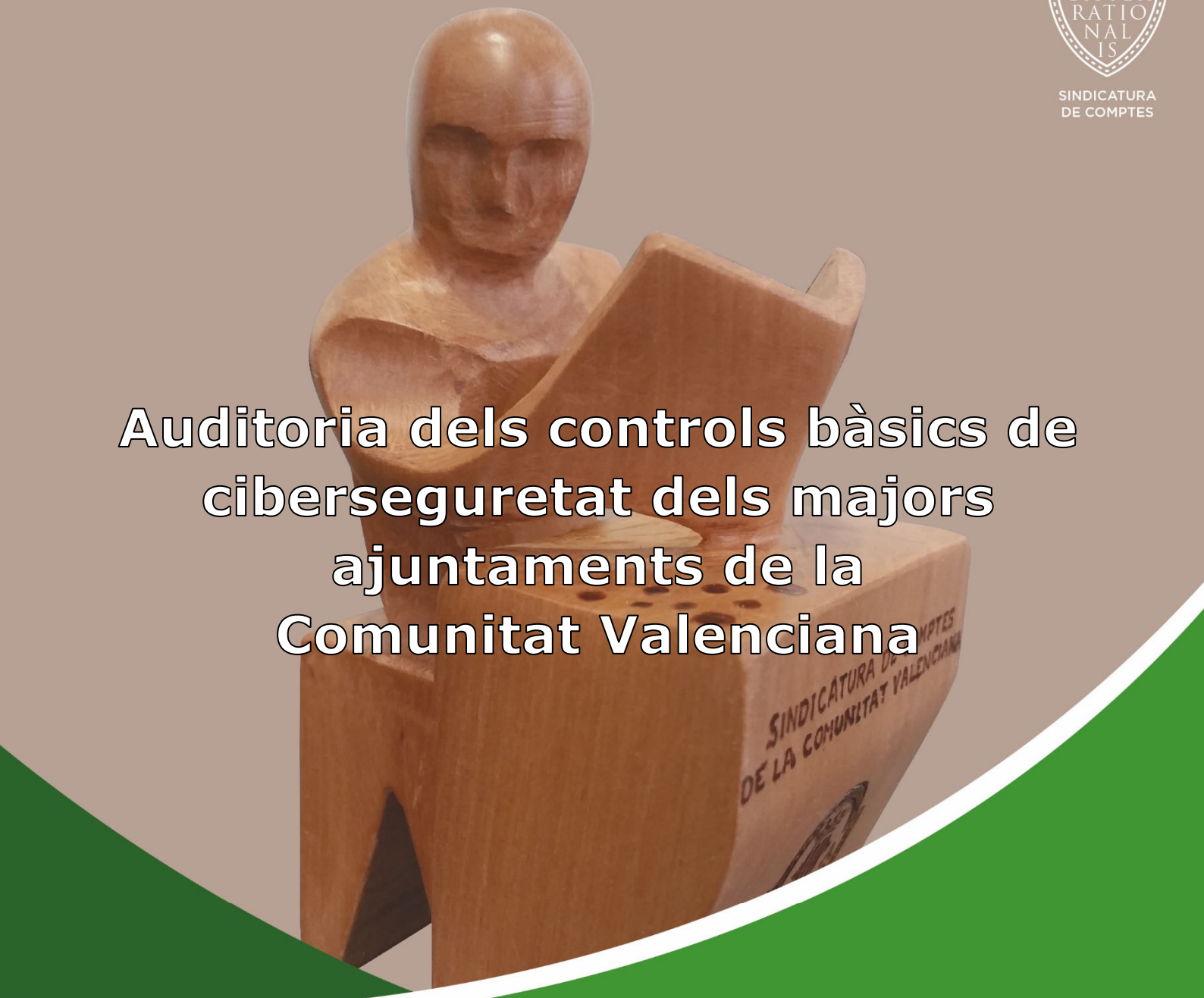
SINDICATURA DE COMPTES



Auditoria dels controls bàsics de ciberseguretat dels majors ajuntaments de la Comunitat Valenciana

Els sistemes d'informació estan en risc davant de les amenaces de ciberseguretat

Exercicis 2019 i 2020

AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DELS MAJORS AJUNTAMENTS DE LA COMUNITAT VALENCIANA

Els sistemes d'informació estan en risc davant de les amenaces de ciberseguretat

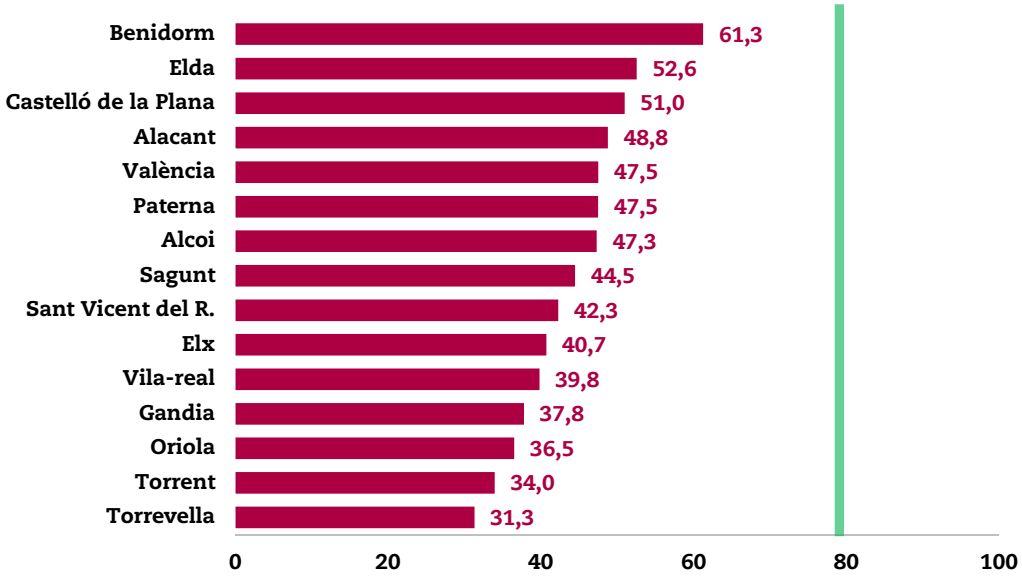
Exercicis 2019 i 2020

RESUM

Els sistemes d'informació analitzats estan en risc davant de les amenaces de ciberseguretat

Cap dels ajuntaments auditats aconsegueix l'índex de maduresa dels controls bàsics de ciberseguretat del 80% requerit per l'ENS (és a dir, només es pot considerar haver obtingut un "aprovat" en ciberseguretat si s'arriba a la línia verda del gràfic).

Baix índex de maduresa dels CBCS



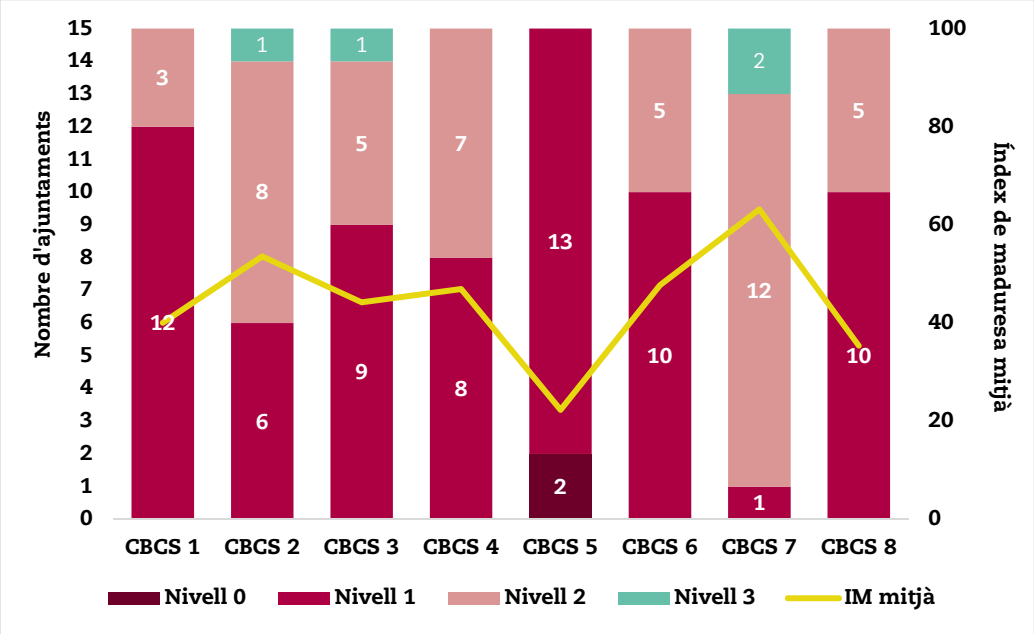
En general, el nivell de compliment amb la normativa relacionada amb la seguretat de la informació és bastant insatisfactori

La revisió del compliment de legalitat en matèria relacionada amb la ciberseguretat ha posat de manifest que hi ha incompliments generalitzats d'aquesta normativa, amb un índex mitjà de compliment del CBCS 8 del 44,2%. Els màxims òrgans de direcció dels ajuntaments tenen la responsabilitat de garantir un nivell adequat de compliment de les normes legals i han d'impulsar les mesures necessàries per a esmenar la deficient situació existent.

Tots els ajuntaments han d'adoptar mesures per a millorar la seua ciberseguretat

D'un total de 120 controls bàsics revisats en els quinze ajuntaments, només quatre controls aconsegueixen el nivell de maduresa N3 establit com a objectiu en l'ENS. En el gràfic següent es mostren de forma resumida els nivells de maduresa observats per als huit controls bàsics en el conjunt dels quinze ajuntaments, i l'índex de maduresa (IM) mitjà de cada CBCS que s'hi ha observat.

Situació dels nivells de maduresa en els quinze ajuntaments auditats



Mantindre una ciberhigiene adequada i un sòlid sistema de protecció davant de les ciberamenaces és més necessari que mai

La situació provocada per l'epidèmia de COVID-19 ha mostrat amb absoluta claredat la dependència total dels sistemes d'informació i les comunicacions que hi ha actualment en la gestió pública, i això fa que les administracions públiques siguen més vulnerables davant dels ciberatacs que mai i ha posat en relleu que mantindre una ciberhigiene adequada i un sòlid sistema de protecció davant d'aquells és de vital importància.

No existeix cost zero en matèria de seguretat de la informació

És necessari un major compromís i conscienciació dels òrgans de govern dels ajuntaments amb la seguretat dels sistemes d'informació i les comunicacions, la qual cosa comporta inevitablement una major inversió econòmica i en recursos humans qualificats.

En la fase final de discussió dels esborranys d'informe amb els diferents responsables ens han manifestat, en general, la seua voluntat d'esmenar les deficiències de control observades. En alguns casos les han esmenades abans de l'emissió de l'informe. En el Programa Anual d'Actuació de 2020 es preveu expressament realitzar un informe de "seguiment de les 11 auditories dels controls bàsics de ciberseguretat el treball de camp de les quals s'ha realitzat en 2019 (una vegada transcorregut un any des de la seua finalització)". Raonablement, aquest seguiment tindrà continuïtat amb els quatre ajuntaments auditats en 2020.

NOTA

Aquest resum pretén ajudar a comprendre els resultats del nostre informe i facilitar la tasca als lectors i als mitjans de comunicació. Recomanem llegir-lo per a conéixer el veritable abast del treball realitzat.

ÍNDEX **Pàgina**

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

DPD: Delegat de protecció de dades

ENISA: European Union Agency for Cybersecurity

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de Gestió de Seguretat de la Informació

SIC: Sistemes d'informació i comunicacions

SIEM: Sistema de gestió d'informació i esdeveniments de seguretat

Ciberamenaça: Esdeveniments amb origen en internet que poden desencadenar un incident en l'organització i produir danys materials, pèrdues immaterials en els seus actius o la interrupció d'un servei.

Ciberhigiene: Conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia. A l'efecte d'aquest treball, aquest conjunt de pràctiques i accions bàsiques són els CBCS.

Ciberresiliència: És la capacitat d'un procés, negoci, organització o nació per a anticipar, resistir, recuperar-se i evolucionar per a millorar les seues capacitats davant de condicions adverses, estrés o atacs als recursos cibernètics que necessiten per a funcionar. En l'àmbit concret del sector públic, és la capacitat d'un ens públic per a evitar o resistir i recuperar-se d'un atac i continuar prestant els seus serveis en un temps raonable.

Ciberseguretat: És la capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o accions il·lícites o malintencionades que comprometen la disponibilitat, autenticitat, integritat i confidencialitat de les dades emmagatzemades o transmeses, així com dels serveis que aquestes xarxes i sistemes ofereixen o fan accessibles.

Declaració d'aplicabilitat: En l'àmbit de l'ENS, és el document en el qual es formalitza la relació de mesures de seguretat que són aplicables a un sistema d'informació, conforme a la seua categoria, i que es troben recollides en l'annex 2 del Reial Decret 3/2010.

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i han de descriure: *a*) l'ús correcte d'equips, serveis i instal·lacions, *b*) el que es considerarà ús indegut i *c*) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat ha d'estar a disposició de tots els membres de l'organització que necessiten conéixer-la, en particular d'aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, ha d'estar disponible en la intranet corporativa de l'entitat a través d'una adreça URL. La normativa de seguretat de cada entitat té l'origen i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i desplegant normativament la política de seguretat de l'entitat en qüestió, en segona instància.

Política de seguretat de la informació: És un document d'alt nivell que defineix què significa *seguretat de la informació* en una organització d'acord amb l'article 11 del Reial Decret 3/2010 i articula la gestió continuada de la seguretat. L'ha d'aprovar la junta de govern de l'ajuntament. Ha de ser accessible a tots els membres de l'organització i redactar-se de manera senzilla, precisa i comprensible. Convé que siga breu, deixant els detalls tècnics per a altres documents més precisos que ajuden a dur a terme el que s'hi proposa: normes de seguretat i procediments de seguretat.

Procediments de seguretat: Aborden tasques concretes i indiquen el que cal fer, pas a pas. Detallen de manera clara i precisa: *a*) com dur a terme les tasques habituals, *b*) qui ha de fer cada tasca i *c*) com identificar i reportar comportaments anòmals.

1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

L'article 6 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, inclou entre les seues funcions, a més de les referides al control extern de la gestió economicofinancera del sector públic valencià i dels seus comptes, aquelles que d'acord amb l'ordenament jurídic siguen convenients per a assegurar adequadament el compliment dels principis financers, de legalitat, d'eficàcia i d'economia i de transparència exigibles al sector públic, així com la sostenibilitat ambiental i la igualtat de gènere. D'altra banda, l'article 11 de la mateixa llei estableix que, en el desenvolupament de la seua funció fiscalitzadora, la Sindicatura de Comptes està facultada per a **verificar la seguretat i fiabilitat dels sistemes informàtics** que donen suport a la informació economicofinancera, comptable i de gestió.

En la guia d'auditoria *GPF-OCEX 5311 Ciberseguretat, seguretat de la informació i auditoria externa*, es destaca la importància creixent que les qüestions relacionades amb la ciberseguretat estan adquirint en la gestió de les administracions públiques, raó per la qual els auditors públics han de prestar cada vegada més atenció a aquestes qüestions. La Sindicatura no és indiferent davant d'aquesta problemàtica i en el Pla Estratègic de la Sindicatura de Comptes per al període 2019-2022 s'assenyala **la ciberseguretat com una de les àrees d'alt risc i prioritàries per a dur a terme la tasca fiscalitzadora**.

Considerant que les entitats locals no són alienes a la problemàtica plantejada per la ciberseguretat, i la seua proximitat als ciutadans, el Consell de la Sindicatura de Comptes va acordar incloure en els programes anuals d'actuació de 2019 i 2020 la realització d'un informe sobre els controls bàsics de ciberseguretat (CBCS) dels quinze ajuntaments més grans de la Comunitat Valenciana per a avaluar la seua preparació davant de l'actual situació de creixents ciberamenaces.

