

SINDICATURA DE COMPTES  
DE LA COMUNITAT VALENCIANA

**INFORME DE SEGUIMENT DE LES  
RECOMANACIONS REALITZADES EN L'INFORME  
D'AUDITORIA DELS CONTROLS BÀSICS DE  
CIBERSEGURETAT DE L'AJUNTAMENT DE  
TORREVELLA DE L'ANY 2019**

Situació a 31 de desembre de 2021



## RESUM

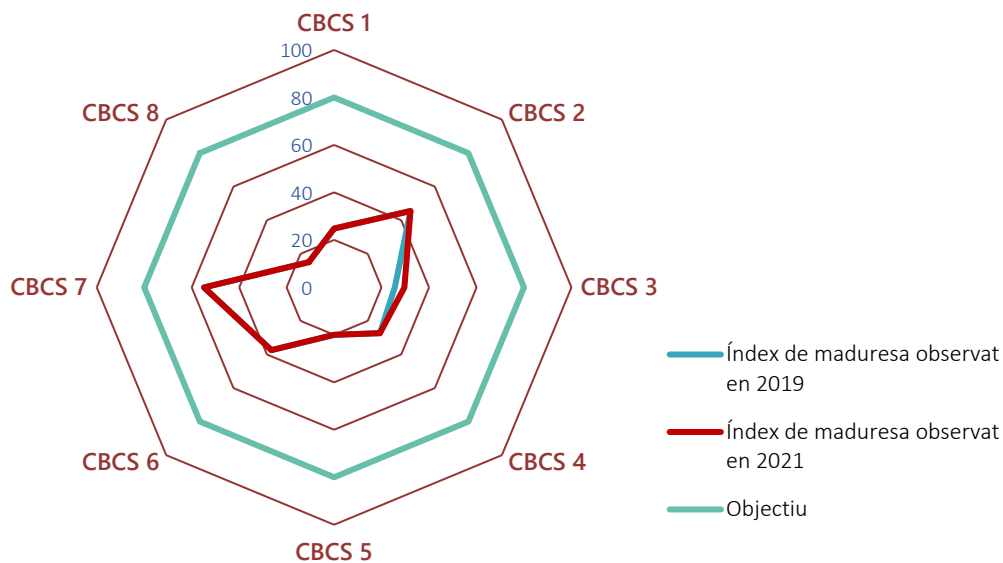
La transformació digital que estan experimentant totes les administracions públiques i la seua interconnexió a través de complexes xarxes informàtiques les exposa de manera cada vegada més intensa a amenaces provinents del ciberespai. Això origina un increment dels riscos associats als sistemes d'informació que sustenten els serveis públics i, per tant, a la informació que manegen. De fet, les entitats locals han sigut un dels objectius més afectats per les onades recents de ciberatacs.

Atenent aquesta realitat, i en sintonia amb el seu pla estratègic actual, la Sindicatura de Comptes ha realitzat un treball de seguiment dels controls bàsics de ciberseguretat (CBCS) de l'Ajuntament de Torrevella respecte de la situació mostrada en l'auditoria de l'any 2019.

### Conclusions i recomanacions

A penes s'han realitzat progressos per a millorar la ciberseguretat des de la nostra auditoria anterior i no s'han atés degudament les nostres recomanacions per a això. Per tant, l'índex de maduresa general dels controls bàsics de ciberseguretat mostra un valor del 31,8% (31,3% en 2019) i, per tant, el nivell d'efectivitat en els controls analitzats continua sent molt deficient i reflecteix un nivell de risc inacceptable per a una entitat pública de la importància de l'Ajuntament de Torrevella.

Encara que hi ha iniciatives posades en marxa en 2022, l'entitat ha de prendre mesures urgents per a reconduir la situació i s'han d'implantar millores per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, l'objectiu dels quals és arribar a un 80% en l'índex de maduresa general.





L'Ajuntament de Torrevella no té establida una estructura de governança de la ciberseguretat, tal com exigeix la normativa i un adequat sistema de control intern. Aquesta situació ha de ser promptament esmenada i, encara que hem constatat iniciatives per part de la corporació per a reconduir la situació i millorar el seu compromís amb la seguretat de la informació i l'administració electrònica, els òrgans superiors de l'Ajuntament, com a responsables del sistema de control, han de reforçar d'una manera decidida el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

Així mateix, la nostra revisió també ha posat de manifest un grau de compliment molt deficient quant a l'adequació a les normes legals relacionades amb la seguretat de la informació. L'informe assenyala diversos aspectes sobre els quals s'ha d'actuar per a una ràpida esmena. En relació amb la protecció de dades personals, l'Ajuntament ha de finalitzar l'elaboració del registre d'activitats de tractament i publicar aquest registre.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament, entre les quals aconsellem realitzar una gestió unificada de pedaços de seguretat sobre tots els sistemes de l'entitat per mitjà de l'eina disponible, formalitzar un procediment unificat per a gestió d'usuaris amb privilegis d'administració i finalitzar el procés de renovació per a actualitzar tots els sistemes que es troben fora del període de suport.

## **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 conèixer el veritable abast del treball realitzat.



**Informe de seguiment de les recomanacions realitzades en  
l'informe d'auditoria dels controls bàsics de ciberseguretat de  
l'Ajuntament de Torrevella de l'any 2019**

**Situació a 31 de desembre de 2021**

**Sindicatura de Comptes  
de la Comunitat Valenciana**



## ÍNDEX (amb hipervincles)

|  |           |
|--|-----------|
| <b>1. Introducció</b>  | <b>3</b>  |
| <b>2. Responsabilitats dels òrgans superiors de l'Ajuntament en relació amb els controls de ciberseguretat</b> | <b>4</b>  |
| <b>3. Responsabilitat de la Sindicatura de Comptes</b>   | <b>4</b>  |
| <b>4. Conclusions</b>  | <b>5</b>  |
| <b>5. Recomanacions i mesures necessàries per al compliment de la legalitat</b>                                | <b>8</b>  |
| <b>Apèndix 1. Metodologia aplicada</b>   | <b>20</b> |
| <b>Apèndix 2. Situació dels controls bàsics de ciberseguretat</b>  | <b>37</b> |
| <b>Acrònims i glossari de termes</b>   | <b>46</b> |
| <b>Tràmit d'al·legacions</b>   | <b>49</b> |
| <b>Aprovació de l'Informe</b>  | <b>50</b> |



## 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, 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 suporten la informació economicofinancera, comptable i de gestió.

En la guia d'auditoria GPF-OCEX 5311, "Ciberseguretat, seguretat de la informació i auditoria externa", del *Manual de fiscalització* de la Sindicatura de Comptes, 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 els han de prestar cada vegada més atenció. En línia amb això, **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.**

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 20 de febrer de 2020 el Consell de la Sindicatura de Comptes va aprovar l'[Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Torrevella. Exercici 2019](#). Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 la realització d'un treball de seguiment de la situació dels controls bàsics de ciberseguretat d'aquest ajuntament i dels altres 14 ajuntaments analitzats.

### La necessitat d'una ciberhigiene adequada

Adicionalment, la crisi provocada per l'epidèmia de COVID-19 i les mesures tecnològiques adoptades per les administracions públiques han posat de manifest amb absoluta claredat la total dependència de l'Administració respecte dels sistemes d'informació i comunicacions i el fort augment de la superfície d'exposició davant de les ciberamenaces. Per a fer front a aquesta realitat, les entitats públiques han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat (ENS), tant per obligació legal com per raons d'autoprotecció i supervivència.

En aquests entorns actuals d'administració electrònica avançada prenen tot el sentit conceptes com la ciberresiliència i la ciberhigiene. Per ciberresiliència es pot entendre 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. La ciberhigiene és un principi fonamental<sup>1</sup> relacionat amb la seguretat de la informació i equival a establir mesures rutinàries senzilles per a minimitzar els riscos de les ciberamenaces. De manera anàloga al que ocorre amb la higiene personal, les bones pràctiques de ciberhigiene poden impulsar una major immunitat en les entitats que les apliquen, la qual cosa redueix el risc davant d'un ciberatac.

Per tant, l'existència d'uns controls eficaços de ciberseguretat és un element essencial per a la prestació de serveis públics en una administració tecnològicament avançada. En aquest sentit, considerem que la implantació dels controls bàsics de ciberseguretat (CBCS) –en definitiva, un subconjunt de les mesures de seguretat obligatòries exigides per l'ENS– constitueix una mesura bàsica de ciberhigiene per a les administracions públiques.

## **2. RESPONSABILITATS DELS ÒRGANS SUPERIORS DE L'AJUNTAMENT EN RELACIÓ AMB ELS CONTROLS DE CIBERSEGURETAT**

Els òrgans superiors de l'Ajuntament (en particular, l'alcalde i la Junta de Govern) són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions. D'acord amb les seues competències, han de garantir que el funcionament de l'entitat resulte conforme amb les normes aplicables i que els controls interns proporcionen una garantia raonable que la informació, els serveis i els sistemes d'informació que els donen suport complisquen les propietats següents, que coincideixen amb les cinc dimensions de la seguretat de la informació que estableix l'Esquema Nacional de Seguretat: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.

## **3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES**

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022 hem efectuat el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Torrevella. Exercici 2019.

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats, proporcionar una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control.

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada a 31 de desembre de 2021 dels huit CBCS revisats en l'auditoria de l'any 2019, relacionats amb les aplicacions i

---

<sup>1</sup> [Review of Cyber Hygiene Practices](#), European Union Agency for Cybersecurity (ENISA), 2016.



sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interés general.

Per a això, hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura recollides en el *Manual de fiscalització de la Sindicatura de Comptes*. Aquests principis exigeixen que complim els requeriments d'ètica, com també que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CBCS revisats.

Considerem que l'evidència d'auditoria obtinguda proporciona una base suficient i adequada per a fonamentar les nostres conclusions sobre l'estat dels controls bàsics de ciberseguretat, d'acord amb l'abast limitat que s'ha assenyalat.

Els procediments realitzats en una auditoria de seguretat limitada són reduïts en comparació amb els que es requereixen per a obtindre una seguretat raonable, però s'espera que el nivell de seguretat siga, d'acord amb el judici professional de l'auditor, significatiu per als destinataris de l'informe. La seguretat limitada no garanteix que una auditoria realitzada de conformitat amb els *Principis fonamentals de fiscalització dels òrgans de control extern* i amb les normes tècniques de fiscalització recollides en el *Manual de fiscalització de la Sindicatura de Comptes* detecte sempre un incompliment significatiu quan existisca.

En l'apèndix 1 es proporciona un major detall de la metodologia utilitzada. En l'apèndix 2 es detallen les constatacions de l'auditoria que fonamenten les conclusions i les recomanacions d'aquest informe.

## 4. CONCLUSIONS

**L'índex de maduresa general dels controls bàsics de ciberseguretat continua sent molt deficient i reflecteix un nivell de risc inacceptable per a una entitat pública de la importància de l'Ajuntament de Torrevella.**

**A penes s'han realitzat progressos per a millorar la ciberseguretat des de la nostra auditoria anterior i no s'han atés degudament les nostres recomanacions per a això. No obstant això, hi ha iniciatives posades en marxa en 2022 que han de reforçar-se amb mesures urgents per a reconduir la situació.**

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconseguix un **índex de maduresa general del 31,8%**, que es correspon amb un nivell de maduresa *N1 inicial / ad hoc*; és a dir, els processos de control existeixen, però la seua gestió no està correctament organitzada.





El nivell d'efectivitat en els controls analitzats és molt deficient i reflecteix un nivell de risc inacceptable; per tant, han d'implantar-se urgentment millores per aconseguir els nivells exigits per l'ENS. En l'apartat 5 es realitzen les recomanacions pertinents amb aquesta finalitat.

Els resultats detallats obtinguts per a cada un dels CBCS i la seua evolució es mostren en el quadre 1.

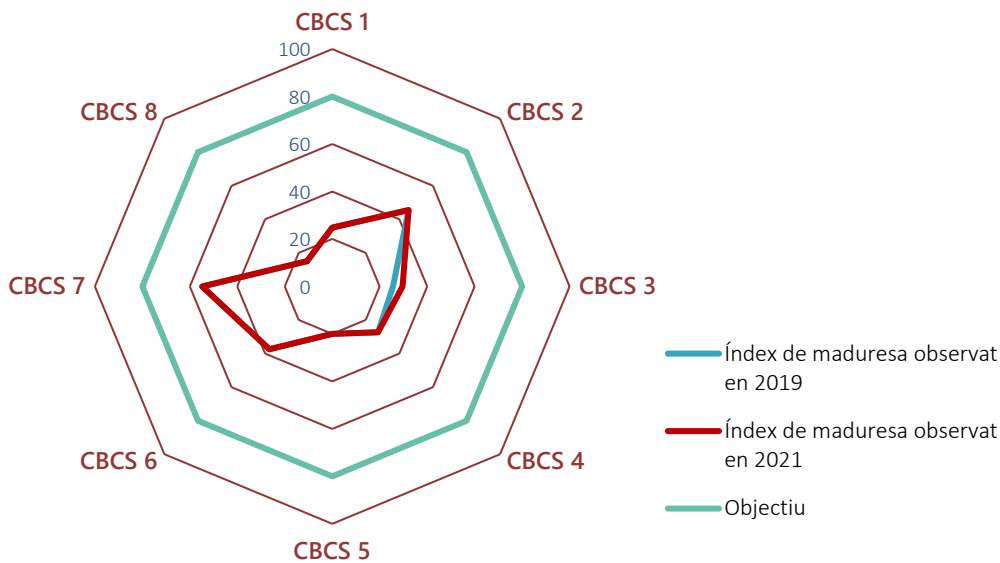
**Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat**

| Control  | 2019              |                    |                     | 2021              |                    |                     |
|--|-------------------|--------------------|---------------------|-------------------|--------------------|---------------------|
|  | Índex de maduresa | Nivell de maduresa | Índex de compliment | Índex de maduresa | Nivell de maduresa | Índex de compliment |
| <b>CBCS 1</b> Inventari i control de dispositius físics                    | 24,8%             | <b>N1</b>          | 30,9%               | 24,8%             | <b>N1</b>          | 30,9%               |
| <b>CBCS 2</b> Inventari i control de programari autoritzat i no autoritzat | 45,5%             | <b>N1</b>          | 56,9%               | 45,5%             | <b>N1</b>          | 56,9%               |
| <b>CBCS 3</b> Procés continu d'identificació i solució de vulnerabilitats  | 25,6%             | <b>N1</b>          | 32,0%               | 29,6%             | <b>N1</b>          | 37,0%               |
| <b>CBCS 4</b> Ús controlat de privilegis administratius                    | 27,3%             | <b>N1</b>          | 34,2%               | 27,3%             | <b>N1</b>          | 34,2%               |
| <b>CBCS 5</b> Configuracions segures del programari i maquinari            | 20,0%             | <b>N1</b>          | 25,0%               | 20,0%             | <b>N1</b>          | 25,0%               |
| <b>CBCS 6</b> Registre de l'activitat dels usuaris                         | 37,4%             | <b>N1</b>          | 46,8%               | 37,4%             | <b>N1</b>          | 46,8%               |
| <b>CBCS 7</b> Còpies de seguretat de dades i sistemes                      | 54,8%             | <b>N2</b>          | 68,5%               | 54,8%             | <b>N2</b>          | 68,5%               |
| <b>CBCS 8</b> Compliment normatiu i governança de ciberseguretat           | 15,0%             | <b>N1</b>          | 18,8%               | 15,0%             | <b>N1</b>          | 18,8%               |
| <b>General</b>   | <b>31,3%</b>      | <b>N1</b>          | <b>39,1%</b>        | <b>31,8%</b>      | <b>N1</b>          | <b>39,8%</b>        |

L'índex de compliment dels CBCS és del 39,8% que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*. La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 únicament mostra una lleu millora en un dels controls. En conjunt, aquesta millora és clarament insuficient.

D'una manera més sintètica i gràfica, la situació observada dels controls queda reflectida en el gràfic 1, tant d'aquesta auditoria com de la realitzada l'any 2019.

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



La nostra auditoria i els indicadors reflecteixen la situació a 31 de desembre de 2021.

**L'Ajuntament de Torrevella no té establida una adequada governança de la ciberseguretat, tal com exigeix la normativa i un adequat sistema de control intern.**

**Aquesta situació ha de ser esmenada promptament i, a més, s'ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.**

Els òrgans superiors de l'Ajuntament (en particular l'alcalde i la Junta de Govern) són els responsables que hi haja uns controls de seguretat adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació que garantisca la ciberresiliència de l'entitat.

El compromís i conscienciació amb la ciberseguretat també s'ha d'estendre a la direcció<sup>2</sup> (tal com queda definida en el glossari al final d'aquest informe), que són els responsables d'articular i facilitar l'execució de les activitats establides per l'alta direcció en matèria de ciberseguretat.

Hi ha mancances rellevants que impedeixen que la governança puga considerar-se efectiva. En aquest sentit, la inexistència fins a l'any 2022 d'una política de seguretat de la informació de l'ajuntament, d'un comitè de seguretat i d'un responsable de seguretat, i particularment

<sup>2</sup> *Prontuario de ciberseguridad para entidades locales*, Centre Criptològic Nacional i Federació Espanyola de Municipis i Províncies, abril 2021.



la falta d'una cultura de la ciberseguretat i d'interés i compromís amb l'administració electrònica, la transformació digital i l'ús de mitjans tecnològics, ens permeten afirmar que l'Ajuntament de Torrevella no té establida una adequada governança de la ciberseguretat.

Encara que no s'han atés les nostres recomanacions a 31 de desembre de 2021, data de l'auditoria, hem constatat iniciatives posteriors per part de la corporació per a reconduir la situació i hem observat un canvi de tendència respecte al compromís de la corporació amb la seguretat de la informació i l'administració electrònica.

Aquest compromís s'ha materialitzat en determinats aspectes positius, particularment l'aprovació de la política de seguretat de la informació, el nomenament del comitè de seguretat (que encara no ha entrat en funcionament en el moment de finalització del treball de camp de l'auditoria) i del responsable de seguretat, la creació d'un càrrec directiu amb dedicació exclusiva per a la gestió TIC, la implantació d'una plataforma per a la gestió electrònica d'expedients i procediments administratius o l'articulació de projectes que tenen com a objecte promoure la seguretat de la informació i aconseguir el compliment normatiu.

Finalment, es urgent solucionar les mancances identificades assenyalades amb detall en l'Informe, ja que afecten de manera negativa el nivell de seguretat de la informació.

### **El grau de compliment de la normativa relativa a la seguretat de la informació és molt deficient.**

La revisió del compliment de legalitat en matèria relacionada amb la seguretat de la informació ha posat de manifest un nivell de compliment de la normativa molt deficient. Hi ha incompliments significatius generalitzats, que s'assenyalen en l'apartat 5, sobre els quals s'ha d'actuar per a una ràpida esmena.

## **5. RECOMANACIONS I MESURES NECESSÀRIES PER AL COMPLIMENT DE LA LEGALITAT**

Per a esmenar les deficiències de control identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 4 anterior, reformulem les recomanacions que es van efectuar en l'auditoria de 2019, considerant, si és el cas, les millores realitzades des d'aquell moment. L'Ajuntament haurà de dedicar els esforços i recursos necessaris per a esmenar les deficiències pendents.

També s'assenyalen les mesures per al compliment de la legalitat que han d'adoptar-se.

### **Sobre l'inventari i control de dispositius físics (CBCS 1)**

1. Aprovar formalment un procediment per a la gestió de l'inventari i el control d'actius físics que reculli el procés complet, incloent-hi el calendari per a les revisions periòdiques de maquinari i actualitzant degudament l'inventari.



En cas de viabilitat tècnica, integrar en el sistema d'inventari la detecció automàtica dels elements del sistema d'informació que actualment es realitza de manera manual.