Després de publicar els quinze informes individuals corresponents a cada ajuntament, la Sindicatura ha considerat convenient fer el treball de compilació inclòs en aquest document. D'aquesta manera s'ofereix una visió de conjunt en què es destaquen les principals observacions realitzades.

L'entorn actual d'administració electrònica i els nous riscos tecnològics

Les lleis 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, i 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, representen la consolidació des del punt de vista jurídic de l'administració electrònica en totes les entitats públiques, i estableixen que la tramitació electrònica ha de constituir l'actuació habitual de les administracions, tant en les relacions amb tercers com entre

administracions i intraadministracions, i s'hi estableix el principi "digital per defecte".

Com a conseqüència de l'aplicació d'aquestes lleis, totes les entitats locals estan immerses en processos de transformació en la forma de prestació dels serveis als ciutadans i de la gestió pública, per a un desplegament ple de l'administració electrònica sustentada en sistemes d'informació cada vegada més complexos tecnològicament i interconnectats a través d'internet.

Els riscos per als sistemes d'informació que donen suport als processos de l'administració electrònica augmenten a mesura que les amenaces a la seguretat provinents del ciberespai evolucionen contínuament i apareixen atacs nous cada vegada més sofisticats i destructius que obliguen els ens públics a fer-los front de manera proactiva i sistemàtica, establint mecanismes de defensa que en el seu fonament s'articulen per mitjà de l'Esquema Nacional de Seguretat, d'aplicació obligatòria per a tot el sector públic.

La necessitat d'una ciberhigiene adequada

Els sistemes d'informació actuals són més complexos i estan més interconnectats que mai, però una major interconnexió origina més riscos de ciberseguretat, ocasiona una major probabilitat que es produïsca una pertorbació significativa en els sistemes d'informació de les entitats locals deguda a un ciberatac i, en conseqüència, una interrupció en els serveis prestats als ciutadans. Per aquesta raó, és imperatiu que els responsables dels ens públics gestionen els riscos associats amb el funcionament i ús de sistemes d'informació que utilitzen per a desenvolupar i prestar els serveis públics.

En l'escenari general descrit, la realitat del nostre entorn pròxim i de la resta de la societat espanyola i mundial en el moment d'elaborar aquest informe és la d'una crisi sanitària i socioeconòmica sense precedents provocada per l'epidèmia de COVID-19. Entre moltes altres qüestions, aquesta crisi ha posat de manifest que les administracions públiques han sigut capaces de mantindre gran part de la seua activitat confiant en el bon funcionament i l'eficàcia dels sistemes d'informació i comunicacions (SIC). Obligats pel confinament decretat pel Govern de la nació per a fer front a l'epidèmia, totes les administracions han recorregut al **treball en remot**, en les seues diferents modalitats tècniques, per a mantindre la seua activitat en nivells raonables. Aquest important salt qualitatiu, impensable en condicions normals, ha sigut possible gràcies a uns SIC àmpliament desenvolupats.

Al mateix temps, aquesta circumstància ha mostrat amb absoluta claredat la **total dependència dels SIC** que hi ha en la gestió pública, la qual cosa fa que les nostres administracions siguen més **vulnerables** davant dels ciberatacs i que **mantindre una ciberhigiene adequada i un sòlid sistema**

de protecció davant d'aquells siga més necessari que mai. La generalització del treball en remot té com a contrapartida de la seua eficiència un fort augment de la superfície d'exposició davant de les ciberamenaces, al qual han de fer front les entitats públiques amb les dificultats pròpies d'un període de crisi.

En aquests entorns actuals adquireix tot el sentit el concepte de ciberresiliència, que es pot entendre com la capacitat d'una entitat per a evitar o resistir i recuperar-se d'un ciberatac en un temps raonable per a continuar prestant els seus serveis.

Si el gran nombre de ciberatacs reeixits que es va produir en 2019 al nostre país s'haguera produït durant la crisi actual, les conseqüències haurien sigut nefastes en els ens atacats, ja que no haurien pogut desenvolupar ni activitat presencial ni de manera remota. **La ciberseguretat és hui un element essencial en els SIC**.

2. OBJECTIUS, ABAST I METODOLOGIA DE L'AUDITORIA

Objectius

L'objectiu general de l'auditoria ha sigut proporcionar una avaluació sobre el grau de ciberseguretat dels ajuntaments més grans de la Comunitat Valenciana, sobre el compliment de la normativa en matèria de seguretat dels sistemes d'informació i efectuar recomanacions per a l'adopció de mesures de ciberhigiene.

Amb aquesta finalitat, el treball d'auditoria ha consistit en:

- L'anàlisi del disseny i l'eficàcia operativa dels CBCS implantats en els ajuntaments auditats.

- La identificació de deficiències de control que puguen afectar negativament la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de les dades, la informació i els actius dels sistemes d'informació d'aquestes entitats.

- La determinació del nivell de maduresa existent en cada un dels CBCS i a nivell general en les diferents entitats auditades i els índexs de compliment respectius.

- La identificació d'incompliments significatius de la normativa sobre seguretat de la informació.

Atés el caràcter limitat de la revisió, l'objectiu no ha consistit a emetre una conclusió general sobre la confiança que mereixen els controls de ciberseguretat existents en el conjunt dels sistemes d'informació dels ajuntaments auditats. No obstant això, l'auditoria proporciona informació rellevant sobre el grau de ciberseguretat i ciberresiliència de les entitats i

sobre les possibles accions de millora, mesures de ciberhigiene, que haurien d'escometre per a esmenar les deficiències observades i aconseguir els nivells de maduresa establits com a objectius en les bones pràctiques i en l'ENS.

Àmbit subjectiu

Se han auditat els quinze municipis de més població (superior als 50.000 habitants) de la Comunitat Valenciana. En el quadre 1 es poden veure els ens auditats amb les dades de població i les obligacions reconegudes netes (ORN) de 2018, en milions d'euros.

Quadre 1. Ajuntaments auditats

Ajuntament	Població 2018	ORN 2018
València	791.413	1.046,1
Alacant	331.577	287,2
Elx	230.625	187,4
Castelló de la Plana	170.888	172,9
Torrevella	82.599	64,8
Torrent	81.245	52,7
Oriola	76.778	72,1
Gandia	73.829	92,9
Paterna	69.156	65,4
Benidorm	67.558	94,7
Sagunt	65.669	64,2
Alcoi	58.977	56,6
Sant Vicent del Raspeig	57.785	36,9
Elda	52.404	35,6
Vila-real	50.577	53,8
Ajuntaments auditats	**2.261.080**	**2.383,3**
Total ajuntaments CV	**4.963.703**	**4.917,0**
Cobertura de l'auditoria	**45,6%**	**48,5%**

Font: *Ministeri d'Hisenda. Liquidacions dels pressupostos de l'exercici 2018. Dades actualitzades 31/07/2019* (<https://serviciostelematicosext.minhap.gob.es/SGCAL/CONPREL>).
Les ORN són informació consolidada obtinguda de la liquidació de cada entitat local.

S'han aprovat quinze informes d'**auditoria dels controls bàsics de ciberseguretat** que estan publicats en el web de la Sindicatura. Aquest és un informe de síntesi que recull les conclusions de caràcter general que s'han pogut extraure després de realitzar aquestes auditories.

Àmbit objectiu

L'auditoria s'ha centrat en l'anàlisi de la situació dels huit CBCS definits en la *GPF-OCEX 5313 Revisió dels controls bàsics de ciberseguretat*:

CBCS 1 Inventari i control de dispositius físics

CBCS 2 Inventari i control de programari autoritzat i no autoritzat

CBCS 3 Procés continu d'identificació i solució de vulnerabilitats

CBCS 4 Ús controlat de privilegis administratius

CBCS 5 Configuracions segures del programari i maquinari

CBCS 6 Registre de l'activitat dels usuaris

CBCS 7 Còpies de seguretat de dades i sistemes

CBCS 8 Compliment normatiu

En l'apèndix es proporciona un major detall sobre aquests controls, els seus objectius de control i els subcontrols que els formen.

Ha sigut necessari delimitar i concretar quins sistemes s'havien d'analitzar, a causa de la naturalesa de l'objecte material a revisar, que comprén els sistemes d'informació i comunicacions d'un ens local de grans dimensions, amb la seua gran amplitud, complexitat i diversitat. En aquest sentit, de cada entitat hem analitzat les aplicacions informàtiques que donen suport a dos dels processos de gestió més rellevants als efectes de la Sindicatura, com ara la gestió comptable i pressupostària i la gestió tributària i recaptatòria.

A més, per la seua importància per al bon funcionament dels sistemes d'informació i la ciberseguretat, en cada ens hem analitzat també una selecció d'aquests tipus d'elements:

- controlador de domini
- programari de virtualització
- equips d'usuari
- elements de la xarxa de comunicacions (encaminador, *switches*, punt d'accés a xarxa wifi, etc.)
- elements de seguretat (tallafocs, IPS, *proxy* de correu, *proxy* de navegació, servidors d'autenticació, infraestructura de generació de certificats, etc.)

Àmbit temporal

L'àmbit temporal analitzat ha comprés el segon semestre de 2019 i el primer semestre de 2020. En l'apartat 9 de l'apèndix s'especifica quan es van donar per finalitzats els treballs en els diferents ajuntaments i a quina data es

refereixen, per tant, els indicadors i les situacions descrites en aquest i en el conjunt dels quinze informes individuals sobre els CBCS.

Metodologia

La Unitat d'Auditoria de Sistemes d'Informació de la Sindicatura de Comptes (UASI) ha realitzat aquesta auditoria dels controls bàsics de ciberseguretat (CBCS) seguint la metodologia establida en la guia pràctica de fiscalització *GPF-OCEX 5313 Revisió dels controls bàsics de ciberseguretat* i en la resta de les seccions aplicables del *Manual de fiscalització* de la Sindicatura de Comptes.

Hem avaluat la situació dels CBCS en les diferents entitats utilitzant el model de nivell de maduresa dels processos ja que, a més de ser un sistema àmpliament acceptat, permet establir objectius i realitzar comparacions de manera homogènia entre diferents entitats i també veure l'evolució al llarg del temps en una entitat. En aquest sentit, la Sindicatura té previst en el seu Programa Anual d'Actuació de 2020 fer un treball de seguiment de la situació i de la implantació de les recomanacions efectuades quan passe un any de la data de l'auditoria realitzada.

Els sistemes d'informació revisats estan classificats com de categoria de seguretat mitjana. Així, d'acord amb aquesta categoria**, el nivell de maduresa requerit per l'ENS i que també hem aplicat als CBCS en les auditories dels quinze ajuntaments és *N3, procés definit*** i un índex de maduresa del 80%. Aquest nivell exigeix que els processos estiguen estandarditzats, documentats i comunicats amb accions formatives. Això implica que es disposa d'un catàleg de processos que es manté actualitzat; que aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general; que hi ha normativa establida i procediments per a garantir la reacció professional davant dels incidents, i que s'exerceix un manteniment regular; que les oportunitats de sobreviure són altes, encara que sempre queda el factor d'allò desconegut (o no planificat). L'èxit és més que bona sort: es mereix.

La metodologia utilitzada està plenament alineada amb el que s'estableix en l'Esquema Nacional de Seguretat (ENS), que és d'aplicació obligatòria en tots els ens públics. En l'apèndix es proporciona un major detall sobre aquesta.

Com s'ha assenyalat abans, els resultats obtinguts en aplicar aquesta metodologia permeten formar una idea general de la situació dels controls de ciberseguretat als ajuntaments auditats, de la seua ciberresiliència i del grau de compliment d'una sèrie de disposicions legals molt importants en matèria de seguretat dels sistemes d'informació.

Els quinze informes individuals s'han sotmés al procediment contradictori per mitjà del tràmit d'al·legacions corresponent, tal com es recull en

aquells. En aquest informe es mostren els resultats comparatius de totes les entitats de manera sintètica.

Confidencialitat

Atés que la informació utilitzada en l'auditoria i els resultats detallats d'aquesta tenen un caràcter sensible i poden afectar la seguretat dels sistemes d'informació de les entitats revisades, les comunicacions d'informació sensible entre la Sindicatura i les entitats s'han realitzat per mitjà de canals xifrats, a fi de garantir així la integritat i confidencialitat de les dades. A més, la Sindicatura disposa de les polítiques, els procediments i els mecanismes necessaris per a garantir que aquesta informació únicament és accessible al personal encarregat de l'execució d'aquest treball.

Una vegada elaborats els diferents informes, els resultats al màxim nivell de detall s'han comunicat amb caràcter confidencial als responsables de cada entitat, a fi que puguen adoptar les mesures correctores que consideren necessàries per a reduir els riscos de seguretat.

3. CONCLUSIONS GENERALS

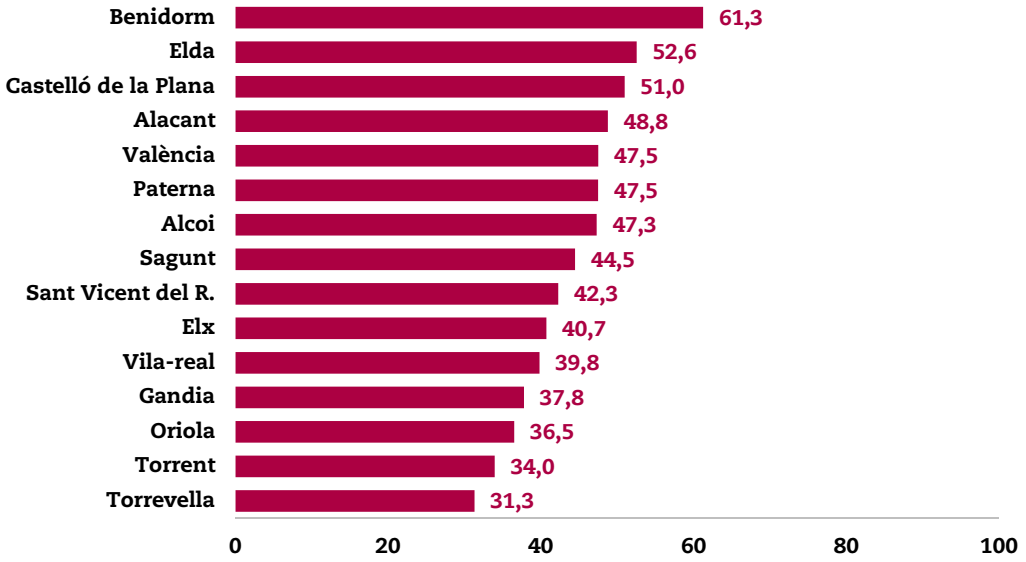
Les conclusions generals més rellevants que es dedueixen del treball realitzat són les que s'assenyalen a continuació:

a) La principal conclusió general és que **cap ajuntament auditat disposa d'un conjunt de controls de ciberseguretat que permeta protegir els seus sistemes d'informació de manera satisfactòria**, això és, al nivell exigit per l'ENS, ni compleixen de manera raonable la normativa relacionada amb la seguretat dels SIC.

L'índex de maduresa mitjà dels quinze ajuntaments és el 44,2%, i en tots els ajuntaments l'índex de maduresa global dels CBCS és inferior a l'objectiu requerit del 80%. Cap aconsegueix el nivell de maduresa N3 requerit. Per a interpretar correctament les dades cal tindre en compte que l'aprovat es correspon amb un índex de maduresa del 80%.