2. Finalitzar la implantació de la solució adquirida per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

### **Sobre l'inventari i control de programari autoritzat (CBCS 2)**

3. Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga:
  - L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques de programari.
  - La definició d'un pla de manteniment de la totalitat del programari utilitzat a l'Ajuntament.
4. Finalitzar el procés de renovació en curs per a actualitzar tots els sistemes que es troben fora del període de suport.

### **Sobre el procés continu d'identificació i solució de vulnerabilitats (CBCS 3)**

5. Establir un procediment d'identificació i solució de vulnerabilitats que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:
  - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i el seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat.
  - La priorització de les vulnerabilitats identificades basada en l'anàlisi dels riscos, així com la resolució i documentació, identificant dates, prioritat, responsable, solució, etc.
6. Fer extensiu l'ús de l'eina de gestió unificada de pedaços de seguretat a tots els sistemes de l'entitat.

### **Sobre l'ús controlat de privilegis administratius (CBCS 4)**

7. Formalitzar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga:



- L'eliminació de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats d'administració hauran de realitzar-se amb usuaris nominatius.
- Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.
- La utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives).
- La política d'autenticació a aplicar a aquest tipus de comptes.

### **Sobre les configuracions segures del programari i maquinari (CBCS 5)**

8. Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del Centre Criptològic Nacional.<sup>3</sup>

Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà de procediment manual o a través d'eines automatitzades de monitoratge de la configuració.

### **Sobre el registre de l'activitat dels usuaris (CBCS 6)**

9. Aprovar formalment un procediment per al tractament de *logs* d'auditoria de l'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.

### **Sobre la còpia de seguretat de dades i sistemes (CBCS 7)**

10. Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes, que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de

---

<sup>3</sup> Les guies STIC (seguretat de les tecnologies de la informació i de les comunicacions) estan estructurades en sèries. Les sèries a què fa referència la recomanació corresponen a "guies generals", "guies d'entorns Windows" i "guies d'altres entorns" respectivament.



les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.

11. Adequar les condicions físiques de les instal·lacions del CPD, que alberguen les còpies de seguretat, per a proporcionar el nivell de protecció requerit per aquestes còpies i garantir la seguretat de les dades emmagatzemades.

### **Sobre el compliment normatiu i governança de la ciberseguretat (CBCS 8)**

12. Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de:

- Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriuen.
- Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010.
- Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.
- Encara que s'ha aprovat en 2022 la creació del comitè de seguretat i nomenat el responsable de seguretat, la seua existència no ha de ser solament formal, sinó que han de mantindre una activitat contínua i proactiva.

13. En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular, ha de:

- Finalitzar l'elaboració del registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.
- Fer una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.
- Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.
- Planificar i executar auditories en matèria de protecció de dades.

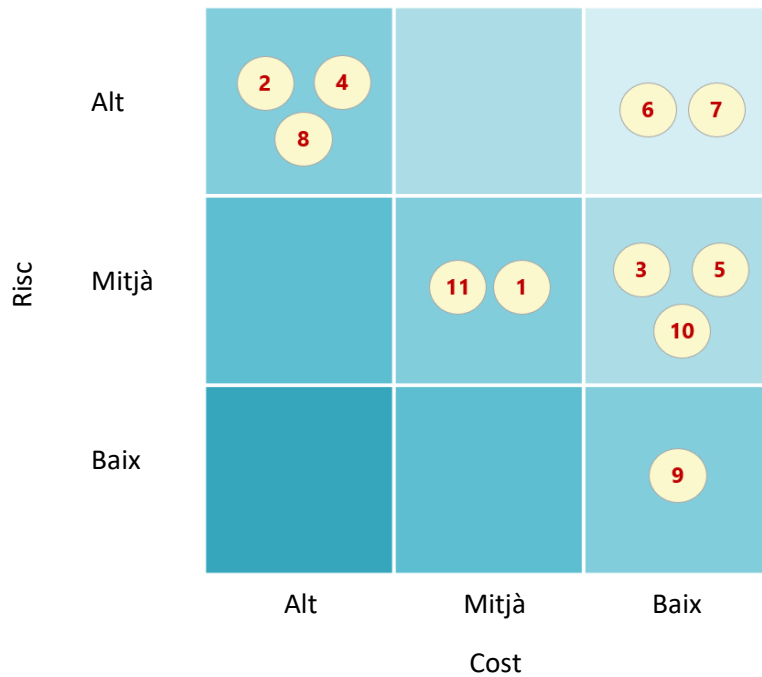
### **Priorització de les recomanacions**

A fi que puguem establir-se accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial a mitigar** i **cost estimat de la seua implantació**. Aquest gràfic no ha sigut modificat



respecte a l'informe de 2019, considerant que no s'ha realitzat cap millora significativa des d'aquell moment. No s'hi inclouen els punts 12 i 13 anteriors, ja que són mesures de compliment obligat.

**Gràfic 2. Riscos que s'atenen i cost d'implantació de les recomanacions**



### Seguiment de recomanacions anteriors

Hem realitzat un seguiment de les recomanacions efectuades en l'informe d'auditoria de l'any 2019.

Tal com es mostra en el quadre 2, de les tretze recomanacions realitzades en aquell informe, set no s'han atés i sis ho han sigut només parcialment.



## Quadre 2. Seguiment de recomanacions

| Recomanacions de l'informe anterior   | Situació a 31 de desembre de 2021 respecte a l'informe anterior   | Estat de la recomanació     | Conseqüència en l'informe              |
|---|---|-----------------------------|--|
| <p><b>1</b> Aprovar formalment un procediment per a la gestió de l'inventari i el control d'actius físics que reculla el procés complet, incloent-hi el calendari per a les revisions periòdiques de maquinari i actualitzant degudament l'inventari.</p> <p>En cas de viabilitat tècnica, integrar en el sistema d'inventari la detecció automàtica dels elements del sistema d'informació que actualment es realitza de manera manual.</p>  | Sense variació.   | <b>No aplicada</b>          | Es manté la redacció.                  |
| <p><b>2</b> Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.</p>  | S'ha adquirit una solució que permetrà l'aplicació de mesures tècniques per a limitar la connexió de dispositius, però aquest fet no és considerat en el càlcul dels índexs de maduresa per trobar-se el projecte en una fase inicial i haver-se adquirit amb posterioritat al 31 de desembre de 2021, però sí que considerem que la recomanació està parcialment aplicada. | <b>Aplicada parcialment</b> | S'actualitza la redacció feta en 2019. |
| <p><b>3</b> Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga:</p> <ul style="list-style-type: none"> <li>- L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques de programari.</li> <li>- La definició d'un pla de manteniment de la totalitat del programari utilitzat, incloent-hi tant el gestionat per mitjà de licitacions i clàusules contractuals com la resta de programari utilitzat a l'Ajuntament.</li> </ul> | Sense variació.   | <b>No aplicada</b>          | Es manté la redacció.                  |





| Recomanacions de l'informe anterior   | Situació a 31 de desembre de 2021 respecte a l'informe anterior  | Estat de la recomanació     | Conseqüència en l'informe                     |
|---|--|-----------------------------|---|
| <p>4 Revisar i actualitzar tots els sistemes que es troben fora del període de suport.</p>  | <p>L'Ajuntament ha realitzat dues auditories que han permès identificar tots els sistemes fora del període de suport del fabricant.</p> <p>L'Ajuntament ha actualitzat part dels equips d'usuari que tenien els sistemes operatius sense suport del fabricant. A més, s'ha iniciat la contractació d'un subministrament d'equips d'usuari per a renovació del parc actual, però aquest fet no és considerat en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021.</p> | <p>Aplicada parcialment</p> | <p>S'actualitza la redacció feta en 2019.</p> |
| <p>5 Establir un procediment d'identificació i solució de vulnerabilitats que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:</p> <ul style="list-style-type: none"> <li>- La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i el seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat.</li> <li>- La priorització de les vulnerabilitats identificades basada en l'anàlisi dels riscos, així com la resolució i documentació, identificant dates, prioritat, responsable, solució, etc.</li> </ul> | <p>L'Ajuntament ha realitzat el desplegament de l'eina microCLAUDIA del CCN en els sistemes i equips d'usuari de l'entitat. No obstant això, no ha sigut possible confirmar el desplegament de l'eina en tots els dispositius d'usuari a causa de les mancances en l'inventari de dispositius, que limiten l'efectivitat de la mesura.</p>   | <p>Aplicada parcialment</p> | <p>Es manté la redacció.</p>                  |
| <p>6 Fer extensiu l'ús de l'eina de gestió unificada de pedaços de seguretat a tots els elements de l'entitat.</p>  | <p>L'Ajuntament ha iniciat la integració d'equips d'usuari en el domini de l'Ajuntament, la qual cosa permet la gestió centralitzada de pedaços i actualitzacions per mitjà d'eines específiques. No obstant això, aquesta mesura té una eficàcia limitada, ja que la integració en el domini només s'ha realitzat per a un reduït nombre d'equips, i particularment a causa de l'ús d'una versió obsoleta de l'eina de gestió de pedaços i actualitzacions.</p>   | <p>Aplicada parcialment</p> | <p>Es manté la redacció.</p>                  |



| Recomanacions de l'informe anterior   | Situació a 31 de desembre de 2021 respecte a l'informe anterior | Estat de la recomanació | Conseqüència en l'informe |
|---|---|-------------------------|---------------------------|
| <p>Formalitzar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga:</p> <ul style="list-style-type: none"> <li>- L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió hauran de realitzar-se amb usuaris nominatius.</li> </ul> <p><b>7</b> - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.</p> <ul style="list-style-type: none"> <li>- La utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives).</li> <li>- La política d'autenticació a aplicar a aquesta mena de comptes.</li> </ul> | Sense variació.   | <b>No aplicada</b>      | Es manté la redacció.     |
| <p>Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del Centre Criptològic Nacional.</p> <p><b>8</b> Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà de procediment manual o a través d'eines automatitzades de monitoratge de la configuració.</p>  | Sense variació.   | <b>No aplicada</b>      | Es manté la redacció.     |