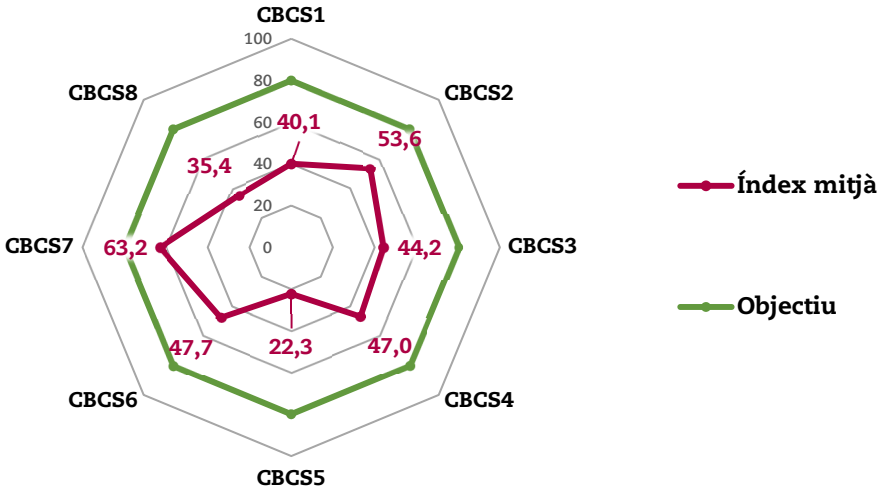
Els mals resultats obtinguts mostren que **els sistemes d'informació estan en risc davant de les amenaces de ciberseguretat** i que els ajuntaments han de millorar els controls per a gestionar la seguretat de la informació, garantir la continuïtat de la prestació dels serveis públics i fer front als ciberriscos.

Gràfic 1. Índex de maduresa general dels CBCS



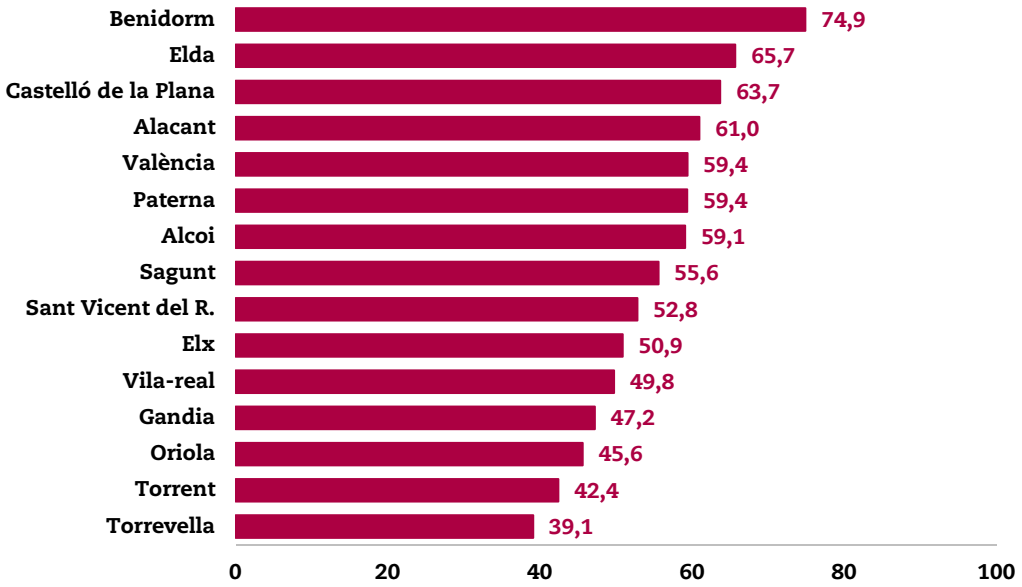
b) L'índex i el nivell de maduresa mitjà de tots els CBCS està per davall del 80% o nivell 3 requerit per l'ENS. Tal com es pot apreciar en el gràfic següent:

Gràfic 2. Índex mitjà de maduresa dels CBCS



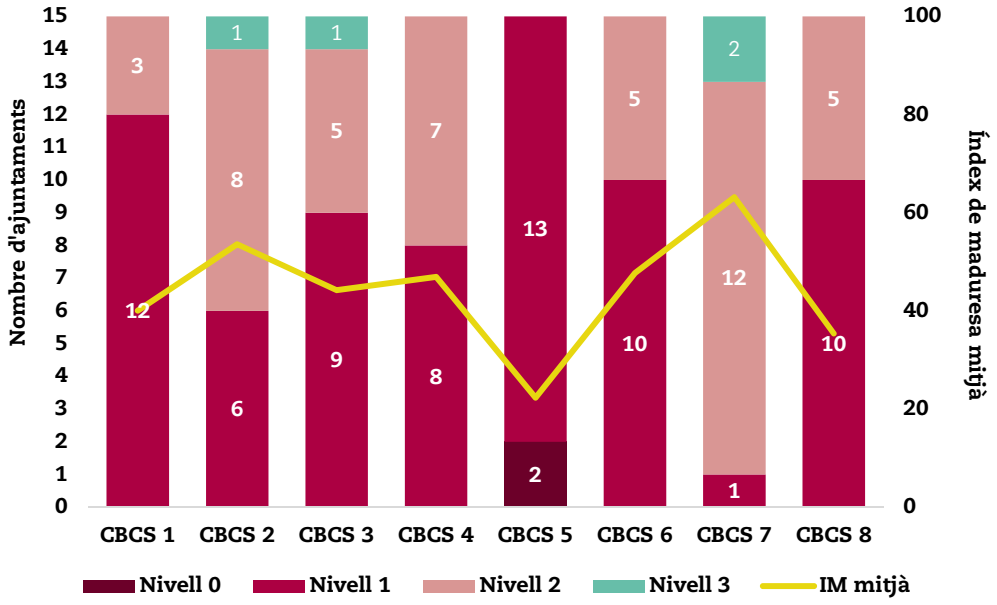
c) L'índex de compliment que resulta de comparar l'índex mitjà de maduresa dels CBCS (44,2%) amb l'objectiu del 80% és molt baix, i la mitjana general és un 55,1%. En el gràfic següent es pot veure l'índex de compliment de cada ajuntament respecte a l'objectiu exigit per l'ENS.

Gràfic 3. Índex de compliment dels CBCS



d) Hi ha deficiències de control significatives i generalitzades en molts dels subcontrols revisats.

Gràfic 4. Situació dels nivells de maduresa en els quinze ajuntaments

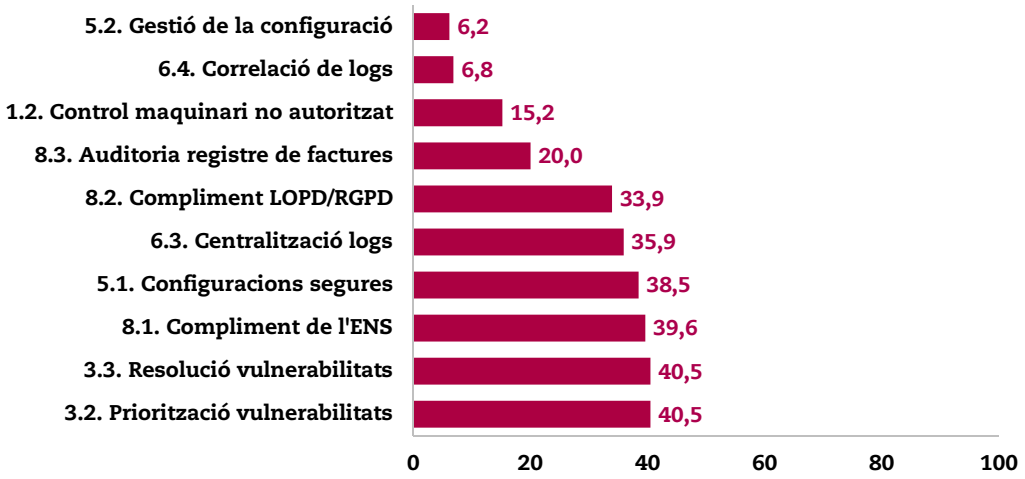


Només quatre d'un total de 120 CBCS revisats en els quinze ajuntaments aconsegueixen el nivell de maduresa mínim N3 (o índex de maduresa del 80%) establit com a objectiu en l'ENS. En el gràfic 4 es mostra aquesta informació de manera detallada.

És preocupant l'existència d'un nombre significatiu de subcontrols l'efectivitat dels quals és molt limitada. En l'apartat 5, "Resultats de l'auditoria", hi ha una descripció més detallada de les principals deficiències observades.

El gràfic següent mostra l'índex de maduresa dels deu subcontrols, d'un total de 26 revisats, amb els pitjors resultats obtinguts per al conjunt dels quinze ajuntaments auditats:

Gràfic 5. Els 10 pitjors resultats obtinguts



e) Hem observat, **en general, un nivell de compliment de la legalitat bastant insatisfactori**, tal com reflecteix l'índex mitjà de compliment del CBCS 8 del 44,2%, que recull el grau de compliment de diverses normes en matèria de seguretat dels sistemes d'informació.

Els màxims òrgans de direcció de les entitats locals tenen la responsabilitat de garantir un nivell adequat de compliment de les normes legals i han d'impulsar les mesures necessàries per a esmenar la deficient situació posada de manifest.

f) Es requereixen inversions sostingudes i un major compromís dels òrgans de govern amb la seguretat dels sistemes d'informació.

La necessària millora dels controls de ciberseguretat requereix actuacions i inversions, tant en mitjans materials com personals, que han de ser adequadament planificades i sostingudes en el temps, ja que cada vegada més serveis es presten utilitzant sistemes d'informació i cada vegada les amenaces provinents del ciberespai són més persistents i nocives.

Si no es prioritzen pressupostàriament els controls de seguretat i es reforça la capacitat de resiliència dels sistemes d'informació, les

entitats assumeixen riscos importants de pertorbacions en la prestació de serveis a la seua comunitat i es compromet la confidencialitat i integritat de la informació que posseeixen.

4. RECOMANACIONS GENERALS

Com a resultat de les auditories realitzades s'han efectuat una sèrie de recomanacions en els informes individuals. A més, les hem classificades en cada un d'aquests segons criteris combinats del risc potencial que cal mitigar amb cada una de les recomanacions i el cost estimat de la seua implantació. D'aquesta manera els responsables dels ajuntaments tenen una orientació per a establir accions correctores basades en criteris de cost/benefici. També s'assenyala en cada informe les mesures que s'han d'adoptar per al compliment de la legalitat.

Per a atendre aquestes recomanacions, els ajuntaments han de dedicar els esforços i recursos necessaris.

Les recomanacions generals més rellevants que es dedueixen del treball realitzat són les que s'assenyalen a continuació:

a) Totes les normes de seguretat i els procediments de seguretat dels sistemes d'informació i les comunicacions **han d'estar formalment aprovats** per l'òrgan superior de direcció de l'ajuntament.

A més, **aquesta normativa interna s'ha de dissenyar per a aplicar-la, no per a complir una formalitat**. El contingut del conjunt de polítiques, normes i procediments aprovat ha de ser una representació fidedigna i precisa del sistema de seguretat implantat per l'ajuntament.

Les polítiques de seguretat han de sintetitzar els objectius i articular la gestió continuada de la seguretat. Les normes han d'especificar l'ús correcte i les responsabilitats dels usuaris dels sistemes, i els procediments han de detallar de manera precisa les accions concretes que cal realitzar.

L'aprovació d'un marc normatiu que no satisfaça aquestes necessitats de contingut i que no represente la realitat de l'ajuntament esdevé un ús estèril de recursos per la falta d'efectivitat i una falsa percepció de compliment que pot comportar l'abandó d'altres mesures més adequades.

b) Hi ha d'haver un **major compromís dels òrgans de govern de l'ajuntament amb la ciberseguretat**. Això s'ha de reflectir en:

- La constitució d'òrgans de govern de seguretat formats per membres de totes les parts implicades i que faciliten la presa de decisions i instrumentalitzen determinades responsabilitats.

- El nomenament de rols de gestió de seguretat, a fi de concentrar i personalitzar les responsabilitats existents en les organitzacions.

- L'elaboració d'uns pressupostos econòmics i la dotació d'equips humans adequats a les exigències d'una ciberdefensa eficaç en els actuals entorns d'administració electrònica avançats.

- L'assimilació dels nous reptes i oportunitats que sorgeixen de l'administració electrònica, que modifiquen el paradigma tradicional de la gestió de serveis municipals, creen la necessitat de noves formes d'organització i gestió dels serveis, i que permeten una millora substantiva en l'aplicació dels principis d'eficàcia i eficiència.

- L'acceptació que la ciberseguretat no es troba constituïda únicament per un component tecnològic. **És una manera d'actuar**, de conduir-se en l'acompliment de les funcions dins de l'organització. En aquest sentit, els òrgans de govern tenen responsabilitat no sols en la formalització i adequació legal, sinó que han de ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat.

c) Tots els sistemes d'informació de l'ajuntament han d'estar governats per les mateixes polítiques i normes de seguretat. Amb caràcter general, han de tindre un responsable de seguretat únic i han d'estar sota el control i la supervisió del departament de TIC.

d) Sobre l'inventari i control de dispositius físics

Si bé moltes de les entitats auditades compten amb un inventari de maquinari actualitzat, la principal recomanació ha sigut que s'aprove un procediment que descriga les accions dutes a terme per a inventariar els elements i actualitzar aquest inventari.

L'inventari s'ha de mantindre sistemàticament actualitzat, utilitzant un procediment d'autorització per a l'alta de nou maquinari i un altre per a actualitzar les baixes.

D'altra banda, la principal mancança en aquest apartat ha sigut la falta de controls de connexió de dispositius físics no autoritzats a la xarxa corporativa. Aquesta mancança s'ha identificat com de risc i cost alts, la qual cosa implica que les entitats han de realitzar inversions per a implantar de manera efectiva aquest control.

e) Sobre l'inventari i control de programari autoritzat i no autoritzat

De manera similar a l'apartat anterior, s'ha evidenciat l'existència d'inventaris de programari actualitzat en moltes de les entitats

auditades. No obstant això, la principal recomanació ha sigut que s'ha d'aprovar formalment un pla de manteniment per al programari llicenciat.

Una altra de les recomanacions generalitzades ha sigut identificar i actualitzar tot el programari que està fora del període de suport, que s'ha considerat com a deficiència greu en quasi totes les entitats auditades. Aquesta recomanació implica risc i cost alts, per la qual cosa es requereixen inversions per a garantir els sistemes actualitzats.

f) Sobre el procés continu d'identificació i solució de vulnerabilitats

Una de les principals recomanacions relatives a aquest CBCS ha sigut que els ajuntaments han de dotar-se d'eines que faciliten la detecció i aplicació d'actualitzacions i pedaços de seguretat. S'ha recomanat a aquest efecte l'ús d'eines centralitzades de gestió de pedaços.

La no utilització d'aquestes eines implica un risc alt per a l'organització, que no té el control necessari sobre els dispositius i sistemes. L'establiment d'aquest tipus de sistemes pot suposar un cost moderat, però el risc disminueix considerablement.

A més, i per a aconseguir un control efectiu sobre les vulnerabilitats, es recomana l'ús d'eines d'escaneig i la realització de proves de *hacking* ètic o de penetració.

g) Sobre l'ús controlat de privilegis administratius

En aquest apartat, les entitats tenen un ampli marge de millora per mitjà de la implantació de certes mesures que suposen un cost baix per a l'organització, però que impliquen la disminució del risc de manera significativa.

Entre les recomanacions realitzades destaquem la necessitat d'eliminar l'ús d'usuaris genèrics, l'ús de permisos basats en la regla de mínims privilegis, canvi d'usuaris i contrasenyes per defecte i la implantació d'una política robusta de contrasenyes que s'aplique a tots els sistemes de l'entitat.

h) Sobre les configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors

La recomanació més freqüent ha sigut que els ajuntaments han d'establir i aprovar un procediment per a l'ús de guies de fortificació basades en les recomanacions dels fabricants i del Centre Criptològic Nacional.

Si bé la pràctica totalitat d'entitats revisades disposa de guies informals de configuració de certs sistemes, la seua elaboració no

considera com a objecte la consecució d'un determinat nivell de seguretat i la inclusió de mesures de seguretat en aquestes no es troba formalitzada. A més, en cas d'incloure configuracions específiques de seguretat, en general es basen únicament en l'experiència i els coneixements dels administradors i implantadors dels sistemes i no en les recomanacions de fabricants i organismes de referència.

i) Sobre el registre de l'activitat dels usuaris

Les principals recomanacions han sigut la formalització i aprovació d'un procediment de gestió de registres d'activitat i la seua centralització en sistemes específics per al seu tractament.

La configuració per defecte dels sistemes inclou en general l'habilitació dels registres d'activitat d'usuaris i administradors. No obstant això, la falta d'organització de la seua gestió i la dispersió en múltiples sistemes dificulten l'explotació de la informació i el seu aprofitament per a identificació d'esdeveniments i vulneracions de seguretat.

j) Sobre les còpies de seguretat de dades i sistemes

Hem recomanat quasi en la totalitat d'ajuntaments la realització de proves planificades de recuperació de les còpies de seguretat de dades i sistemes. La falta d'això impedeix garantir l'eficàcia completa del procés de gestió de còpies de seguretat, atés que en general només es realitzen recuperacions de dades d'usuaris a demanda.

k) Sobre el compliment normatiu

Cal adoptar les mesures necessàries per a donar compliment als diferents requeriments legals en matèria de seguretat de la informació.

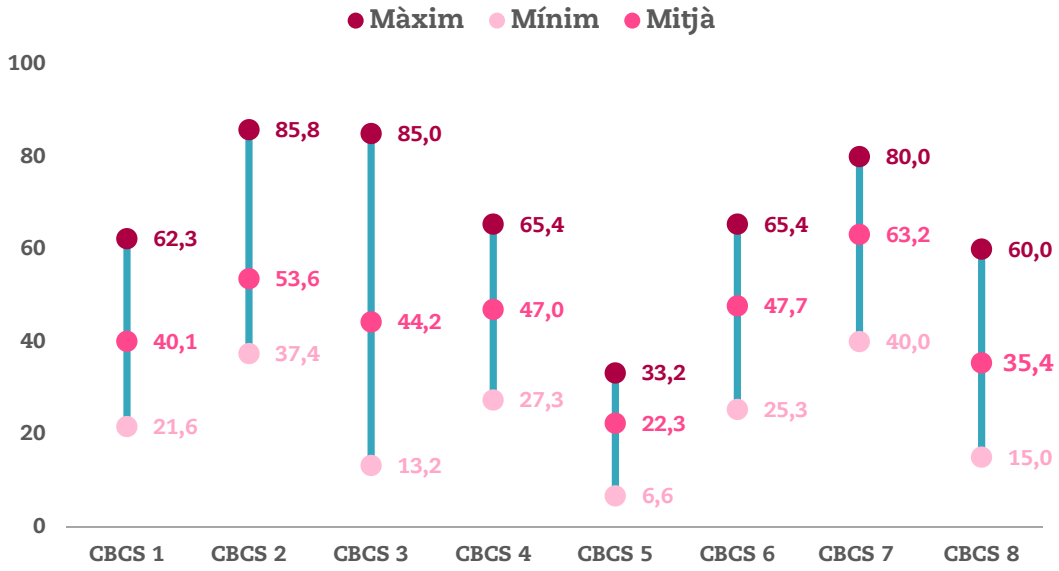
5. RESULTATS DETALLATS DE L'AUDITORIA

5.1 Consideracions generals

Hem constatat una falta generalitzada de procediments de seguretat i control formalment aprovats. D'acord amb la definició dels nivells del *model de maduresa*, per a aconseguir un nivell 3 de maduresa dels CBCS és requisit necessari l'existència de procediments formalment aprovats. En alguns casos hem constatat que hi ha procediments escrits que, encara que són formalment correctes, els han realitzat empreses externes i tenen poca o nul·la adaptació a l'entorn de l'ajuntament i no reflecteixen la realitat de les accions dutes a terme en la pràctica. En altres casos, el contingut dels procediments no detalla de manera clara i precisa les tasques que cal realitzar ni qui ha d'executar-les, i únicament s'especifica

el deure de realitzar l'acció, un aspecte que correspon a les normes de seguretat de rang superior, la qual cosa genera procediments ineficaços.

Gràfic 6. Dispersió dels resultats obtinguts dels índexs de maduresa dels CBCS



També hem observat una situació molt dispar en els quinze ajuntaments auditats, amb grans diferències en els resultats obtinguts, tal com es pot observar en el gràfic 6, que mostra la dispersió dels resultats obtinguts en els índexs de maduresa dels CBCS.

Aquesta disparitat de resultats es correspon amb la impressió rebuda durant el treball de camp. Encara que és comú el marc legal de compliment obligat, l'ENS, la realitat mostra que la percepció de la seguretat és molt dispar entre entitats, depenent d'aspectes com:

a) Els coneixements, experiències i perfils dels professionals que componen els departaments fiscalitzats.

b) El major o menor compromís dels màxims responsables dels ajuntaments amb la seguretat de la informació.

En analitzar les dades és interessant observar que, en el cas del CBCS 3, "Procés continu d'identificació i solució de vulnerabilitats", hi ha algun ajuntament que ha complit àmpliament els requeriments i excedeix en cinc punts l'objectiu del 80%, i no obstant això hi ha algun ajuntament en una situació molt deficient i només ha obtingut una valoració del 13,2%.

Particularment rellevant, pels riscos derivats de la seua deficiència, és l'insuficient nivell del CBCS 4, "Ús controlat de privilegis administratius", per al qual únicament un cas supera l'índex de maduresa del 60%, molt

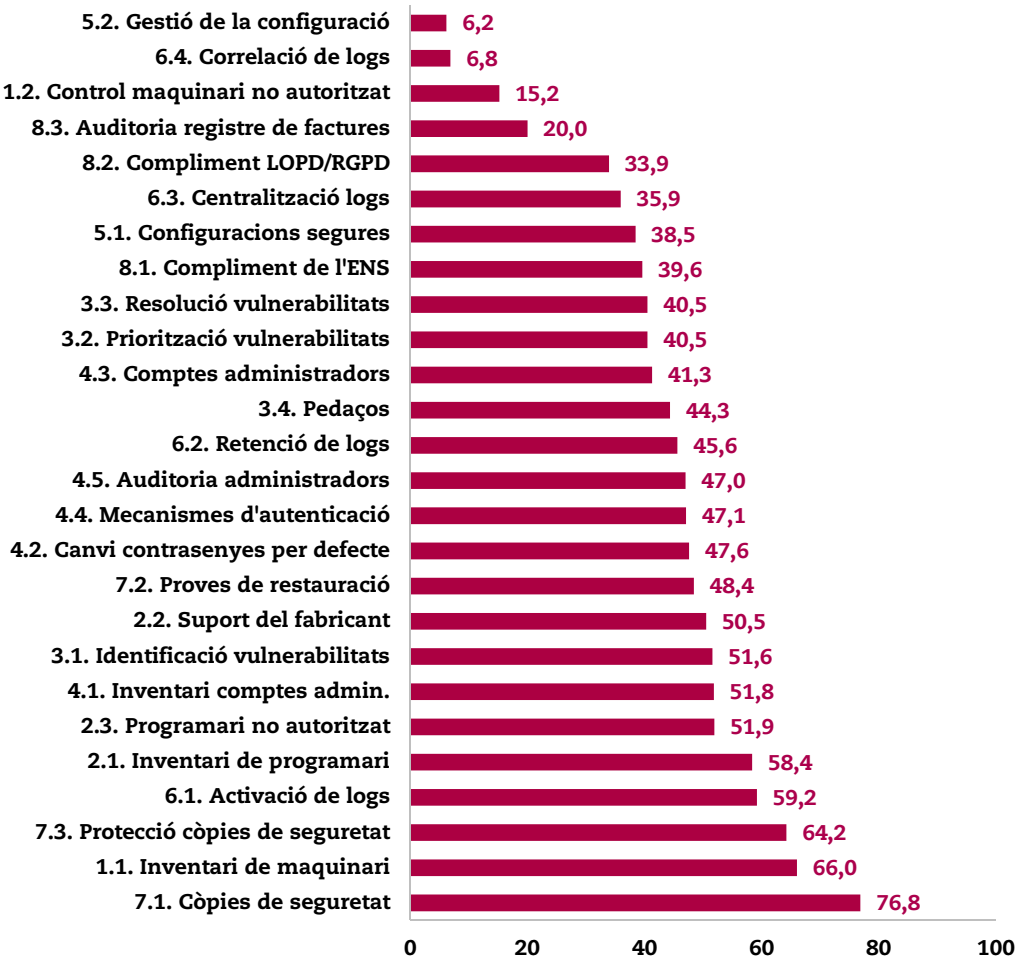
inferior al nivell requerit. En el curs del treball detallat hem constatat que el control no sols ofereix una certa dispersió entre ajuntaments, sinó també entre sistemes d'un mateix ajuntament, ja que en els casos en què existeix un procés de control adequat, en general, mai és considerat de manera integral per a tots els sistemes de l'entitat, i això limita la seua efectivitat i el nivell de maduresa.

També s'observa que en el cas del CBCS 5, "Configuracions segures del maquinari i programari", els resultats han sigut molt deficients en tots els casos. En general, no hi ha procediments específics establits a fi de conferir a les configuracions un nivell determinat de seguretat, i la limitada eficàcia dels controls existents depén quasi exclusivament dels coneixements tècnics del personal del departament.

Finalment, s'observa que el CBCS 7, "Còpies de seguretat de dades i sistemes", és el que ha obtingut la millor valoració mitjana de tots els CBCS analitzats.

Analitzant els resultats obtinguts amb un major grau de detall, podem veure en el gràfic 7 l'índex de maduresa mitjà obtingut per a cada un dels 26 subcontrols que s'han analitzat en els quinze ajuntaments.

Gràfic 7. Índexs de maduresa dels mitjans dels subcontrols



S'observa que en cap subcontrol l'índex mitjà de maduresa aconsegueix l'objectiu del 80%.

De l'anàlisi dels subcontrols amb majors nivells de maduresa podem extraure les reflexions següents:

- Dos dels subcontrols millor valorats corresponen a processos d'inventari d'actius, tant físics com elements de programari. En la major part dels ens auditats es fa ús d'una eina (GLPI/OCS Inventory) per a la gestió automatitzada d'aquests inventaris. L'ús d'aquesta eina ha sigut promogut i facilitat per les diputacions provincials. Els organismes d'assistència i coordinació externs, com les diputacions, exerceixen una acció positiva per a aconseguir majors nivells d'eficàcia sobre el compliment de determinats controls.

- Dos subcontrols corresponents a la gestió de còpies de seguretat aconsegueixen els nivells de maduresa més elevats. Aquest resultat

ens permet evidenciar que les entitats prioritzen l'aplicació de mesures de recuperació, de cost de gestió mitjà/baix, enfront de controls preventius i detectius amb més cost d'implantació i gestió.

D'altra banda, hi ha tres subcontrols amb un índex de maduresa molt deficient. Els tres presenten un perfil semblant, ja que són tècnicament complexos i requereixen un gran esforç de recursos per a aconseguir l'efectivitat. Per consegüent, ofereixen una relació cost/benefici molt reduïda, la qual cosa limita la seua implantació en entorns d'escassos mitjans personals i pressupostaris. A més, dos d'aquests tres subcontrols són detectius, més complexos que els preventius. L'únic subcontrol preventiu (la gestió de la configuració) també és tècnicament complex i sol estar reemplaçat per compensatoris tècnicament simples, però d'efectivitat limitada.

Altres observacions generals sense impacte directe en els indicadors calculats

A més de les deficiències específiques per a cada CBCS que s'assenyalen en els apartats següents, hi ha algunes consideracions de caràcter general que no tenen un impacte directe en la quantificació dels indicadors de maduresa utilitzats, però que per la seua importància interessa destacar:

- Hem observat en diversos ajuntaments l'existència de departaments/zones de la xarxa que realitzen la seua pròpia gestió del sistema d'informació, de manera independent del departament TIC. Si bé aquestes organitzacions descentralitzades es trobaven previstes en la normativa interna, la descentralització en la gestió dificulta l'aplicació homogènia de mesures de seguretat, imposa al responsable de seguretat, si n'hi ha, un esforç addicional de coordinació i incrementa els riscos de control.

- Hem constatat diversos casos d'aplicacions certificades en l'ENS com de nivell de seguretat alt amb deficiències de control significatives (nombre excessiu d'usuaris administradors, falta de doble factor d'autenticació, etc.).

- En molts casos, a pesar de l'aplicació de determinades mesures de seguretat, no es pot considerar que hi haja un sistema de gestió de seguretat de la informació (SGSI), atés que el conjunt de mesures, accions i procediments implantats no es troben coordinats i gestionats a fi d'aconseguir objectius definits.

- S'aprecia en la majoria dels casos una falta en l'ús d'eines adequades per a la gestió dels procediments de seguretat implantats, que poden ser adequadament suportats per eines de cicle de treball (*workflow*) i BPM (gestió de processos de negoci). Aquesta insuficiència dificulta la consideració dels controls implantats com a gestionats i impedeix aconseguir un nivell de maduresa N3.

- Hem observat que, a pesar de l'existència de normativa, com l'ENS, que actua com a element normalitzador de la seguretat, la percepció sobre els processos crítics de seguretat que s'han d'establir és molt dispar entre entitats, i això comporta una implantació desigual de determinats controls o mesures de seguretat rellevants.

- S'ha evidenciat el desconeixement en moltes de les entitats sobre processos de seguretat, controls, solucions o eines que proporcionen resposta a determinats problemes comuns a tots els ens. L'existència de casos d'èxit en molts dels subcontrols revisats evidencia la necessitat de coordinació entre entitats i l'establiment de sinergies que permeten compartir solucions efectives a problemes col·lectius. Aquesta tasca hauria de ser impulsada per les diputacions provincials.

En els apartats següents es detalla la situació dels controls bàsics de ciberseguretat en els quinze ajuntaments auditats.

5.2 CBCS 1. Inventari i control de dispositius físics

Objectiu del control

Gestionar activament (inventariar, revisar i corregir) tots el dispositius de maquinari connectat en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.

Per què és important aquest control bàsic de ciberseguretat

La finalitat del control és conéixer el que hi ha connectat a la xarxa perquè es puga defensar i, posteriorment, impedir que dispositius no autoritzats es connecten a la xarxa. Aquest control ajuda les organitzacions a definir la base del que cal defensar, ja que si es desconeix quins dispositius hi ha connectats no es poden defensar.

L'òrgan competent ha d'aprovar formalment un procediment que especifique les accions que cal realitzar per a mantindre actualitzat l'inventari de tot el maquinari de l'entitat, que incloga aspectes com la realització periòdica de revisions i la descripció de les mesures implantades per a impedir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

L'inventari ha de ser tan complet com siga possible. En organitzacions amb un nivell de maduresa bàsic, l'inventari es pot realitzar i mantindre amb procediments manuals i, en altres més madures, utilitzant eines d'escaneig que detecten els dispositius connectats a la xarxa corporativa.

Hi ha d'haver en tota la xarxa corporativa un control efectiu que impedisca l'accés a qualsevol dispositiu físic no autoritzat. És més probable que les màquines no controlades estiguen executant programari que no siga

necessari per a les finalitats de l'entitat (introduint possibles vulnerabilitats de seguretat) o executant programari maliciós introduït per un atacant després que un sistema ha sigut compromés.