| Recomanacions de l'informe anterior  | Situació a 31 de desembre de 2021 respecte a l'informe anterior  | Estat de la recomanació     | Conseqüència en l'informe              |
|--|--|-----------------------------|--|
| <p><b>9</b> Aprovar formalment un procediment per al tractament de <i>logs</i> d'auditoria de l'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels <i>logs</i>. Per a la revisió de <i>logs</i> és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.</p>  | Sense variació.  | <b>No aplicada</b>          | Es manté la redacció.                  |
| <p><b>10</b> Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.</p>  | Sense variació.  | <b>No aplicada</b>          | Es manté la redacció.                  |
| <p><b>11</b> Adequar les condicions físiques de les instal·lacions del CPD, que alberguen les còpies de seguretat, per a proporcionar el nivell de protecció requerit per aquestes còpies i garantir la seguretat de les dades emmagatzemades.</p>   | Sense variació.  | <b>No aplicada</b>          | Es manté la redacció.                  |
| <p><b>12</b> Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de:</p> <ul style="list-style-type: none"> <li>- Elaborar i aprovar la política de seguretat per l'òrgan competent.</li> <li>- Designar les persones per als rols definits en la política de seguretat i constitució dels òrgans que s'hi descriuen.</li> <li>- Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriuen.</li> <li>- Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010.</li> <li>- Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.</li> </ul> | <p>Sense variació en 2021.</p> <p>S'ha elaborat i aprovat l'any 2022 la política de seguretat. Aquesta política inclou la designació de les persones per als rols definits, la constitució del comitè de seguretat i els membres d'aquest comitè.</p> <p>Encara que aquest fet no és considerat en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021, sí que ho tenim en compte per a actualitzar la nostra recomanació.</p> <p>A més, els òrgans i rols de seguretat han de desenvolupar una activitat real i proactiva.</p> | <b>Aplicada parcialment</b> | S'actualitza la redacció feta en 2019. |
| <p><b>13</b> En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de:</p>   | Sense variació en 2021.  | <b>Aplicada parcialment</b> | S'actualitza la redacció feta en 2019. |



| Recomanacions de l'informe anterior  | Situació a 31 de desembre de 2021 respecte a l'informe anterior  | Estat de la recomanació | Conseqüència en l'informe |
|--|--|-------------------------|---------------------------|
| <ul style="list-style-type: none"> <li>- Nomenar un DPD d'acord amb el que es preveu en l'article 37.1.a de l'RGPD.</li> <li>- Elaborar el registre d'activitats de tractament amb la informació requerida en l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.</li> <li>- Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.</li> <li>- Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.</li> <li>- Planificar i executar auditories en matèria de protecció de dades.</li> </ul> | <p>S'ha contractat l'any 2022 un servei extern que assumeix les funcions del delegat de protecció de dades. En el moment de la revisió es trobava en procés d'elaboració del registre d'activitats del tractament.</p> <p>Encara que aquest fet no és considerat en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021, sí que ho tenim en compte per a actualitzar la nostra recomanació.</p> |                         |                           |



## Actuacions en curs

Encara que no s'han tingut en compte en el càlcul dels indicadors mostrats en l'apartat 4, hem verificat que en el moment de finalització del treball de camp de l'auditoria s'han iniciat o planificat actuacions en matèria de ciberseguretat en diversos àmbits que atendrien algunes de les recomanacions anteriors. Aquestes actuacions es troben alineades amb els objectius de l'Ajuntament per a l'adequació a l'ENS i algunes s'han iniciat a conseqüència de les recomanacions realitzades en l'auditoria de l'any 2019. La implantació efectiva d'aquestes actuacions tindrà un impacte positiu en el nivell de ciberseguretat de l'entitat.

Enumerem a continuació les actuacions que es troben en execució quan es va emetre aquest informe i que per la seua rellevància cal destacar:

- S'ha iniciat la contractació d'un projecte per a millorar el condicionament físic del CPD existent.
- S'ha iniciat un projecte per a la construcció d'un segon CPD, la qual cosa permetrà la instal·lació de sistemes i l'aplicació de mesures que tindran un efecte positiu en la disponibilitat i protecció de dades i serveis proporcionats per l'Ajuntament.
- L'Ajuntament ha adjudicat l'any 2022 un projecte per a l'adquisició d'una plataforma de seguretat que inclou la instal·lació d'un tallafoç d'última generació i d'agents de protecció d'*endpoint*, que permetrà l'aplicació de mesures tècniques amb un alt impacte en la seguretat de les xarxes i dispositius de l'Ajuntament.
- L'Ajuntament es troba en procés de licitació d'un projecte per a la renovació completa del parc microinformàtic municipal, que proporciona els mitjans tècnics que possibiliten el teletreball i el treball en mobilitat de manera segura i de confiança i assegura l'ús d'elements de maquinari i programari amb les últimes versions i suport del fabricant.
- L'Ajuntament ha iniciat els treballs per al desplegament de serveis i eines proporcionats pel CSIRT-CV, com a part de les accions del Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana, i s'han iniciat accions per a la licitació de solucions finançades per mitjà dels fons europeus Next Generation EU. Entre les actuacions previstes es troben:
  - La posada en servei d'un centre d'operacions de seguretat.
  - El desplegament d'un sistema amb funcionalitats SIEM i EDR.
- S'han iniciat accions per a reorganització i millora dels recursos humans relacionats amb la seguretat de la informació, que inclouen les mesures següents:
  - Hi ha prevista la contractació de dos tècnics informàtics per a reforçar de manera urgent el personal del departament.



- Proposta de reforma de l'RLT, que inclou una dotació de personal adequada a les necessitats departamentals.



**APÈNDIX 1**  
**Metodologia aplicada**



## Introducció

Cada vegada un major nombre d'aspectes de la gestió pública es realitzen amb el suport de complexos sistemes informatitzats, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de tota classe provinents del ciberespai, majors riscos de ciberseguretat i s'han multiplicat els incidents de seguretat dels quals són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials –i en molts casos, reals– tant econòmiques com en la prestació dels serveis públics.

Les entitats locals, i els ajuntaments en particular, no són alienes a aquesta problemàtica de la ciberseguretat en la seua mateixa operatòria, per la qual cosa han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat, que és **de compliment obligat**.

Per aquestes raons, és imperatiu que els responsables dels ajuntaments gestionen els riscos associats amb el funcionament i ús dels sistemes d'informació que s'utilitzen per a desenvolupar i prestar els serveis públics. Així mateix, han d'establir controls de ciberseguretat adequats per a mantindre els sistemes d'informació protegits davant de les amenaces de seguretat i evitar la interrupció en els serveis prestats als ciutadans i ajuntaments.

La gestió dels riscos de ciberseguretat comprén una àmplia gamma d'activitats orientades a protegir els sistemes d'informació i les dades davant d'accessos no autoritzats i altres amenaces cibernètiques, detectar anomalies i incidents que els afecten negativament i mitigar el seu impacte, i també respondre i recuperar-se d'incidents.

Tot i que l'adopció de mesures de seguretat adequades fa més resilients les organitzacions davant dels ciberatacs, l'anàlisi dels incidents produïts que es realitza en els informes INES<sup>4</sup> del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs es mantinguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan correctament implementades.

En definitiva, l'existència d'uns controls eficaços de ciberseguretat és un element essencial per a la prestació de serveis públics d'una administració tecnològicament avançada. En aquest sentit considerem que **la implantació dels controls bàsics de ciberseguretat (CBCS)** –un subconjunt de les mesures de seguretat obligatòries exigides per l'ENS–, **constitueix una mesura bàsica de ciberhigiene** per a les administracions públiques.

---

<sup>4</sup> Informe Nacional de l'Estat de Seguretat dels Sistemes de les TIC del CCN.





## Objectiu de l'auditoria

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022, el nostre objectiu ha sigut realitzar el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Torrevella. Exercici 2019 i obtenir una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats, i proporcionar una avaluació tant sobre el seu disseny<sup>5</sup> com sobre la seua eficàcia operativa<sup>6</sup> per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport, així com sobre el compliment de la normativa bàsica relativa a la seguretat de la informació.

També formulem recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control, tenint en consideració les millores introduïdes des de la nostra auditoria anterior.

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada dels huit CBCS revisats en l'auditoria de l'any 2019 relacionats amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interés general.

## Abast

L'auditoria s'ha centrat en l'anàlisi de la situació dels huit CBCS:

- 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 i governança de ciberseguretat

Atesa la naturalesa de l'objecte material que cal revisar –la gran amplitud, complexitat i diversitat dels sistemes d'informació d'un ens local de grans dimensions–, ha sigut necessari delimitar i concretar quins sistemes s'havien d'analitzar. En aquest sentit, hem analitzat les

---

<sup>5</sup> L'avaluació del disseny d'un control implica la consideració per l'auditor de si el control, de manera individual o en combinació amb altres controls, és capaç de previndre de manera eficaç, o de detectar i corregir, la materialització dels riscos previstos. És a dir, és capaç de complir l'objectiu de control.

<sup>6</sup> L'auditor comprova que el control existeix i que l'entitat l'està utilitzant.



aplicacions que suporten els processos de gestió comptable i pressupostària i la gestió tributària i recaptadora, així com els controls que tenen implantats.

Adicionalment, per la seua importància per al bon funcionament dels sistemes d'informació i la ciberseguretat, hem analitzat els següents tipus d'elements:

- controlador de domini
- programari de virtualització
- equips d'usuari (una mostra)
- elements de la xarxa de comunicacions (una mostra)
- elements de seguretat (una mostra)

### Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls a 31 de desembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe, ja que fins a aquell moment s'ha admés qualsevol evidència disponible. Per tant, amb caràcter general l'Informe 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 són considerades d'aquesta manera en les conclusions i en els indicadors.

Adicionalment, les constatacions de l'auditoria, les conclusions i l'esborrany previ de l'informe es discuteixen amb els responsables de l'entitat auditada, d'acord amb el que s'estableix en el nostre *Manual de fiscalització*.

### Metodologia

Hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura i recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica, com també que planifiquem i executem l'auditoria amb la finalitat d'obtenir una seguretat limitada sobre la situació dels CBCS revisats.

Som independents de l'entitat auditada, de conformitat amb els requeriments d'ètica i protecció de la independència exigits per la normativa reguladora de l'activitat d'auditoria dels òrgans de control extern i per l'article 8 de l'LSC.