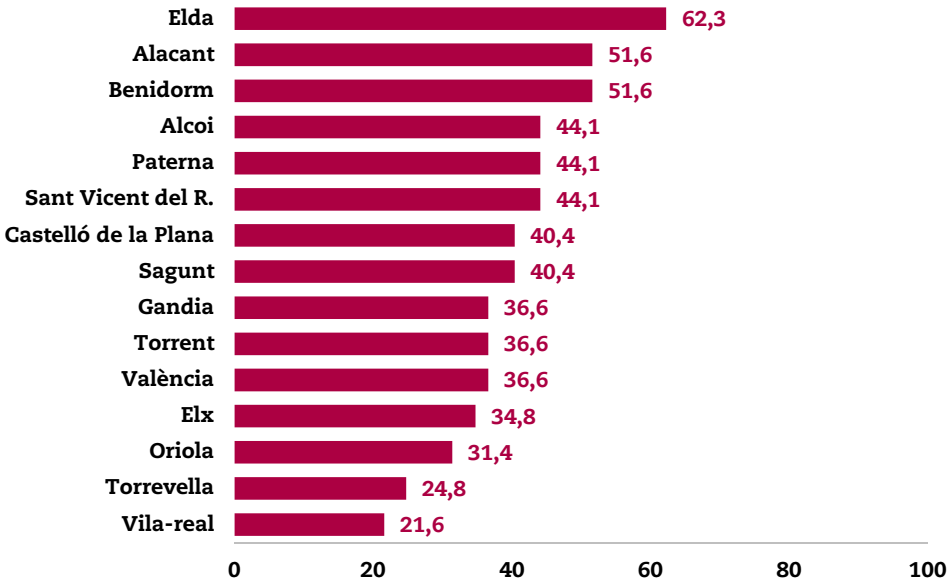
Altres dispositius que es connecten a la xarxa corporativa (per exemple, sistemes per a demostracions, xarxes per a convidats, etc.) s'han de gestionar amb cura o aïllats per a previndre accessos no autoritzats que comprometen la seguretat.

Els dispositius personals dels empleats (portàtils, tauletes, mòbils) que es connecten a la xarxa corporativa també es poden veure compromesos i ser usats per a infectar els recursos interns.

Situació del control als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 1 en els quinze ajuntaments revisats. Només tres ajuntaments aconsegueixen el nivell de maduresa N2, *repetible, però intuïtiu (50%)*, i cap el nivell N3 (80%) requerit per l'ENS.

Gràfic 8. Índexs de maduresa del CBCS 1



Principals deficiències observades

Les principals deficiències relacionades amb l'inventari i el control de dispositius físics autoritzats i no autoritzats han sigut:

- Absència de un procediment formalment aprovat per a la gestió de l'inventari i el control d'actius físics, que incloga les revisions periòdiques de maquinari (tretze casos).

- L'inventari de maquinari existent no està degudament actualitzat o no preveu tot el maquinari de l'entitat (tres casos).

- Els controls per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa són inefectius o inexistents (catorze casos).

5.3 CBCS 2. Inventari i control de programari autoritzat i no autoritzat

Objectiu del control

Gestionar activament (inventariar, revisar i corregir) tot el programari en la xarxa, de manera que només es puga instal·lar i executar programari autoritzat i que el no autoritzat siga detectat i s'evite la seua instal·lació i execució.

Per què és important aquest control bàsic de ciberseguretat

La finalitat d'aquest control és assegurar que només s'executa programari autoritzat en els sistemes de l'organització, de manera que s'impedeix l'execució de programari potencialment vulnerable.

Mantindre un inventari actualitzat de programari és important, ja que permet conéixer què cal protegir. Per exemple, el control de tot el programari existent exerceix un paper fonamental en la planificació i execució de còpies de seguretat i en la recuperació del sistema. Sense el coneixement o el control apropiats dels programes desplegats en una organització, els defensors no poden assegurar adequadament els seus actius. Les organitzacions que no tenen inventaris complets de programari no poden trobar quin és el vulnerable o maliciós per a mitigar problemes o eliminar els atacants.

D'altra banda, disposar d'una llista blanca d'aplicacions autoritzades limita la capacitat d'executar únicament aquelles que estan expressament autoritzades. Aquest control sovint es considera un dels més eficaços per a la prevenció i detecció de ciberatacs. La implementació del control sovint requereix que les organitzacions reconsideren les seues polítiques i la seua cultura, ja que els usuaris ja no podran instal·lar el programari que desitgen.

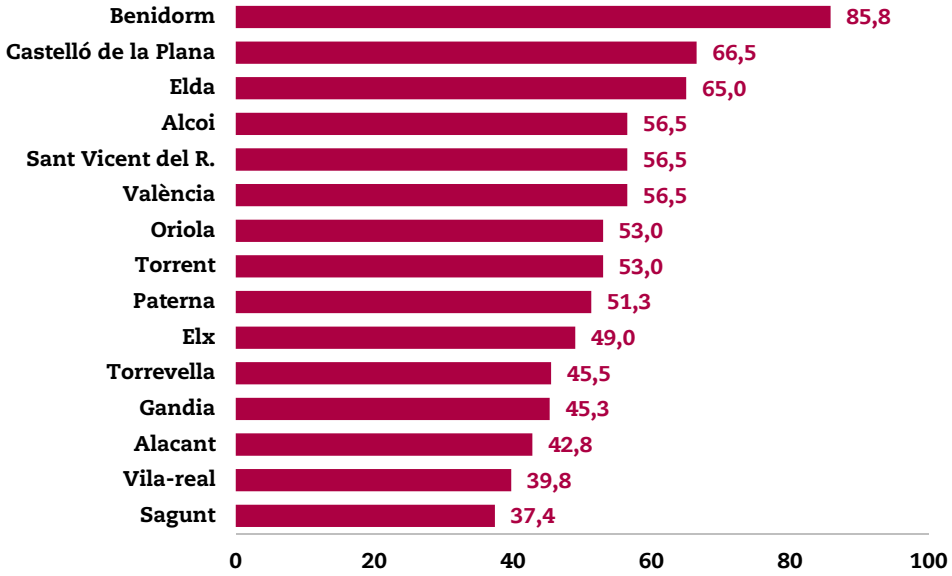
L'aplicació de pedaços i actualitzacions en el programari inventariat i controlat permet a les entitats eliminar les vulnerabilitats o reduir els riscos derivats de la materialització de les amenaces. Perquè el procés d'actualització i pedaços siga possible, és necessari que l'entitat complisca els requisits següents: els programes utilitzats han de trobar-se en un estat del seu cicle de vida que permeta l'alliberament d'actualitzacions del fabricant, les llicències de programari comercial han de trobar-se actives, i aquell que ha sigut adaptat i implantat específicament per a l'entitat ha de trobar-se suportat per contractes de manteniment amb les empreses corresponents.

Les entitats han de disposar d'un procediment que descriga la gestió de l'inventari, que incloga totes les aplicacions i identifique els seus responsables. A més, cal realitzar revisions periòdiques dels programes, que han de ser documentades. L'efectivitat del control és producte d'un inventari de programari actualitzat, juntament amb una llista blanca d'aplicacions permeses i la implantació de les mesures necessàries per a bloquejar qualsevol aplicació no inclosa dins d'aquesta llista.

Situació del control als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 2 en els quinze ajuntaments revisats. Només un ajuntament aconsegueix el nivell de maduresa N3 (80%) requerit per l'ENS.

Gràfic 9. Índexs de maduresa del CBCS 2



Principals deficiències observades

Les principals deficiències relacionades amb l'inventari i el control de programari autoritzat i no autoritzat han sigut:

- Absència de un procediment formalment aprovat que considere de manera integral el control i la gestió de tot el programari, per mitjà de l'aprovació d'una llista blanca de programari autoritzat, revisions periòdiques i que descriga les mesures implantades per a impedir l'execució del no autoritzat (catorze casos).

- Inexistència de plans de manteniment per a la gestió del suport de tot el programari utilitzat en l'entitat (quinze casos).

- Les mesures per a impedir l'execució de programari no autoritzat o són inexistents o no són efectives (tres casos).

- Existeix un nombre significatiu d'equips amb programari fora del període de suport per part del fabricant (dotze casos).

5.4 CBCS 3. Procés continu d'identificació i solució de vulnerabilitats

Objectiu del control

Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.

Per què és important aquest control bàsic de ciberseguretat

La finalitat d'aquest control és conéixer i eliminar febleses tècniques que hi ha en els sistemes d'informació de l'organització, a fi de reduir la probabilitat que els sistemes continuen sent vulnerables.

Les entitats han de comptar amb un pla de manteniment de l'equipament físic i lògic, que detalle els components que cal revisar i els responsables. Cal especificar el seguiment continu d'anuncis de defectes publicats pels fabricants i documentar les accions dutes a terme per a analitzar, prioritzar i determinar quan s'han d'aplicar les actualitzacions de seguretat, pedaços, millores i noves versions, tenint en compte el risc que pot implicar aquest canvi.

Les organitzacions han d'implementar eines que centralitzen i automatitzen el procés de gestió de vulnerabilitats, actualitzacions i pedaços, per a dotar-se de la capacitat de detectar i solucionar debilitats de programari explotable.

Les organitzacions capdavanteres implementen eines especialitzades en l'escaneig i gestió de vulnerabilitats de seguretat. Això permet detectar-les en els diferents sistemes de manera automàtica, contínua i proactiva i facilita la instal·lació d'actualitzacions i pedaços per a solucionar les vulnerabilitats existents.

Els ciberdefensors han d'operar amb un flux constant d'informació nova: actualitzacions de programes, pedaços, avisos de seguretat, butlletins d'amenaces, etc. La comprensió i gestió de les vulnerabilitats s'ha convertit en una activitat contínua que requereix temps, atenció i recursos significatius. Els atacants tenen accés a la mateixa informació i poden aprofitar les bretxes entre l'aparició de nous coneixements i la seua solució. Per exemple, quan els investigadors reporten noves vulnerabilitats, comença una carrera entre totes les parts que inclou atacants (per a "armar-se", desplegar un atac i explotar-lo), proveïdors (per

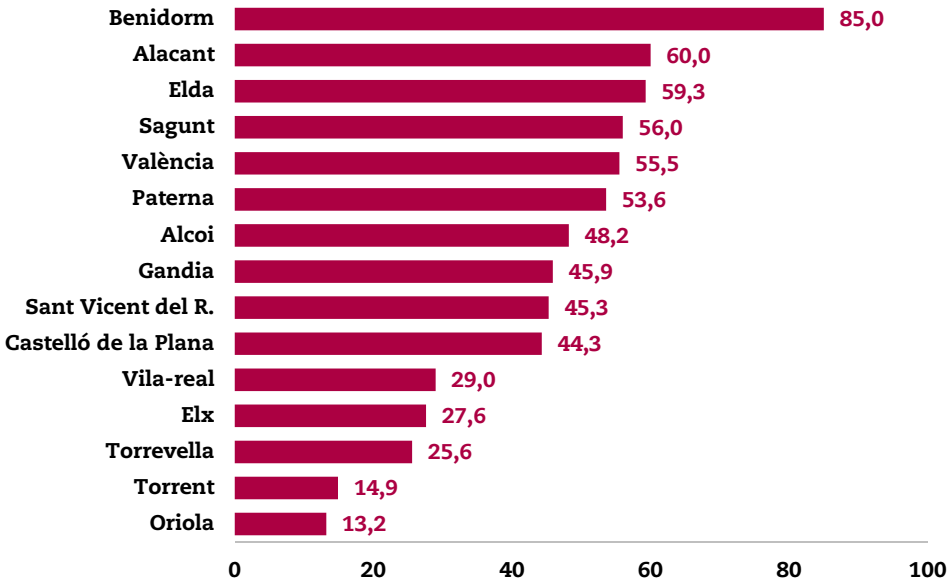
a desenvolupar, implementar pedaços o signatures i actualitzacions) i defensors (per a avaluar riscos, pedaços de prova, i instal·lar-los).

Les organitzacions que no escanegen les vulnerabilitats i aborden de manera proactiva els defectes trobats s'enfronten a una alta probabilitat que els seus sistemes informàtics siguen compromesos.

Situació del control als ajuntaments revisats

En el gràfic 10 es mostren els índexs de maduresa del CBCS 3 en els quinze ajuntaments revisats. Només un ajuntament aconsegueix el nivell de maduresa N3 (80%) requerit per l'ENS.

Gràfic 10. Índexs de maduresa del CBCS 3



Principals deficiències observades

Les principals deficiències relacionades amb el procés d'identificació i solució de vulnerabilitats han sigut:

- Absència de un procediment formalment aprovat per a la identificació, priorització, resolució i pedaços de les vulnerabilitats detectades (tretze casos).

- Els equips d'usuari no s'actualitzen ni reben pedaços de seguretat (tres casos).

- No existeix gestor de pedaços i actualitzacions de programari o la gestió no està correctament implantada (huit casos).

- Absència d'eines per a realitzar escanejos periòdics a la recerca de vulnerabilitats en la xarxa (dotze casos).

5.5 CBCS 4. Ús controlat de privilegis administratius

Objectiu del control

Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'ús, assignació i configuració de privilegis administratius en ordinadors, xarxes i aplicacions.

Per què és important aquest control bàsic de ciberseguretat

Aquest control garanteix que els privilegis d'administració dels sistemes estiguen assignats únicament als empleats que els necessiten, sobre la base de les funcions que exerceixen (principi de mínim privilegi), i que l'entitat puga atribuir les accions administratives a usuaris identificables (traçabilitat).

Desafortunadament, per a facilitar l'agilitat i la comoditat, moltes organitzacions permeten que el seu personal tinga drets d'administrador tant a escala d'una aplicació de gestió com en els sistemes que li donen suport (sistema operatiu, base de dades, etc.), així com en els seus equips. Aquesta situació deriva en l'existència del risc d'accés i de canvis no autoritzats als sistemes i dades, que pot materialitzar-se utilitzant els privilegis excessius d'un usuari com a porta d'entrada per a accedir des de fora a la xarxa interna de l'entitat.

Aquest control comporta que els comptes d'usuaris administradors d'aplicacions, bases de dades, sistemes operatius i equips d'usuari han d'estar identificats i el seu ús, controlat, s'han d'eliminar les que no s'utilitzen i s'han de canviar les que estan definides per defecte. A més, han de complir la política de fortalesa de contrasenyes.

L'ús inadequat de privilegis administratius és un mètode primari perquè els atacants es propaguen dins d'una entitat objectiu. Hi ha tècniques d'atac molt comunes que aprofiten els privilegis administratius incontrolats. Per exemple, un usuari administrador del seu equip obri un adjunt de correu electrònic maliciós, descarrega i obri un arxiu d'un lloc web maliciós o simplement navega en un lloc web que allotja contingut de l'atacant que pot explotar automàticament navegadors. L'arxiu o *exploit* conté codi executable que s'activa en l'equip de la víctima, ja siga automàticament o enganyant l'usuari perquè execute el seu contingut. Si la víctima té privilegis administratius, l'atacant pot apoderar-se completament de la seua màquina i instal·lar els registradors de tecles, els detectors o *sniffers* i el programari de control remot per a trobar contrasenyes administratives i altres dades sensibles. A més, l'atacant és capaç d'accedir a tots els recursos compartits de la víctima

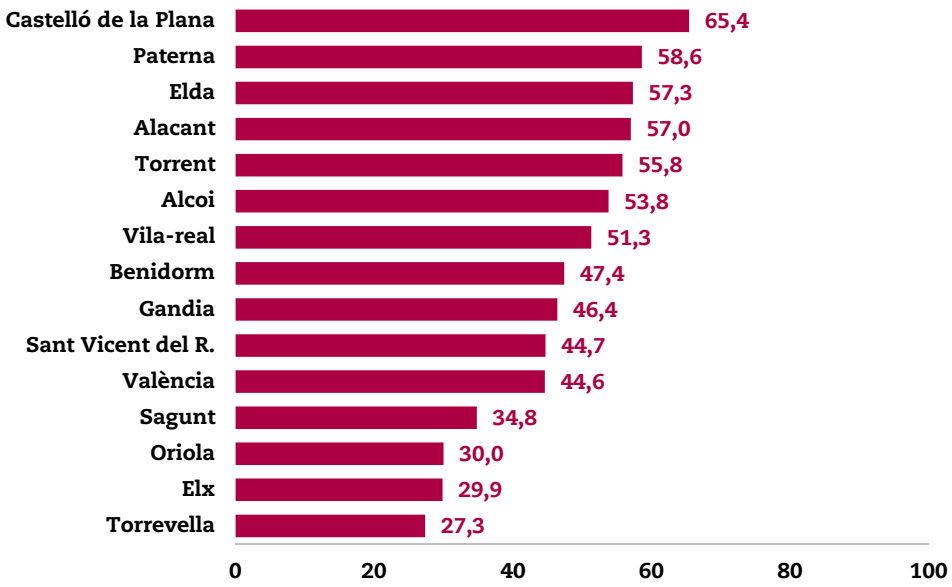
Si els privilegis administratius es distribueixen de manera ampla, o són idèntics a les contrasenyes utilitzades en sistemes menys crítics o a les que venen d'origen per defecte, a l'atacant li costa molt menys prendre el control total dels sistemes, perquè hi ha molts més comptes que poden actuar com a vectors de penetració.