La Unitat d'Auditoria de Sistemes d'Informació de la Sindicatura de Comptes (UASI) ha realitzat aquesta auditoria dels controls bàsics de ciberseguretat seguint la metodologia establida en la guia pràctica de fiscalització GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat (CBCS)".



Hem avaluat la situació dels CBCS utilitzant el model de nivell de maduresa dels processos, definit en l'apèndix 1 de la guia esmentada, ja que, a més de ser un sistema àmpliament acceptat, permet establir objectius, realitzar comparacions entre entitats diferents i veure'n l'evolució al llarg del temps.

## La guia pràctica de fiscalització dels OCEX 5313

La guia pràctica de fiscalització dels OCEX GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat", va ser aprovada per la Conferència de Presidents dels Òrgans de Control Extern el 12 de novembre de 2018, i forma part del *Manual de fiscalització* de la Sindicatura de Comptes, 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. 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 triar els més rellevants es va atendre el marc conceptual establert per la prestigiosa organització Center for Internet Security (CIS),<sup>7</sup> que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. 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%.

Es van triar els set CBCS més rellevants i se'n va afegir un huité relacionat amb el compliment normatiu, per la seua importància en una administració pública. En aquest informe hem destacat, a més, els aspectes relacionats amb la governança de ciberseguretat establerts en l'ENS i en l'RGPD.

## Alineació dels CBCS amb l'Esquema Nacional de Seguretat

Atés que l'ENS és de compliment obligat per a tots els ens públics, s'ha tingut especial cura que la metodologia d'auditoria dels controls bàsics de ciberseguretat estiguera 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 són requerits per l'ENS. D'aquesta manera, els huit controls bàsics de ciberseguretat presenten una correspondència (no exacta) amb les referències següents de l'ENS:

---

<sup>7</sup> Center for Internet Security, <[www.cisecurity.org](http://www.cisecurity.org)>.



### 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<br>op.exp.2          |
| CBCS 3 Procés continu d'identificació i solució de vulnerabilitats  | mp.sw.2<br>op.exp.4           |
| CBCS 4 Ús controlat de privilegis administratius                    | op.acc.4<br>op.acc.5          |
| CBCS 5 Configuracions segures del programari i maquinari            | op.exp.2<br>op.exp.3          |
| CBCS 6 Registre de l'activitat dels usuaris                         | op.exp.8<br>op.exp.10         |
| CBCS 7 Còpies de seguretat de dades i sistemes                      | mp.info.9                     |
| CBCS 8 Compliment normatiu i governança de la ciberseguretat        |                               |

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

### Els CBCS com a mesures de ciberhigiene

La European Union Agency for Cybersecurity (ENISA) assenyala<sup>8</sup> que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a 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.<sup>9</sup>

Sintetitzant, la ciberhigiene es refereix 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.<sup>10</sup>

En aquesta direcció, ENISA estableix deu punts d'acció per a una ciberhigiene adequada. Com s'observa en el quadre 4, dels set CBCS, sense comptar el de compliment normatiu, cinc són coincidents amb els punts d'acció prioritariats recomanats per ENISA com a bones pràctiques de ciberhigiene.

<sup>8</sup> [Review of Cyber Hygiene Practices](#), ENISA, desembre de 2016. Vegeu-ne la pàgina 14.

<sup>9</sup> Segons experts citats en l'informe [DOD Needs to Take Decisive Actions to Improve Cyber Hygiene](#), de la US Government Accountability Office (2020), fins al 90% dels ciberatacs podrien evitar-se implantant mesures adequades de ciberhigiene.

<sup>10</sup> Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* <[https://resources.sei.cmu.edu/asset\\_files/Presentation/2017\\_017\\_001\\_508771.pdf](https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf)>, 2017.



#### Quadre 4. 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'hi han posat correctament els pedaços | CBCS 2 |
| 3. Utilitzar guies de configuració segura i fortificació per a tots els dispositius                       | CBCS 5 |
| 4. Gestionar les dades que entren i ixen de la 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 |

A l'efecte d'aquest treball, considerem que els CBCS constitueixen un conjunt de pràctiques i accions bàsiques per a mantindre una adequada ciberhigiene.

També pot consultar-se el nostre [Informe d'auditoria dels controls bàsics de ciberseguretat dels majors ajuntaments de la Comunitat Valenciana. Exercicis 2019 i 2020](#), en l'apartat 5 del qual expliquem per què són importants els CBCS.

#### **Críteris d'auditoria: els controls bàsics de ciberseguretat i els seus subcontrols**

Utilitzem els controls bàsics de ciberseguretat com a críteris d'auditoria o críteris d'avaluació. Els CBCS són controls globals formats per 26 subcontrols detallats, tal com es mostra en el quadre següent. Totes les nostres comprovacions tenen com a objectiu contrastar la situació real dels subcontrols en l'entitat davant de les bones pràctiques recollides en la GPF-OCEX 5313, en les quals s'especifica amb el màxim detall els aspectes comprovats en cada control.



### Quadre 5. Els CBCS i els seus subcontrols

| Control  | Objectiu del control  | Subcontrol   |  |
|--|---|--|--|
| <b>CBCS 1</b><br>Inventari i control de dispositius físics                   | Gestionar activament tots el dispositius 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.                                    |
| <b>CBCS 2</b><br>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 programari autoritzat             | L'entitat disposa d'un inventari de programari complet, actualitzat i detallat.  |
|  |   | CBCS 2-2: Programari suportat pel fabricant              | El programari 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 programari no autoritzat            | L'entitat disposa de mecanismes que impedeixen la instal·lació i execució de programari no autoritzat.   |
| <b>CBCS 3</b><br>Procés continu d'identificació i solució de vulnerabilitats | Disposar d'un procés continu per a obtenir informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.                  | CBCS 3-1: Identificació de vulnerabilitats               | Hi ha 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 fa 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.                            |
| <b>CBCS 4</b><br>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 en facilita el correcte control.      |
|  |   | CBCS 4-2: Canvi de contrasenyes per defecte              | Les contrasenyes per defecte dels comptes que no s'utilitzen o bé 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   |  |
|--|--|--|--|
| <b>CBCS 5</b><br>Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors | Establir, implantar i gestionar la configuració de seguretat, 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 estàndards de configuració segura per a tots els sistemes operatius i programari.   |
|  |  | 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.   |
| <b>CBCS 6</b><br>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 ( <i>security information and event management</i> ) o una eina d'anàlisi de logs per a realitzar correlació i anàlisi de logs.  |
| <b>CBCS 7</b><br>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 permeti 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 fa un procés de recuperació de dades que permeti 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.  |
| <b>CBCS 8</b><br>Compliment normatiu i governança de ciberseguretat  | L'entitat compleix els requisits legals i reglamentaris que li són aplicables i té establida una adequada governança de ciberseguretat.  | 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.   |



## Avaluació dels resultats del treball

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

### Subcontrols

Els CBCS són controls globals compostos per diversos controls detallats o subcontrols (tal com es pot veure en el quadre 5 anterior), dels quals hem revisat tant el disseny com l'eficàcia operativa.

El treball d'auditoria consisteix bàsicament a avaluar cada subcontrol en funció dels resultats de les proves realitzades i de les evidències obtingudes. Cada subcontrol s'avalua segons l'escala mostrada en el quadre següent:

#### Quadre 6. Avaluació dels subcontrols

| Avaluació                                | Descripció   |
|--|--|
| <b>Control efectiu</b>                   | <p>Cobreix al 100% l'objectiu de control i:</p> <ul style="list-style-type: none"><li>- El procediment està formalitzat (documentat i aprovat) i actualitzat.</li><li>- El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.</li></ul>  |
| <b>Control bastant efectiu</b>           | <p>En línies generals, compleix l'objectiu de control, si bé pot haver-hi certs aspectes no coberts al 100% i:</p> <ul style="list-style-type: none"><li>- Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.).</li><li>- Les proves realitzades per a verificar la implementació són satisfactòries.</li><li>- S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.</li></ul>   |
| <b>Control poc efectiu</b>               | <p>Cobreix de forma molt limitada l'objectiu de control i:</p> <ul style="list-style-type: none"><li>- Se segueix un procediment, encara que aquest pot no estar formalitzat.</li><li>- El resultat de les proves d'implementació i d'eficàcia no és satisfactori.</li></ul> <p>Cobreix en línies generals l'objectiu de control, però:</p> <ul style="list-style-type: none"><li>- No se segueix un procediment clar.</li><li>- 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).</li></ul> |
| <b>Control no efectiu o no implantat</b> | <p>No cobreix l'objectiu de control.</p> <p>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).</p>   |

### Controls

Per a determinar la situació global de cada control de ciberseguretat 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 CCN, usant una escala que es resumeix en el quadre següent.

#### Quadre 7. Nivells de maduresa

| Nivell                                   | Índex | Descripció  |
|--|-------|---|
| <b>N0</b><br>Inexistent                  | 0     | El control no s'està aplicant en aquest moment.   |
| <b>N1</b><br>Inicial /<br>ad hoc         | 10    | El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat.<br><i>L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depèn 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 depèn de tindre personal d'alta qualitat.</i>  |
| <b>N2</b><br>Repetible,<br>però intuïtiu | 50    | Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives.<br><i>L'eficàcia del procés depèn de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredecible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.</i>   |
| <b>N3</b><br>Procés definit              | 80    | Els processos estan estandarditzats, documentats i comunicats amb accions formatives.<br><i>Es disposa d'un catàleg de processos que es manté actualitzat. Aquests 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 d'allò desconegut (o no planificat).</i><br><i>L'èxit és més que bona sort: es mereix.</i><br><i>Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2 i que sí que es gestiona en el nivell 3.</i> |
| <b>N4</b><br>Gestionat<br>i mesurable    | 90    | La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix.<br><i>Es disposa d'un sistema de mesures i mètriques per a conèixer 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.</i><br><i>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, la confiança era solament qualitativa.</i>   |
| <b>N5</b><br>Optimitzat                  | 100   | Se segueixen bones pràctiques en un cicle de millora contínua.<br><i>El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.</i><br><i>S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, utilitzant-se com a indicadors en la gestió de la millora dels processos.</i><br><i>En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes a base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.</i>  |



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 comprovació de la seua aplicació pràctica.

Per a avaluar el nivell de maduresa de cada control s'han tingut en compte els resultats obtinguts en la revisió dels subcontrols que el formen.

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

### 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.

A fi de poder determinar l'impacte que tindria sobre l'organització un incident d'aquest tipus, i de poder establir la categoria del sistema, s'han de tindre en compte les **cinc dimensions de la seguretat** que els controls de ciberseguretat han de garantir:

|                  |   |
|------------------|---|
| 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, assegurant que no se n'ha produït l'alteració, pèrdua o destrucció, ja siga de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals. |
| Disponibilitat   | Es tracta de la capacitat d'un servei, un sistema o una informació, de ser accessible i utilitzable pels usuaris o processos autoritzats quan aquests ho requerisquen.  |



**Autenticitat** És la propietat o característica consistent en el fet que una entitat és qui 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'adscriurà 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 aconseguix el nivell ALT.
- b) Un sistema d'informació serà de categoria MITJANA si alguna de les seues dimensions de seguretat aconseguix el nivell MITJÀ, i cap aconseguix un nivell superior.
- c) Un sistema d'informació serà de categoria BÀSICA si alguna de les seues dimensions de seguretat aconseguix el nivell BAIX, i cap aconseguix 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 a què 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:<sup>11</sup>

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

Els sistemes auditats en aquest informe són considerats a l'efecte de l'ENS com de categoria MITJANA i el nivell de maduresa requerit o objectiu és *N3, procés definit*, i un índex de maduresa del 80%.

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

<sup>11</sup> Guia de seguretat de les TIC. CCN-STIC 824. Informe Nacional de l'Estat de Seguretat dels Sistemes TIC.



## Indicadors globals

A l'efecte de l'ENS, la guia CCN-STIC-824 inclou 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 la seua aplicació als CBCS, ja que permeten dur a terme un resum de l'estat de les mesures de seguretat dels ens auditats:

- L'**índex de maduresa** sintetitza, en tant per cent, el nivell de maduresa aconseguït per un organisme respecte del conjunt de controls de ciberseguretat.
- L'**índex de compliment** analitza igualment el nivell de maduresa aconseguït, 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 exigít per a aquesta categoria en l'ENS, que en aquesta auditoria és N3 (80%) per a tots els casos.

## Governança de ciberseguretat

A l'efecte d'aquest treball, s'entendrà per governança de la seguretat de la informació i les comunicacions o de ciberseguretat (termes que utilitzem de manera indistinta en aquest informe) el conjunt de responsabilitats i activitats realitzades per l'alta direcció amb l'objectiu de proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconsegueixen els objectius, verificar que el risc es gestiona adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una manera responsable.<sup>12</sup>

Els principals elements d'una adequada governança de ciberseguretat estan implícits en l'ENS i la normativa relativa a la protecció de dades de caràcter personal, normes que revisem en el CBCS 8. Atesa la seua importància nuclear per a la ciberresiliència de l'entitat destaquem de manera explícita la nostra avaluació de la governança existent.

La governança és el procés d'establir i mantindre un marc de referència, i donar suport a l'estructura i els processos de gestió per a garantir la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de les dades.

És més que una mera qüestió tècnica, per la qual cosa **exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització.**<sup>13</sup>

La responsabilitat sobre aquest procés és de l'alta direcció, que, en el cas de les entitats locals, correspon al seu president i a la junta de govern. Ells són els responsables de garantir que el funcionament de l'organització resulta conforme amb les normes aplicables i que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions. La responsabilitat de l'execució de les activitats establides per l'alta direcció correspon als gestors, a la direcció executiva.

---

<sup>12</sup> Vegeu el [glossari de la Information Systems Audit and Control Association \(ISACA\)](#).

<sup>13</sup> Vegeu l'apartat 66 d'[Anàlisis núm. 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE](#) del Tribunal de Comptes Europeu.



La implicació dels òrgans superiors és, potser, el factor més important per a la implantació amb èxit d'un sistema de gestió de la seguretat de la informació o de ciberseguretat.<sup>14</sup> L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació<sup>15</sup> que ha de materialitzar-se en aspectes com ara:

- D'acord amb l'article 11 del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat, ha de formular-se la **política de seguretat de la informació (PSI) que ha de ser aprovada pel titular de l'òrgan superior** de l'entitat. Aquesta PSI s'ha de difondre entre la totalitat dels membres de l'organització, com també, si és el cas, a proveïdors i tercers.
- Assignar els rols i responsabilitats en matèria de seguretat de la informació. Els òrgans superiors de l'entitat han de nomenar el **responsable de la informació** (que pot tractar-se d'una persona o un òrgan col·legiat), el **responsable del servei** (que pot ser el mateix que l'anterior), el **responsable de la seguretat** i el **responsable del sistema**.

El procediment de nomenament formal dels responsables esmentats ha de constar en la política de seguretat de la informació de l'entitat.

- Autoritzar la implementació i operació d'un **comité de seguretat TIC**.

La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,<sup>16</sup> que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat, i és la màxima autoritat en l'organització respecte a les decisions de seguretat que afecten els sistemes que manegen informació o presten algun servei. La seua composició ha de constar en la PSI.

- **Proporcionar els recursos materials i humans** necessaris i assegurar que s'implanten programes de conscienciació, formació i capacitatció.

El manteniment actualitzat i la millora dels controls de ciberseguretat requerirà actuacions i inversions, tant en mitjans materials com personals, que han de ser adequadament planificades.

- Decidir els criteris d'acceptació del risc i els nivells acceptables de risc.
- Dirigir les revisions periòdiques de la PSI i vetlar per la realització de les auditories internes de seguretat.

---

<sup>14</sup> [Guía de iniciación a actividad profesional. Implantación de sistemas de gestión de la seguridad de la información \(SGSI\) según la norma ISO 27001](#), Col·legi Oficial d'Enginyers de Telecomunicació.

<sup>15</sup> [UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información](#), apartat 3.4.

<sup>16</sup> [Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC](#), CCN, gener de 2021.



## Seguiment de les recomanacions

En aquest treball s'ha realitzat el seguiment de les recomanacions recollides en l'apartat 6 de l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Torrevella. Exercici 2019.

En la valoració de la situació actual, s'ha seguit la GPF-OCEX 1735, "Les recomanacions i el seu seguiment", que proposa la categorització següent:

### Quadre 8. Situació de les recomanacions

|   |  |
|---|--|
| <b>Totalment o substancialment aplicada</b> | Si l'ens fiscalitzat ha adoptat les mesures correctores, raonables i proporcionades en l'esfera de les seues competències, que permeten considerar que la recomanació ha produït efectes i no ha quedat pendent de resolució cap qüestió d'importància significativa. En aquests casos s'entendrà que la recomanació s'ha complert raonablement. A més, s'ha obtingut evidència suficient que acredita les mesures adoptades.  |
| <b>Aplicada parcialment</b>                 | Si l'ens fiscalitzat ha pres en consideració les recomanacions i ha realitzat actuacions encaminades a corregir les deficiències, debilitats o insuficiències que s'han posat de manifest, però solament en un estat incipient, en una part o en alguns aspectes, la qual cosa no permet considerar que la recomanació s'ha complert raonablement.   |
| <b>No aplicada</b>                          | Si l'ens fiscalitzat no ha realitzat les actuacions encaminades a corregir les deficiències, debilitats o insuficiències que s'han posat de manifest o bé ho ha fet insuficientment o inadequadament de manera que la recomanació segueix sense aplicar-se.  |
| <b>Sense validesa en el marc actual</b>     | S'hi inclouen les recomanacions que, encara que vàlides i pertinents quan es va emetre l'informe i per a l'exercici fiscalitzat, i fins i tot sent acceptades i reconegudes per l'ens fiscalitzat, no poden aplicar-se en el context actual perquè no es donen les circumstàncies que ho permeten o la mateixa casuística que llavors, és a dir, no es donen en el moment actual els supòsits dels fets en funció dels quals es va efectuar la recomanació en el passat. La recomanació ha esdevingut inaplicable. |
| <b>No verificada</b>                        | S'inclouen en aquesta categoria les recomanacions que, encara que acceptades o fins i tot aplicades i corregides per l'ens fiscalitzat, necessitarien obligatòriament alguna prova addicional per a contrastar el que ha manifestat l'ens fiscalitzat que excedeixen l'abast previst en el treball.  |

En el quadre 2 es mostren les recomanacions contingudes en l'informe esmentat amb els comentaris relatius al seguiment realitzat i la situació a 31 de desembre de 2021.

## Comunicació i confidencialitat

Ens comuniquem amb els responsables de l'entitat en relació, entre altres qüestions, amb l'abast i el moment de realització de l'auditoria planificats i les constatacions significatives de l'auditoria, com també amb qualsevol deficiència significativa dels controls interns que identifiquem en el transcurs d'aquesta.

Atés que la informació utilitzada en l'auditoria té un caràcter sensible i pot afectar la seguretat dels sistemes d'informació, els resultats amb el màxim detall de cada un dels



controls revisats només es comuniquen amb caràcter confidencial als responsables de l'Ajuntament perquè puguin adoptar les mesures correctores que consideren necessàries. En aquest informe els resultats es mostren de manera sintètica.



## APÈNDIX 2

### Situació dels controls bàsics de ciberseguretat





## CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

### Objectiu del control

Gestionar activament (inventariar, revisar i corregir) els dispositius físics connectats en la xarxa, de manera que només els dispositius autoritzats tinguin accés a la xarxa.

### Situació del control

L'Ajuntament no ha fet canvis significatius respecte de la situació de l'inventari i control de dispositius físics que vam observar en la revisió anterior. Es realitzen accions de control com a part d'un procés que està implantat de manera general per a tots els sistemes de l'entitat, encara que aquest procés no es troba establert en un procediment formalment aprovat.

El procés d'inventari rep el suport de l'ús d'una eina específica, però únicament es realitza de manera automàtica per a un determinat subconjunt d'actius físics, mentre que la resta es fan de manera manual. L'inventari existent no es troba actualitzat.