En conseqüència, les entitats han de disposar d'un procediment formalment aprovat que descriga les accions dutes a terme per a la gestió dels seus usuaris administradors, que complisca una sèrie de bones pràctiques per a garantir l'efectivitat del control, entre les quals cal destacar l'assignació d'usuaris nominatius, permetre la traçabilitat de les accions, el canvi de comptes i contrasenyes per defecte i una política robusta de contrasenyes que s'aplique de manera homogènia a tots els dispositius i sistemes que componen el sistema d'informació.

Situació del control als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 4, "Ús controlat de privilegis administratius", en els quinze ajuntaments revisats. Només set ajuntaments aconsegueixen el nivell de maduresa *N2, repetible, però intuïtiu* (50%), i cap el nivell N3 (80%) requerit per l'ENS.

Gràfic 11. Índexs de maduresa del CBCS 4



Principals deficiències observades

Les principals deficiències relacionades amb l'ús controlat dels comptes d'administració dels sistemes han sigut:

- Absència de un procediment formalment aprovat per a la gestió d'usuaris amb privilegis d'administració que s'aplique a tots els sistemes de l'entitat (dotze casos).

- Existència d'usuaris no nominatius amb privilegis d'administració en els diferents sistemes, que impedeix la traçabilitat de les accions en cas d'incidents de seguretat (deu casos).

- Sistemes i dispositius amb els usuaris i contrasenyes per defecte (set casos).

- Nombre excessiu d'usuaris administradors o d'usuaris amb privilegis d'administració sobre els seus equips (dos casos).

- Els administradors de sistemes no utilitzen diferents comptes amb diferents nivells de seguretat depenent de les tasques que cal realitzar (tasques d'administració del sistema o tasques ofimàtiques que no requereixen privilegis administratius), de manera que s'incompleix així la regla de la mínima funcionalitat (nou casos).

- Inexistència de una política robusta de contrasenyes que s'aplique a tots els dispositius i sistemes, o si existeix no està aplicada correctament (sis casos).

5.6 CBCS 5. Configuracions segures del maquinari i programari de dispositius mòbils, portàtils, equips de taula i servidors

Objectiu del control

Establir una configuració base segura per a dispositius mòbils, portàtils, equips de taula i servidors, i gestionar-la activament utilitzant un procés de gestió de canvis i configuracions rigorós, per a previndre que els atacants exploten serveis i configuracions vulnerables.

Per què és important aquest control bàsic de ciberseguretat

Per defecte, la majoria dels sistemes estan configurats per a facilitar el seu ús i no necessàriament pensant en la seguretat. Tal com l'entreguen els fabricants i venedors, quan es rep un equip és habitual trobar-se amb controls poc robustos, serveis i ports oberts, comptes o contrasenyes predeterminats, protocols antics, programari preinstal·lat innecessari. Tots aquests aspectes són vulnerables en el seu estat predeterminat.

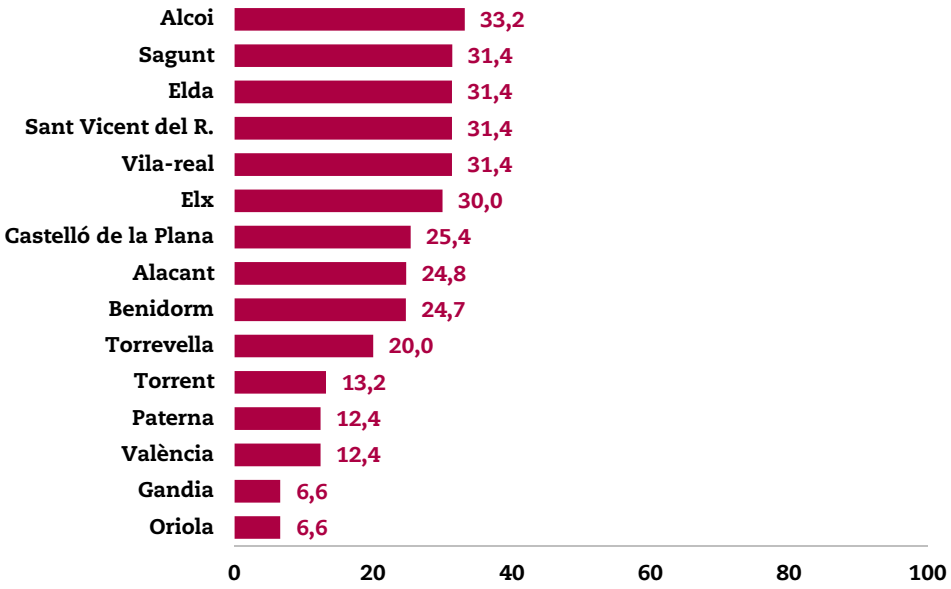
Per a implantar de manera efectiva aquest control, les organitzacions necessiten reconfigurar els sistemes d'acord amb estàndards de seguretat. El desenvolupament d'opcions de configuració amb bones propietats de seguretat no és una tasca senzilla, va més enllà de la capacitat dels usuaris individuals i requereix anàlisis a vegades complexes i costoses per a prendre bones decisions. Per aquesta raó, és altament recomanable el seguiment i l'aplicació de bones pràctiques que alguns organismes publiquen en matèria de seguretat, aplicables a dispositius i sistemes.

Fins i tot si es desenvolupa i s'instal·la una configuració inicial forta, s'ha de revisar i actualitzar contínuament per a evitar la deterioració de la seguretat, en particular quan el programari s'actualitza o es posen pedaços, es divulguen les noves vulnerabilitats de la seguretat o les configuracions s'"ajusten" per a permetre la instal·lació de nous programes o per a donar suport a nous requeriments operacionals. Si no es revisa i s'actualitza de manera contínua, els atacants trobaran oportunitats per a explotar tant el programari com els serveis accessibles a la xarxa.

Situació del control als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 5 en els quinze ajuntaments revisats. Cap ajuntament aconsegueix el nivell de maduresa *N2, repetible, però intuïtiu* (50%). Els resultats obtinguts en aquest important CBCS són molt deficients en tots els casos.

Gràfic 12. Índexs de maduresa del CBCS 5



Principals deficiències observades

Les principals deficiències detectades relacionades amb la configuració segura del maquinari i del programari han sigut:

- Absència de procediments formalment aprovats per a la aplicació de configuracions segures a dispositius i sistemes, considerant la seguretat per defecte i el criteri de mínima funcionalitat (catorze casos).

- En els casos en què es disposa de plantilles per a la configuració de determinats dispositius i sistemes, aquestes no tenen caràcter de fortificació, ni la configuració segura d'aquests dispositius es troba formalment establida (set casos).

- Absència de mecanismes que garantisquen un monitoratge efectiu de canvis no autoritzats en la configuració en els sistemes crítics de l'entitat (quinze casos).

5.7 CBCS 6. Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria)

Objectiu del control

Recollir, gestionar i analitzar *logs* d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.

Per què és important aquest control bàsic de ciberseguretat

Implica que tots els sistemes i aplicacions haurien de tindre habilitades les traces d'auditoria, incloent-hi respostes a des d'on, qui i quan s'ha realitzat una determinada acció, com també tindre definides actuacions d'alerta.

En organitzacions amb pressupost i personal suficient se sol disposar d'un SIEM (sistema de gestió d'incidències i informació de seguretat), un sistema que, a més de centralitzar registres d'auditoria i disposar en temps real d'alertes de seguretat, és capaç de relacionar esdeveniments de seguretat dels diferents dispositius.

En l'actualitat, tots els sistemes operatius, serveis i dispositius de xarxa ofereixen capacitats de *log*, però aquests registres han de ser correctament configurats per a emmagatzemar tota la informació disponible i permetre'n l'anàlisi posterior. En són un exemple els servidors, que han d'estar configurats per a crear registres de control d'accés quan un usuari intenta accedir a recursos sense els privilegis adequats. Per a avaluar si aquest registre està operatiu, l'organització ha d'escanejar periòdicament els seus *logs* i comparar-los amb l'inventari d'actius instal·lat com a part

dels CBCS 1 i 2 per a assegurar que els elements crítics de la xarxa estiguen generant periòdicament *logs*.

Els programes analítics per a revisar registres poden ser valuosos, però els mitjans utilitzats per a analitzar els *logs* d'auditoria són bastant diversos; fins i tot un ràpid examen realitzat per una persona és important per a aquesta finalitat. Les eines de correlació poden fer molt més útils els registres d'auditoria per a una inspecció manual posterior, i poden ser de gran ajuda en la identificació d'atacs subtils. No obstant això, aquestes eines no reemplacen els administradors de sistemes i personal experimentat de seguretat de la informació. Fins i tot amb eines d'anàlisi de registre automatitzat es requereix la intuïció i l'experiència humana per a identificar i comprendre els atacs.

Deficiències en els registres de seguretat i en la seua anàlisi permeten als atacants ocultar la seua ubicació, el programari maliciós introduït i les activitats il·lícites que realitzen en les màquines víctimes. Fins i tot si els ens atacats saben que els seus sistemes han sigut compromesos, sense registres de *logs* complets i protegits són cecs als detalls de l'atac i a les accions posteriors dels atacants.

Sense uns *logs* d'auditoria sòlids, un atac pot passar desapercebut per temps indefinit i els danys infligits poden ser irreversibles. A causa de deficients o inexistents processos d'anàlisi de registres, a vegades els atacants controlen les màquines víctima durant mesos o anys sense que ningú se n'adone en l'organització de destinació, a pesar que l'evidència de l'atac consta en aquests registres no examinats.

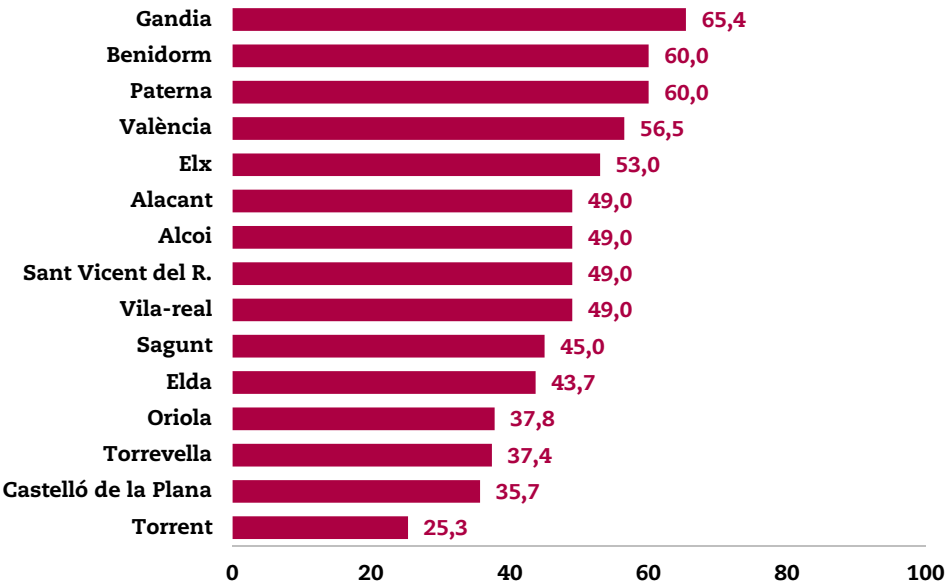
Per tot el que s'ha exposat adés, les organitzacions han d'incloure entre els seus procediments de seguretat la gestió dels registres d'auditoria, en els quals es definisquen els sistemes afectats, els tipus d'esdeveniments que cal registrar, el període de retenció, els responsables i els mecanismes de protecció aplicats a aquests.

A més, i atés l'ampli volum de registres generats pels diferents dispositius d'un sistema d'informació actual, és convenient l'ús d'eines per a la centralització o correlació d'esdeveniments d'auditoria per a gestionar-los eficientment.

Situació del control als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 6 en els quinze ajuntaments revisats. Només cinc aconsegueixen el nivell de maduresa *N2, repetible, però intuïtiu* (50%), i cap el nivell N3 (80%) requerit per l'ENS.

Gràfic 13. Índexs de maduresa del CBCS 6



Principals deficiències observades

Les principals deficiències relacionades amb el registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria) que hem detectat han sigut:

- Falta de procediments formalment aprovats per l'òrgan competent que descriga la gestió dels registres d'activitat dels usuaris, incloent-hi els sistemes afectats, la informació recollida, el període de retenció i els mecanismes de protecció d'aquests registres (catorze casos).

- Encara que els registres d'activitat es troben activats, es manté la configuració per defecte definida pel fabricant, sense tindre en compte aspectes com el període de retenció, tipus d'accions que cal registrar, etc. (set casos).

- Els registres d'auditoria dels diferents dispositius i sistemes no estan centralitzats en eines de recol·lecció de *logs* que en faciliten la revisió (quinze casos).

5.8 CBCS 7. Còpies de seguretat de dades i sistemes

Objectiu del control

Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú.

Per què és important aquest control bàsic de ciberseguretat

Quan els atacants comprometen els sistemes, sovint realitzen canvis significatius de les configuracions i el programari. A vegades, els atacants també realitzen alteracions subtils de les dades emmagatzemades en els sistemes compromesos, i això pot posar en perill l'eficàcia de l'organització amb informació contaminada. Altres vegades simplement destrueixen o invaliden totes o part de les dades i programari d'una entitat.

Quan es descobreixen els atacants, pot ser extremadament difícil per a les organitzacions eliminar tots els aspectes de la presència de l'atacant en els sistemes. Els danys de ciberatacs per mitjà de programari de segrest (*ransomware*) poden ser minimitzats si es disposa de còpia de seguretat de les dades segrestades.

Els ciberdelinqüents han anat evolucionant amb el pas del temps, millorant els mètodes de xifratge o l'accés als recursos del sistema. Aquest tipus d'atacs "millorats" s'ha utilitzat amb efectes devastadors en les últimes onades de programari de segrest. Per això, comptar amb una còpia de seguretat no accessible a nivell de xarxa, és a dir, que es trobe aïllada o desconnectada, és una bona mesura de protecció addicional a les de xifratge i seguretat física.

Les còpies de seguretat s'han de verificar. Per a això, periòdicament, un equip de proves ha d'avaluar una mostra aleatòria de les còpies de seguretat realitzades planificant restauracions en entorns de proves. Les proves de restauració de sistemes han d'incloure la verificació no sols del procés de recuperació, sinó també del seu contingut, és a dir, que el sistema operatiu, l'aplicació i les dades de la còpia de seguretat estiguen intactes i siguen funcionals.

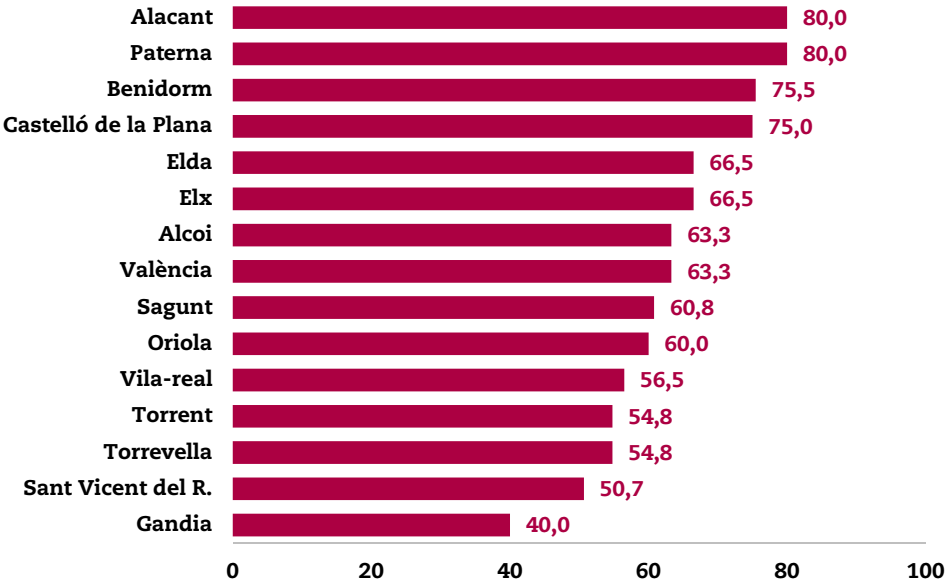
Amb l'evolució de la ciberdelinqüència i els mètodes d'atac cada vegada més sofisticats, és necessari que les organitzacions estiguen preparades no sols per a defensar-se, sinó també per a refer-se davant d'atacs reeixits: és un element clau de la ciberresiliència d'una entitat.