No hi ha mesures orientades a controlar la connexió de dispositius físics no autoritzats a la xarxa corporativa. No obstant això, l'any 2022 s'ha adjudicat un contracte per al desplegament d'una solució de seguretat que inclou la instal·lació d'un tallafoc d'última generació i d'agents de protecció d'*endpoint*, la qual cosa permetrà l'aplicació de mesures tècniques per a limitar la connexió de dispositius a aquells que complisquen determinats criteris tècnics. Aquest projecte no s'ha considerat per a la valoració del control, atès que s'ha iniciat amb posterioritat al 31 de desembre de 2021.

El nivell de control sobre l'inventari i el control d'actius físics és insuficient, i la seua valoració global aconsegueix un **índex de maduresa del 24,8%**, que es correspon amb un **nivell de maduresa N1, inicial / ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 1 del 30,9%**, igual que el de la nostra auditoria anterior.

## CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

### Objectiu del control

Gestionar activament (inventariar, revisar i corregir) tot el programari, de manera que només es pugui instal·lar i executar programari autoritzat i que el no autoritzat siga detectat i se n'eviti la instal·lació i execució.

### Situació del control

L'Ajuntament no ha fet canvis significatius en aquest control des de la revisió anterior. Les accions realitzades com a part del procés de gestió del programari no s'han establert en un procediment aprovat.



Hem verificat que, si bé s'han realitzat determinades accions encaminades a actualitzar o substituir sistemes que es troben fora del període de suport del fabricant, en el moment de la revisió hi ha un elevat nombre de servidors i sistemes crítics que no han sigut actualitzats, un fet que suposa un greu risc per al sistema d'informació i constitueix una deficiència significativa.

L'Ajuntament ha contractat en els anys 2021 i 2022 la realització d'auditories de sistemes per a establir l'abast de les deficiències tècniques, incloent-hi la identificació de sistemes que es troben fora del període de suport, a fi d'iniciar les accions correctives necessàries. El resultat d'aquestes auditories s'està utilitzant per a planificar i iniciar els projectes que permeten, si s'executen, disposar de sistemes amb suport dels fabricants corresponents.

L'Ajuntament ha actualitzat part dels equips d'usuari que tenien els sistemes operatius sense suport del fabricant. A més, ha iniciat el procés de licitació d'un subministrament d'equips d'usuari per a la renovació completa del parc actual de l'Ajuntament, però no ha sigut considerat per a la valoració del control, atès que s'ha iniciat amb posterioritat al 31 de desembre de 2021.

Hi ha un insuficient nivell de control sobre l'inventari i control de programari autoritzat, amb un **índex de maduresa del 45,5%**, que es correspon amb un **nivell de maduresa N1, inicial / ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 2 del 56,9%**, igual que el de la nostra auditoria anterior.

### **CBCS 3. PROCÉS CONTINU D'IDENTIFICACIÓ I SOLUCIÓ DE VULNERABILITATS**

#### **Objectiu del control**

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

#### **Situació del control**

L'Ajuntament ha iniciat determinats canvis en el control, però aquests tenen un impacte limitat respecte a la gestió de vulnerabilitats que vam observar en l'auditoria anterior o no s'ha finalitzat la seua aplicació.

L'Ajuntament ha realitzat el desplegament de l'eina microCLAUDIA del CCN en els sistemes i equips d'usuari de l'entitat, eina que proporciona protecció contra codi nociu de tipus *ransomware*. No obstant això, i encara que hem verificat que la instal·lació s'ha realitzat de manera massiva, en el moment de la revisió no ha sigut possible confirmar el desplegament de l'eina en tots els dispositius d'usuari, a causa de les mancances en l'inventari i gestió de dispositius de l'Ajuntament, que limiten l'efectivitat de la mesura.

Adicionalment, s'ha iniciat recentment la integració d'equips d'usuari al domini de l'Ajuntament. Aquesta integració permet la gestió centralitzada de pedaços i actualitzacions



per a aquests equips per mitjà d'eines específiques, cosa que possibilita un control més eficient respecte a la gestió manual. No obstant això, aquesta mesura té una eficàcia limitada, ja que la integració en el domini només s'ha realitzat per a un nombre limitat d'equips d'usuari, i a més s'està utilitzant una versió obsoleta de l'eina de gestió de pedaços i actualitzacions.

El nivell de control és insuficient i la valoració global sobre aquest control aconseguix un **índex de maduresa del 29,6%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada, i suposa una lleu millora de 4 punts respecte de la nostra auditoria de 2019. Això representa un **índex de compliment del CBCS 3 del 37,0%**.

## CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

### Objectiu del control

Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'assignació i ús de privilegis administratius en els sistemes d'informació.

### Situació del control

L'Ajuntament no ha fet canvis significatius en l'ús controlat de privilegis administratius respecte de la situació observada en la revisió anterior. Es realitzen accions per al control dels comptes d'administració, però no hi ha un control efectiu ja que, si bé existeixen determinades mesures adequades per al control de comptes, aquestes no es troben implantades de manera homogènia en tots els sistemes i no han sigut formalment establides.

No existeix una política d'autenticació homogènia en tots els sistemes o la política aplicada no és robusta en tots els casos.

No s'han fet canvis respecte a l'ús de comptes d'administració no nominatius o per defecte, ni s'han creat comptes sense privilegis per a limitar l'ús de comptes amb privilegis d'administració únicament a tasques que ho requerisquen.

Hi ha un insuficient nivell de control sobre els comptes amb privilegis administratius i la valoració global del control suposa un **índex de maduresa del 27,3%**, que es correspon amb un **nivell de maduresa N1, inicial / ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment d'aquest CBCS 4 del 34,2%**, el mateix que en la nostra auditoria anterior.



## CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

### Objectiu del control

Establir una configuració base segura del programari i maquinari de 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.

### Situació del control

L'Ajuntament no ha fet canvis significatius respecte a les configuracions segures de programari i maquinari que vam observar en l'auditoria anterior i no disposa d'un procediment formalment aprovat. Encara que l'entitat aplica configuracions de seguretat en determinats sistemes i es disposa de plantilles per a la configuració d'alguns dispositius, aquestes accions no són suficients per a assegurar l'efectivitat del control.

No obstant això, en 2022 s'ha adjudicat un contracte per al desplegament d'una solució de seguretat que inclou la instal·lació d'un talla-foc d'última generació i d'agents de protecció d'*endpoint*, la qual cosa permetrà proporcionar un nivell de protecció addicional als dispositius d'usuari. A més, està preparant-se la licitació d'un projecte per al desplegament conjunt de sistemes SIEM i EDR, per mitjà de l'ús dels fons europeus Next Generation. Aquests projectes no s'han considerat per a la valoració del control, atès que les seues activitats s'han iniciat amb posterioritat al 31 de desembre de 2021.

Existeix, per tant, un deficient nivell de control en l'aplicació de configuracions segures en dispositius i programari, per la qual cosa s'haurà de dedicar esforços i recursos per a millorar-la. La valoració global del control aconsegueix un **índex de maduresa del 20,0%**, que es correspon amb un **nivell de maduresa N1, inicial / ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 25,0%**, igual que el de la nostra auditoria anterior.

## CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

### Objectiu del control

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

### Situació del control

No s'han fet canvis significatius respecte a la situació observada en l'auditoria anterior.

L'Ajuntament té habilitats els registres d'activitat en els sistemes revisats i hi ha controls en funcionament, però aquests controls s'apliquen de manera informal i no estan establits en



un procediment formalment aprovat. A més, no es realitza la centralització de registres d'auditoria, ni el personal de l'Ajuntament en fa una revisió de manera sistemàtica.

En aquells sistemes que per imperatiu legal han d'emmagatzemar la informació d'activitat dels usuaris durant un determinat període de temps, l'Ajuntament disposa d'un procés de gestió dels registres a fi d'assegurar el compliment d'aquests requisits legals.

Hem verificat que en 2022 s'està preparant la licitació d'un projecte per al desplegament conjunt de sistemes SIEM i EDR, per mitjà de l'ús dels fons europeus Next Generation, que si s'apliquen permetran millorar el control.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 37,4%**, que es correspon amb un **nivell de maduresa N1, inicial / ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 6 del 46,8%**. No s'ha produït cap variació respecte de la nostra auditoria anterior.

## CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

### Objectiu del control

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

### Situació del control

L'Ajuntament no ha fet canvis significatius respecte a la situació observada en la revisió anterior, ni s'ha aprovat un procediment que detalle el procés implantat.

No es realitzen de manera sistemàtica proves de recuperació planificades, ni s'han implantat mesures addicionals per a la protecció de les còpies, a pesar que en la revisió anterior vam identificar que aquestes no eren completament efectives.

En l'auditoria anterior vam constatar que l'emplaçament del centre de procesament de dades (CPD) no disposava de les condicions físiques adequades per a garantir la seguretat de les dades emmagatzemades i dels components del sistema d'informació allí situats, particularment davant d'incidents causats per l'aigua, ni comptava amb les mesures físiques necessàries per al control dels accessos. En aquest sentit, s'ha iniciat la contractació d'un projecte per a millorar el condicionament físic del CPD existent.

A més, ens han informat que s'han iniciat accions per a l'execució d'un projecte d'instal·lació d'un segon CPD en les dependències de l'Ajuntament, que proporcione mesures addicionals per a la protecció de les còpies. Aquest projecte no s'ha considerat per a la valoració del control, atés que únicament s'han produït activitats preparatòries per a la instal·lació del CPD secundari.



La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 54,8%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 68,5%**. No s'han produït millores respecte de la nostra auditoria anterior.

## **CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT**

### **Objectiu del control**

Assegurar el compliment de la normativa bàsica en matèria de seguretat de la informació, la qual cosa inclou l'establiment d'una adequada governança de ciberseguretat.