Les organitzacions han de decidir quina informació s'ha de protegir d'acord amb els responsables funcionals dels sistemes, i han de documentar el procés de còpies de seguretat en un procediment formalment aprovat que definisca la ubicació d'aquestes, el període de retenció, el tipus de còpies i la periodicitat. A més, les còpies s'han de proveir de les mesures de seguretat necessàries per a la seua protecció i han de realitzar-se proves de restauració planificades, que garantisquen que els sistemes poden ser restaurats de manera efectiva.

Situació del control als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 7 en els quinze ajuntaments revisats. Només dos ajuntaments aconsegueixen el nivell N3 (80%) requerit per l'ENS.

Gràfic 14. Índexs de maduresa del CBCS 7



Principals deficiències observades

Les principals deficiències detectades en aquest control han sigut:

- Absència de procediments formalment aprovats per l'òrgan competent que descriga les accions que han de dur-se a terme per a realitzar còpies de seguretat de dades i sistemes (deu casos).

- En general, les polítiques de còpia de seguretat existents s'han desenvolupat d'acord amb criteris del departament TIC, sense la participació activa dels responsables funcionals de les aplicacions que assenyalen les seues necessitats (cinc casos).

- No es realitzen proves de recuperació planificades dels sistemes crítics de l'entitat (deu casos).

- Les mesures implantades per a la protecció de les còpies no són efectives, i n'hi ha còpies no separades físicament del CPD principal, altres són accessibles a través de la xarxa o no existeixen còpies desconnectades (tres casos).

5.9 CBCS 8. Control de legalitat

Objectiu del control

Assegurar el compliment de la normativa bàsica en matèria de seguretat de la informació.

Per què és important aquest control bàsic de ciberseguretat

Amb la inclusió d'aquest control es pretén assegurar que es compleixen diverses normes relacionades amb la seguretat de la informació que considerem rellevants per a mantindre un adequat control sobre la seguretat dels sistemes d'informació i les comunicacions i la privacitat de la informació.

Considerem molt important acomplir degudament les disposicions de l'Esquema Nacional de Seguretat, ja que la seua finalitat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, de manera que es permeta als ciutadans i a les administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans. L'ENS estableix una sèrie de mesures de seguretat que han d'implantar les entitats públiques **amb caràcter obligatori** amb la finalitat de fonamentar la confiança que els sistemes d'informació prestaran els seus serveis i custodiaran la informació d'acord amb les seues especificacions funcionals, sense interrupcions o modificacions fora de control, i sense que la informació puga arribar al coneixement de persones no autoritzades.

D'altra banda, les administracions públiques, en el desenvolupament de les seues activitats, actuen com a responsables de tractar dades personals i han de garantir el dret de les persones a la protecció de les seues dades. Per tant, han d'adoptar les mesures necessàries per a garantir el nivell de seguretat requerit per la normativa vigent en matèria de protecció de dades personals.

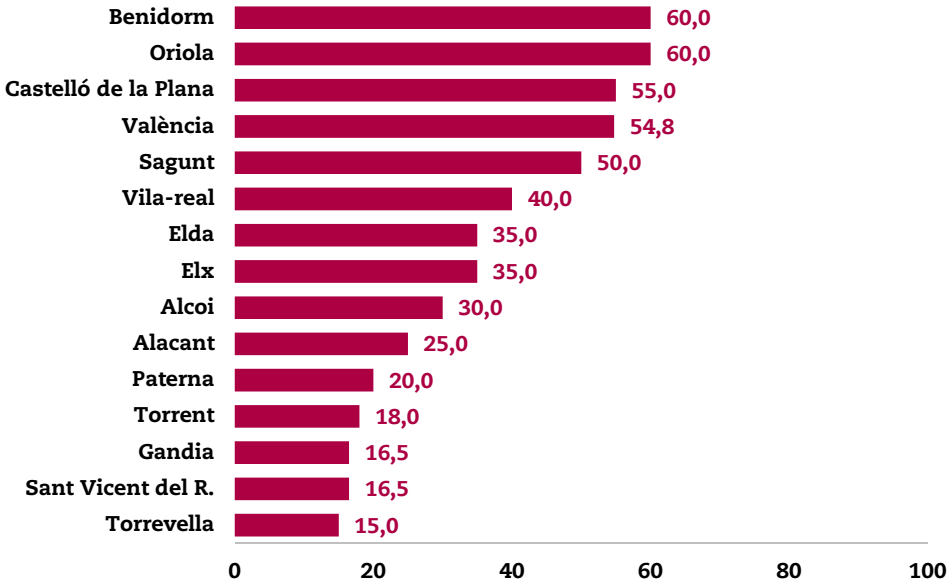
Finalment considerem que, dins de l'àmbit de la gestió econòmica, és important disposar de l'informe d'auditoria de sistemes anual del Registre Comptable de Factures en compliment del que exigeix la Llei 25/2013, de 27 de desembre, d'Impuls de la Factura Electrònica i Creació del Registre Comptable de Factures, ja que un dels objectius d'aquestes auditories és la "revisió de la gestió de la seguretat en aspectes relacionats amb la confidencialitat, autenticitat, integritat, traçabilitat i disponibilitat de les dades i serveis de gestió".

Maduresa del control de compliment als ajuntaments revisats

En el gràfic següent es mostren els índexs de maduresa del CBCS 8 referit al compliment legal, en els quinze ajuntaments revisats. Només cinc

ajuntaments aconsegueixen el nivell de maduresa N2, *repetible, però intuïtiu* (50%), i cap el nivell N3 (80%).

Gràfic 15. Índexs de maduresa del CBCS 8



Principals deficiències observades

La revisió del compliment de diverses normes relacionades amb la seguretat de la informació **ha posat de manifest, en general, un nivell de compliment bastant insatisfactori**.

Atés el baix nivell detectat en el compliment de legalitat, pràcticament la totalitat de requisits han sigut sovint incomplits. Caldria destacar, per tant, els que suposen un major impacte a l'efecte de protecció de dades de caràcter personal i de consecució del nivell requerit de seguretat dels sistemes d'informació:

- L'absència de política de seguretat aprovada i de cos normatiu i procedimental, que evidencia la falta de consciència i de compromís de l'entitat amb la seguretat de la informació i la protecció de dades personals (cinc casos).

- La inexistència d'òrgans de govern i dels perfils requerits per la normativa vigent, particularment del DPD i del responsable de seguretat, mancances que dificulten la presa de decisions, la unificació de criteris i la implantació homogènia de mesures de seguretat (sis casos).

- La falta d'un registre d'activitats del tractament, que implica la identificació i consideració de tots els usos de dades de caràcter

personal, requisit previ imprescindible per a la implantació de mesures i el compliment d'obligacions per a l'ús d'aquestes dades (set casos).

APÈNDIX. Metodologia aplicada

1. Introducció

Els sistemes d'informació actuals són més complexos i estan més interconnectats que mai, però una major interconnexió origina majors riscos de ciberseguretat, ocasiona una major probabilitat que es produïsca una pertorbació significativa en els sistemes d'informació de les entitats locals deguda a un ciberatac i, en conseqüència, una interrupció en els serveis prestats als ciutadans.

Per aquesta raó, és imperatiu que els responsables dels ens públics gestionen els riscos associats amb el funcionament i l'ús de sistemes d'informació que utilitzen per a desenvolupar i prestar els serveis públics. Així mateix, és fonamental establir controls de ciberseguretat adequats per a mantindre els sistemes d'informació protegits davant de les amenaces de seguretat.

La gestió dels riscos de ciberseguretat comprén una àmplia gamma d'activitats empreses per a protegir els sistemes d'informació i les dades d'accés no autoritzades i altres amenaces cibernètiques; mantindre la consciència de les amenaces cibernètiques; detectar anomalies i incidents que afecten negativament els sistemes d'informació i les dades, i mitigar el seu impacte, respondre i recuperar-se d'incidents.

L'existència d'uns CBCS eficaços és un element essencial per a la prestació de serveis públics d'una manera tecnològicament sostenible.

Tot i que l'adopció de mesures de seguretat adequades fa més resilients les organitzacions davant dels ciberatacs, la descripció dels incidents produïts en 2017 que es realitza en l'Informe Nacional de l'Estat de Seguretat dels Sistemes de les TIC, del CCN, revela que les organitzacions no sempre implementen, ni tan sols, les mesures més bàsiques que podrien haver previngut o mitigat el mal causat. Se citen en aquest informe un parell d'exemples: atacs com WannaCry o Bad Rabbit van explotar vulnerabilitats conegudes. Les actualitzacions per a aquestes vulnerabilitats havien estat disponibles durant mesos, però no s'havien instal·lat en les organitzacions afectades. En altres casos, encara que les vulnerabilitats eren desconegudes, l'adopció de les mesures de seguretat més elementals haurien suposat un impediment per a l'atac o haurien mitigat els seus efectes.

D'altra banda, el fet que els ciberatacs romanguen sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan correctament implementades. Investigacions recents han revelat que les empreses, els governs i les organitzacions a Europa, sovint, només descobreixen que han sigut víctimes d'un ciberatac mesos després.

2. La guia pràctica de fiscalització dels OCEX 5313

Aquesta auditoria està basada en la guia pràctica de fiscalització dels OCEX ***GPF-OCEX 5313 Revisió dels controls bàsics de ciberseguretat***, aprovada per la Conferència de Presidents dels Òrgans de Control Extern el 12 de novembre de 2018, que forma part del *Manual de fiscalització* de la Sindicatura de Comptes i que pot consultar-se en el nostre web. Per a més detall sobre la metodologia utilitzada ens remetem a aquesta guia.

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS, que és de compliment obligat per a tots els ens públics. No obstant això, atesa l'amplitud de l'ENS, que està format per 75 mesures de seguretat, per a la seua inclusió en els CBCS es va seleccionar una sèrie limitada de controls. Per a seleccionar els més rellevants es va atendre el marc conceptual establit per la prestigiosa organització Center for Internet Security (CIS),[1] que prioritza i classifica els controls segons la seua importància per a fer front a les ciberamenaces.

Els vint controls de seguretat crítics del CIS són un conjunt concís i prioritzat d'accions de ciberdefensa, i el seu avantatge principal és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant de ciberatacs al voltant del 85%. Si s'implementen els vint controls, el risc es pot reduir un 94%.

La versió 7 dels controls CIS classifica els sis primers controls com a bàsics i són els que s'han utilitzat com a referència en la GPF-OCEX 5313 per a establir els controls bàsics de ciberseguretat (CBCS) dels OCEX. S'hi va afegir el relatiu a les còpies de seguretat de dades i sistemes (desé control CIS) per la seua importància per a la recuperació davant d'un desastre o atac reeixit i, per tant, per a garantir una ciberresiliència raonable. Si tots els controls preventius fallen i un ciberatac traspassa totes les línies de defensa i té èxit, l'últim recurs de l'entitat atacada és restaurar els seus sistemes i dades en un termini predeterminat per a poder continuar prestant els seus serveis.

Als set CBCS se'n va afegir un huité relacionat amb el compliment normatiu, per la seua importància en una administració pública.

3. Els CBCS com a mesures de ciberhigiene

L'European Union Agency for Cybersecurity (ENISA) assenyala[2] que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la

---

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

2 *Review of Cyber Hygiene Practices*, ENISA, desembre de 2016.

informació i, com l'analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen" i reduir els ciberriscos.

En síntesi, la ciberhigiene s'utilitza per a fer referència al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.

En aquesta direcció, ENISA estableix deu punts d'acció per a una ciberhigiene adequada. Com s'observa en la taula següent, els set primers són en bona part coincidents amb els CBCS:

Quadre 2. Punts d'acció d'ENISA

ENISA	CBCS
1. Tindre un registre de tot el maquinari	CBCS 1
2. Tindre un registre de tot el programari per a assegurar-se que s'han introduït correctament els pedaços	CBCS 2
3. Utilitzar guies de configuració segura i fortificació per a tots els dispositius	CBCS 5
4. Gestionar les dades dins i fora de la seua xarxa	--
5. Escanejar tots els correus electrònics entrants	--
6. Minimitzar els usuaris administradors	CBCS 4
7. Realitzar còpies de seguretat de dades regularment i fer proves de restauració	CBCS 7

Dels set CBCS, sense comptar el compliment normatiu, cinc són coincidents amb els punts d'acció prioritaris recomanats per ENISA com a bones pràctiques de ciberhigiene. A l'efecte d'aquest treball, considerem que els CBCS constitueixen un conjunt de pràctiques i accions bàsiques per a mantindre una ciberhigiene adequada.

4. Alineació amb l'Esquema Nacional de Seguretat

Atés que l'ENS és de compliment obligat per a tots els ens públics, s'ha tingut una cura especial perquè qualsevol metodologia d'auditoria dels controls de ciberseguretat estiga plenament alineada amb l'ENS. Aquesta alineació facilita la realització de les auditories de ciberseguretat per part de la Sindicatura i coadjuva a la implantació de l'ENS en els ens auditats, ja que pràcticament tots els subcontrols o controls detallats que verifica la Sindicatura estan exigits per l'ENS.

Els huit controls bàsics de ciberseguretat degudament referenciats amb l'ENS són:

Quadre 3. Els CBCS i l'ENS

	Control	Mesura de seguretat de l'ENS*
CBCS 1	Inventari i control de dispositius físics	op.exp.1
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	op.exp.1 op.exp.2
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	mp.sw.2 op.exp.4
CBCS 4	Ús controlat de privilegis administratius	op.acc.4 op.acc.5
CBCS 5	Configuracions segures del programari i maquinari, dispositius mòbils, portàtils, equips de taula i servidors	op.exp.2 op.exp.3
CBCS 6	Registre de l'activitat dels usuaris	op.exp.8 op.exp.10
CBCS 7	Còpies de seguretat de dades i sistemes	mp.info.9
CBCS 8	Compliment de la legalitat	

* Aquestes sigles identifiquen cada una de les mesures de seguretat de l'annex I de l'ENS.

Quan una auditoria es realitze en entitats que hagen passat l'auditoria de seguretat obligatòria establida en l'article 34 del Reial Decret 3/2010, pel qual s'aprova l'ENS, la revisió de la Sindicatura podrà basar-se, en la mesura que siga possible, en els resultats d'aquesta auditoria i determinades comprovacions podran donar-se per complides.

Per a depositar confiança en aquestes auditories externes de seguretat, han de complir els requisits legalment establits com són, entre altres, que les entitats certificadores estiguen acreditades i constar en la secció "Entitats de certificació acreditades" del web del CCN (és necessària l'acreditació si es pretén certificar el compliment de l'ENS). A més, l'equip d'auditoria ha d'obtindre alguna evidència que el treball realitzat ha sigut adequat per a suportar les conclusions d'aquest informe. Quan s'haja depositat confiança en aquestes auditories s'ha d'assenyalar expressament en l'informe.

5. Criteris d'auditoria: els controls bàsics de ciberseguretat i els seus subcontrols

Els CBCS són controls globals formats per diversos subcontrols detallats que es mostren en la taula següent. Totes les nostres comprovacions tenen per finalitat contrastar la seua situació real en l'entitat amb les

bones pràctiques recollides en la GPF-OCEX 5313, que es resumeixen en el quadre següent.