### **Situació del control**

#### **Compliment de l'ENS**

Des de la revisió realitzada l'any 2019, l'Ajuntament ha realitzat les accions següents que han millorat el nivell de compliment exigint pel Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica:

- Al gener de 2022 i per mitjà de resolució d'Alcaldia es va aprovar la política de seguretat de la informació, d'acord amb l'Esquema Nacional de Seguretat.
- La política de seguretat de la informació inclou la designació dels responsables per als rols previstos en la política i inclou la creació i composició del comitè de seguretat.

L'aprovació de la política de seguretat no es considera en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021, però sí que ho tenim en compte per a l'actualització de la nostra recomanació sobre aquest control.

Encara es mantenen mancances que s'han d'esmenar:

- No s'han elaborat i aprovat la declaració d'aplicabilitat i el pla d'adequació.
- No s'ha emplenat i remés anualment l'Informe de l'Estat de la Seguretat (Informe INES).
- No s'ha realitzat l'auditoria prevista en l'article 34 del Reial Decret 3/2010.
- No s'ha certificat el compliment de l'ENS.

En conseqüència, continua vigent una part de les mancances identificades i les recomanacions realitzades en l'informe precedent.



## Compliment del RGPD

Quant al compliment en matèria de protecció de dades personals, des de la revisió realitzada l'any 2019 l'Ajuntament ha realitzat accions que han millorat el nivell de compliment del que s'exigeix en l'RGPD.

S'ha contractat l'any 2022 un servei extern que assumeix les funcions del delegat de protecció de dades a l'Ajuntament. Aquest contracte es trobava en execució en el moment de la revisió.

S'han iniciat diverses tasques a fi de donar compliment a les obligacions de l'RGPD, incloent-hi l'elaboració d'un registre d'activitats de tractament, tal com s'especifica en l'article 30 de l'RGPD, o la celebració de sessions formatives per al personal de l'Ajuntament.

La contractació d'aquest servei no es considera en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021, però sí que ho tenim en compte per a l'actualització de la nostra recomanació en aquest control.

No obstant això, hi ha mancances que s'han d'esmenar:

- No s'ha finalitzat i publicat el registre d'activitats de tractament, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.
- No s'han realitzat les anàlisis de riscos sobre els tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.
- No s'han aplicat les mesures organitzatives i tècniques necessàries per a protegir les dades personals, requerides per l'article 24.1 de l'RGPD.
- No s'han executat auditories de compliment en matèria de protecció de dades.

En conseqüència, segueix vigent una part de les mancances identificades i les recomanacions realitzades en l'informe precedent.

## Compliment de la legalitat del registre de factures

S'han realitzat les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.

## Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió no es modifica respecte a l'informe emés l'any 2019, i l'Ajuntament aconsegueix un **índex de maduresa del 15,0%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 8 del 18,8%**.



Si bé s'han produït determinades millores respecte de la nostra auditoria anterior, aquestes no s'han considerat per al càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021.

### Governança de ciberseguretat

L'Ajuntament de Torrevella no té establida una adequada governança de la seguretat de la informació.

Hem observat mancances rellevants que indiquen que la governança no pot considerar-se efectiva. Aquestes mancances són les següents:

- La inexistència, a 31 de desembre de 2021, de la política de seguretat de la informació (PSI), d'un comitè de seguretat de la informació i dels rols clau de la seguretat en l'organització, particularment el responsable de seguretat.
- La inexistència d'un marc normatiu i procedimental de seguretat formalment assumit per l'organització i que s'aplique de manera homogènia a totes les seues àrees.
- La inexistència d'una cultura de la ciberseguretat i de compromís amb l'administració electrònica, la transformació digital i l'ús de mitjans tecnològics per a facilitar la gestió administrativa de l'entitat.

En 2022 s'han adoptat algunes mesures que suposen un canvi de tendència respecte al compromís de la corporació amb la seguretat de la informació i l'administració electrònica, que s'ha materialitzat en determinats aspectes positius en la gestió de la ciberseguretat:

- S'ha aprovat la política de seguretat de la informació (PSI), que inclou la creació del comitè de seguretat i el nomenament del responsable de seguretat. No obstant això, el comitè de seguretat de la informació encara no s'havia reunit fins al moment de finalització del treball de camp de l'auditoria. En una entitat de la grandària i complexitat de l'Ajuntament, hauria de reunir-se amb periodicitat mensual, ja que la seua existència no ha de ser merament formal.
- L'articulació de projectes, en el context d'utilització dels fons Next Generation EU i el Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana, que tenen com a objecte promoure la seguretat de la informació i aconseguir el compliment normatiu.
- La licitació de projectes i serveis per a solucionar algunes de les greus mancances de seguretat identificades, que s'han comentat al llarg de l'Informe.
- La implantació, a nivell tecnològic i operatiu, d'una plataforma per a la gestió electrònica d'expedients i procediments administratius de la corporació, que implica el redisseny complet dels processos gestionats per mitjà de la nova plataforma.

És urgent solucionar les mancances identificades, ja que afecten de manera negativa el nivell de seguretat de la informació, i explotar les fortaleeses existents, que facilitaran l'aplicació de mesures necessàries i recomanacions efectuades en aquest informe.





## ACRÒNIMS I GLOSSARI DE TERMES

- CBCS: Controls bàsics de ciberseguretat
- CCN: Centre Criptològic Nacional
- CGTI: Controls generals de tecnologies de la informació
- ENS: Esquema Nacional de Seguretat
- INES: Informe Nacional de l'Estat de la Seguretat
- LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal
- PSI: Política de seguretat de la informació
- RGPD: Reglament General de Protecció de Dades
- SGSI: Sistema de gestió de seguretat de la informació
- SIC: Sistemes d'informació i comunicacions

**Alta direcció:** A l'efecte d'aquest treball, ens referim als òrgans superiors de l'Ajuntament (en particular, l'alcalde o l'alcaldesa i la Junta de Govern). Són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions i una adequada governança de ciberseguretat.

**Ciberamenaces:** 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 als quals 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.

**Cibervigilància / Vigilància digital:** Vigilància Digital és un servei de detecció d'amenaques i rastreig d'informació sensible a través d'internet basada en intel·ligència artificial que



facilita a les empreses adequar la seua estratègia de negoci i millorar el procés de presa de decisions.

**Correlador d'esdeveniments:** Correlar és el procés de comparar diferents fonts d'informació d'esdeveniments, donant d'aquesta manera sentit a esdeveniments que, analitzats per separat, no en tindrien o passarien desapercebuts. Un SIEM (*security information and event management*) o sistema de gestió d'incidències i informació de seguretat, va un pas més enllà de les capacitats de monitoratge, emmagatzematge i interpretació de les dades rellevants per mitjà de tècniques de correlació complexa d'esdeveniments.

**Direcció:** Són els responsables de l'execució de les activitats establides per l'alta direcció en matèria de ciberseguretat, és la direcció executiva. En aquest grup, a l'efecte d'aquest informe, s'inclou el regidor responsable dels sistemes d'informació i les comunicacions, el secretari general, l'interventor general, els funcionaris directors del departament TIC i els caps d'àrea o servei.

**EDR:**<sup>17</sup> Un sistema EDR, sigla en anglés d'*endpoint detection and response*, és un sistema de protecció dels equips i infraestructures de l'empresa. Combina l'antivirus tradicional juntament amb eines de monitoratge i intel·ligència artificial per a oferir una resposta ràpida i eficient davant els riscos i les amenaces més complexes.

**Governança de ciberseguretat:** Segons el Tribunal de Comptes Europeu, la governança de la seguretat de la informació consisteix en la creació d'estructures i polítiques per a garantir la confidencialitat, integritat i disponibilitat de les dades. És més que una mera qüestió tècnica, per la qual cosa exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització. A l'efecte d'aquest informe li donem el mateix significat que a *governança de la seguretat de la informació*.

**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 la disposició de tots els membres de l'organització que necessiten conèixer-la, en particular 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 deriva i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desenvolupament normatiu de 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 el que 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. Ha de ser aprovada pel

---

<sup>17</sup> [Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa](#), Institut Nacional de Ciberseguretat (INCIBE).



president o presidenta o la junta de govern d'una entitat local o el consell d'administració d'una societat. Ha d'estar accessible per a tots els membres de l'organització i redactada de manera senzilla, precisa i comprensible. Convé que siga breu, i que deixe 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, amb indicació del 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.

**Sistema de gestió de seguretat de la informació:** Un SGSI és un enfocament sistemàtic per a establir, implementar, operar, monitorar, revisar, mantindre i millorar la seguretat de la informació d'una organització i aconseguir els seus objectius.

**vSOC (*virtual security operations center*):** Centre d'operacions de ciberseguretat (SOC) virtual. El projecte vSOC per a entitats locals a la Comunitat Valenciana és una eina cedida pel Centre Criptològic Nacional i gestionada pel CSIRT-CV que permet controlar la seguretat dels ajuntaments des d'un únic punt o centre d'operacions de ciberseguretat virtual.



## TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir amb el regidor delegat responsable d'Innovació i Modernització, amb la secretària de l'Ajuntament, amb el director general de Desenvolupament, Innovació, Modernització i TIC, i amb els tècnics responsables del departament TIC, perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.c del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'informe d'auditoria corresponent a 2021, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

Transcorregut aquest termini no s'han rebut al·legacions.



## **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, i de l'article 55.1.h del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 21 d'octubre de 2022, va aprovar aquest informe d'auditoria.



NIF: S9600001C

## Informe seguiment CBCS Torrevella 2019 - SEFYCU 3593929

Podeu accedir a aquest document en format PDF-PAdES i comprovar la seua autenticitat en la Seu Electrònica usant el codi CSV següent:



**URL (adreça en Internet) de la Seu Electrònica:** <https://sindicom.sedipualba.es/>

**Codi Segur de Verificació (CSV):** KUAA ZN32 NZ3N TKNX 9MUZ

En aquesta adreça podeu obtenir més informació tècnica sobre el procés de firma, així com descarregar les firmes i els segells en format XAdES corresponents.

## Resum de firmes i/o segells electrònics d'aquest document

Empremta del document per a la persona firmant

Text de la firma

Dades addicionals de la firma



Vicent Cucarella Tormo  
Síndic Major

Firma electrònica - ACCV - 02/11/22 07:19  
VICENT CUCARELLA TORMO