Els aspectes que es comproven en cada CBCS s'especifiquen amb el màxim detall en la GPF-OCEX 5313.

Quant als índexs o nivells objectiu que han d'aconseguir-se en cada CBCS i subcontrol, vegeu l'apartat 6 següent.

Quadre 4. Els CBCS i els seus subcontrols

Control	Objectiu del control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots el dispositiu de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats	L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
		CBCS 1-2: Control d'actius físics no autoritzats	L'entitat disposa de mesures de seguretat per a controlar (detectar i restringir) l'accés de dispositius físics no autoritzats.
CBCS 2 Inventari i control de programari autoritzat	Gestionar activament tot el programari en els sistemes, de manera que només es puga instal·lar i executar programari autoritzat.	CBCS 2-1: Inventari de maquinari autoritzat	L'entitat disposa d'un inventari de maquinari complet, actualitzat i detallat.
		CBCS 2-2: Maquinari suportat pel fabricant	El maquinari utilitzat per l'entitat té suport del fabricant. En cas contrari, es marca en l'inventari com fora de suport.
		CBCS 2-3: Control de maquinari no autoritzat	L'entitat disposa de mecanismes que impedeixen la instal·lació i execució de maquinari no autoritzat.
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats	Existeix un procés per a identificar les vulnerabilitats dels components del sistema que assegura que aquestes són identificades en temps oportú.
		CBCS 3-2: Priorització	Les vulnerabilitats identificades són analitzades i prioritzades per a la seua resolució atés el risc que suposen per a la seguretat del sistema.
		CBCS 3-3: Resolució de vulnerabilitats	Es realitza un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que aquestes es resolen en el temps previst en el procediment.
		CBCS 3-4: Pedaços	L'entitat disposa de procediments i eines que permeten aplicar els pedaços de seguretat publicats pels fabricants en un temps raonable.
CBCS 4 Ús controlat de privilegis administratius	Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'ús i configuració de privilegis administratius en ordinadors, xarxes i aplicacions.	CBCS 4-1: Inventari i control de comptes d'administració	Els privilegis d'administració estan limitats adequadament i l'entitat disposa d'un inventari de comptes d'administració que facilita el seu correcte control.
		CBCS 4-2: Canvi de contrasenyes per defecte	Les contrasenyes per defecte dels comptes que no s'utilitzen o són estàndard es canvien abans de l'entrada en producció del sistema.
		CBCS 4-3: Ús dedicat de comptes d'administració	Els comptes d'administració només es realitzen per a les tasques que són estrictament necessàries.
		CBCS 4-4: Mecanismes d'autenticació	Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes.
		CBCS 4-5: Auditoria i control	L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades.

Control	Objectiu del control	Subcontrol	
CBCS 5 Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors	Establir, implantar i gestionar la configuració de seguretat dels dispositius mòbils, portàtils, servidors i de taula, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de previndre atacs per mitjà de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndard de configuració segura per a tots els sistemes operatius i maquinari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6 Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria)	Recollir, gestionar i analitzar *logs* d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de *logs* d'auditoria	El *log* d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
		CBCS 6-2: Emmagatzematge de *logs*: retenció i protecció	Els *logs* es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de *logs*	Els *logs* de tots els sistemes són revisats periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels *logs* d'auditoria, de manera que se'n facilite la revisió.
		CBCS 6-4: Monitoratge i correlació	L'entitat disposa d'un SIEM (sistema de gestió d'incidències i informació de seguretat) o una eina d'analítica de *logs* per a realitzar correlació i anàlisi de *logs*.
CBCS 7 Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú.	CBCS 7-1: Realització de còpies de seguretat	L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema.
		CBCS 7-2: Realització de proves de recuperació	Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica, i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmeses a través de la xarxa.
CBCS 8 Compliment de legalitat	L'entitat compleix els requisits legals i reglamentaris que hi són aplicables.	CBCS 8-1: Compliment de l'ENS	L'entitat compleix els requeriments establits en l'ENS.
		CBCS 8-2: Compliment de la LOPD/RGPD	L'entitat compleix els requeriments establits en la LOPD/RGPD.
		CBCS 8-3: Compliment de la Llei 25/2013	L'entitat compleix els requeriments establits en la Llei 25/2013, de 27 de desembre.

6. Avaluació dels resultats del treball

Els resultats del treball s'analitzen i avaluen a dos nivells: subcontrols i controls (CBCS).

Subcontrols

Els CBCS són controls globals compostos per diversos subcontrols detallats (tal com es pot veure en l'apartat 2 anterior), dels quals hem revisat el disseny i l'eficàcia operativa.

El treball d'auditoria consisteix bàsicament a avaluar cada subcontrol en funció dels resultats de les proves realitzades i les evidències obtingudes, o bé de la informació proporcionada en l'informe d'auditoria de l'ENS, si existeix i si hi confiem. Cada subcontrol s'avalua segons l'escala mostrada en el quadre següent:

Quadre 5. Avaluació dels subcontrols

Avaluació	Descripció
Control efectiu	Cobreix al 100% l'objectiu de control i: - El procediment està formalitzat (documentat i aprovat) i actualitzat. - El resultat de les proves realitzades per a verificar-ne la implementació i l'eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	A grans trets, compleix l'objectiu de control, si bé pot haver-hi certs aspectes no coberts al 100% i: - Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.). - Les proves realitzades per a verificar-ne la implementació són satisfactòries. - S'han detectat incompliments en les proves realitzades per a verificar-ne l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	Cobreix de manera molt limitada l'objectiu de control i: - Se segueix un procediment, encara que pot no estar formalitzat. - El resultat de les proves d'implementació i d'eficàcia no és satisfactori. Cobreix a grans trets l'objectiu de control, però: - No se segueix un procediment clar. - Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	No cobreix l'objectiu de control. El disseny cobreix l'objectiu de control, però el resultat de la revisió realitzada posa de manifest que la implementació o l'eficàcia operativa del control no són satisfactòries (s'han detectat incompliments significatius i generalitzats).

D'acord amb els resultats obtinguts en cada subcontrol s'estableix una correspondència amb el nivell de maduresa descrit en el quadre següent.

Nivell de maduresa dels CBCS

Per a determinar la situació global de cada CBCS hem utilitzat el **model de nivell de maduresa** dels processos de control d'acord amb el que s'estableix en la GPF-OCEX 5313, que al seu torn està basada en la *Guia de seguretat CCN-STIC 804* del Centre Criptològic Nacional, usant una escala, tal com es resumeix en el quadre següent.

Quadre 6. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El CBCS no s'està aplicant en aquest moment.
N1 Inicial / *ad hoc*	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *L'organització no proporciona un entorn estable. L'èxit o el fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan els procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. *L'eficàcia del procés depén de la bona sort i de la bona voluntat de les persones. Hi ha un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.*
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. *Es disposa un catàleg de processos que es manté actualitzat, els quals garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant dels incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor del desconegut (o no planificat).* *L'èxit és més que bona sort: es mereix.* *Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, una coordinació que no existeix en el nivell 2, i que es gestiona en el nivell 3.*

Nivell	Índex	Descripció
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. *Es disposa d'un sistema de mesures i mètriques per a conéixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.* *En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3 era solament qualitativa.*
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. *El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.* *S'estableixen objectius quantitatius de millora, es revisen contínuament per a reflectir els canvis en els objectius de negoci i s'utilitzen com a indicadors en la gestió de la millora dels processos.* *En aquest nivell, l'organització és capaç de millorar l'acompliment dels sistemes sobre la base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.*

L'avaluació que realitzem sobre el nivell de maduresa no s'ha basat únicament en els processos teòrics o en els procediments aprovats, sinó també en la verificació de l'aplicació pràctica.

Per a avaluar el nivell de maduresa de cada CBCS s'han tingut en compte els resultats obtinguts en la revisió dels subcontrols que el formen i considerant la ponderació o importància relativa que els assignem per al compliment de l'objectiu de control del CBCS.

Aquest model proporciona una base sòlida per a formar-se una idea general de la situació en l'entitat revisada dels controls de ciberseguretat i el compliment de la legalitat en aquesta matèria. També permet comparar resultats entre diferents ens i entre diferents períodes.

7. Nivell de maduresa mínim requerit en funció de la categoria dels sistemes d'informació auditats

Als sistemes de les tecnologies de la informació i la comunicació dels organismes del sector públic obligats al compliment de l'ENS se'ls assigna una categoria en funció de la valoració de l'impacte que tindria sobre l'organització un incident que afectara la seguretat de la informació o dels sistemes, amb repercussió en la capacitat organitzativa per a:

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

La categoria d'un sistema serà aplicable a tots els sistemes utilitzats per a la prestació dels serveis de l'administració electrònica i suport del procediment administratiu general.

A fi de poder determinar l'impacte que tindria sobre l'organització un incident que afectara la seguretat de la informació o dels sistemes, i de poder establir la categoria del sistema, s'han de tindre en compte les cinc dimensions de la seguretat:

- Confidencialitat. És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.

- Integritat. És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, i s'assegura que no se n'ha produït l'alteració, pèrdua o destrucció, tant de manera accidental com intencionada, per errors de programari o maquinari o per condicions mediambientals.

- Disponibilitat. És tracta de la capacitat d'un servei, un sistema o una informació de ser accessible i utilitzable pels usuaris o processos autoritzats quan ho requerisquen.

- Autenticitat. És la propietat o característica consistent en el fet que una entitat és la que diu ser o bé que garanteix la font de la qual procedeixen les dades.

- Traçabilitat. És la propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

Una informació o un servei es poden veure afectats en una o més de les seues dimensions de seguretat. Cada dimensió de seguretat afectada s'adscriu a un dels nivells següents: baix, mitjà o alt.

Tenint en compte això, es defineixen tres categories de sistemes d'informació:

a) Un sistema d'informació serà de categoria alta si alguna de les seues dimensions de seguretat aconsegueix el nivell alt.

b) Un sistema d'informació serà de categoria mitjana si alguna de les seues dimensions de seguretat aconsegueix el nivell mitjà, i cap aconsegueix un nivell superior.

c) Un sistema d'informació serà de categoria bàsica si alguna de les seues dimensions de seguretat aconsegueix el nivell baix, i cap aconsegueix un nivell superior.

La categoria d'un sistema d'informació, en matèria de seguretat, modula l'equilibri entre la importància de la informació que maneja, dels serveis que presta i l'esforç de seguretat requerit, en funció dels riscos als quals està exposat, sota el criteri del principi de proporcionalitat.

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[3]

Categoria del sistema	Nivell mínim d'exigència/maduresa requerit
BÀSICA	N2 – Reproduïble, però intuïtiu (50%)
MITJANA	N3 – Procés definit (80%)
ALTA	N4 – Gestionat i mesurable (90%)

Els sistemes auditats en aquest informe estan classificats com de categoria mitjana.

Per tant, hem analitzat si els resultats obtinguts d'acord amb el model de nivell de maduresa aconsegueixen el nivell mínim d'exigència requerit en l'ENS, que en aquest cas és *N3, procés definit* i un índex de maduresa del 80%.

8. Indicadors globals

Als efectes de l'ENS, la guia CCN-STIC-824 preveu una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics. Aquests indicadors s'han adaptat per a aplicar-los als CBCS, ja que permeten dur a terme tant un resum de l'estat de les mesures de seguretat de cada ajuntament als efectes de l'ENS com dels CBCS:

- L'índex de maduresa sintetitza, en tant per cent, el nivell de maduresa aconseguit per un organisme respecte del conjunt de CBCS.

- L'índex de compliment analitza igualment el nivell de maduresa aconseguit, però en relació amb l'exigència aplicable en cada cas, tenint en compte la categoria del sistema. És a dir, compara l'índex de maduresa amb el nivell mínim exigit per a aquesta categoria en l'ENS, que en aquesta auditoria és N3 (80%) per a tots els casos.

[3] Informe Nacional de l'Estat de Seguretat dels Sistemes de les Tecnologies de la Informació i la Comunicació, de 2018, apartat 3.1. En els diferents perfils s'avaluen els controls per mitjà d'un nivell d'exigència, també conegut com a *nivell de maduresa*, i es fixa el nivell mínim d'exigència requerit.

9. Dates de l'examen

Els treballs d'auditoria dels quinze ajuntaments es van iniciar progressivament a la primavera de 2019 i van finalitzar a la de 2020. Els informes recullen i informen sobre la situació dels CBCS en acabar el treball de camp i emetre l'informe d'auditoria.

Considerem com a fi del treball de camp la data en què les constatacions de l'auditoria, les conclusions i l'esborrany previ de l'informe es discuteix amb els responsables de l'entitat auditada, d'acord amb el que s'estableix en el nostre *Manual de fiscalització*. S'admet qualsevol evidència addicional disponible en aquell moment i es corroboren els fets posats de manifest en l'informe. **L'informe, amb caràcter general, reflecteix la situació en aquell moment**, ja que és freqüent que, des que s'inicia el treball de camp, determinades deficiències observades i assenyalades als gestors s'esmenen i es recullen d'aquesta manera en les conclusions i en els indicadors.

Per a conéixer les dates a què es refereixen els diferents informes assenyalem els dos moments clau per a això en el quadre següent.

Quadre 7. Moment que reflecteix la situació dels CBCS en els diferents ajuntaments

Ajuntament	Fi del treball de camp	Termini per a remissió d'al·legacions
Benidorm	04/10/2019	20/12/2019
Gandia	24/10/2019	10/01/2020
Alacant	23/10/2019	20/12/2019
Paterna	25/10/2019	28/02/2020
València	30/10/2019	20/12/2019
Oriola	13/11/2019	10/01/2020
Torrent	25/11/2019	03/02/2020
Torrevella	11/12/2019	13/02/2020
Elx	26/12/2019	03/02/2020
Castelló de la Plana	16/01/2020	28/02/2020
Sagunt	23/01/2020	28/02/2020
Sant Vicent del Raspeig	24/04/2020	12/06/2020
Elda	20/04/2020	12/06/2020
Alcoi	30/04/2020	12/06/2020
Vila-real	05/06/2020	06/07/2020

La tramitació formal dels informes inclou el tràmit d'al·legacions, en el qual les entitats poden aportar evidències addicionals sobre la situació dels CBCS en la data de la fi del treball de camp. Si és així s'analitzen, es consideren i, si s'admeten, es poden modificar conclusions i indicadors. Si s'aporten evidències amb efecte posterior a la data assenyalada per a la remissió d'al·legacions a la Sindicatura podrien recollir-se en l'informe, però en aquest cas no alterarien les conclusions ni els indicadors. En tot cas, tant les al·legacions com l'anàlisi d'aquestes i l'efecte en els informes es publiquen com un annex dels informes.

A més, és important saber a quina data es refereix l'informe, ja que en el Programa Anual d'Actuació de 2020 està expressament previst realitzar un informe de "seguiment de les 11 auditories dels controls bàsics de ciberseguretat el treball de camp de les quals s'ha realitzat en 2019 (una vegada transcorregut un any des de la seua finalització)". Raonablement, aquest seguiment tindrà continuïtat amb els quatre ajuntaments auditats en 2020.

La finalitat del seguiment de les auditories serà verificar si els ajuntaments han introduït mesures correctores a les deficiències assenyalades en els informes.

Amb l'ànim de facilitar aquesta tasca, en els informes hem classificat les nostres recomanacions segons criteris combinats de risc potencial que cal mitigar i cost de la implantació; d'aquesta manera es poden establir accions basades en criteris de cost/benefici, i les hem reflectides en un gràfic.

A més de les recomanacions assenyalades en els informes, juntament amb el detall al màxim nivell de les deficiències de seguretat observades, s'ha comunicat als responsables de cada ajuntament altres recomanacions amb una relació de risc potencial que cal mitigar i cost de la implantació menys favorable que les anteriors.

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*h* del seu Reglament de Règim Interior i del Programa Anual d'Actuació de 2020 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 9 de juliol de 2020, va aprovar aquest informe d'auditoria.