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 SAGUNT DE L'ANY 2019

Situació a 31 de desembre de 2021

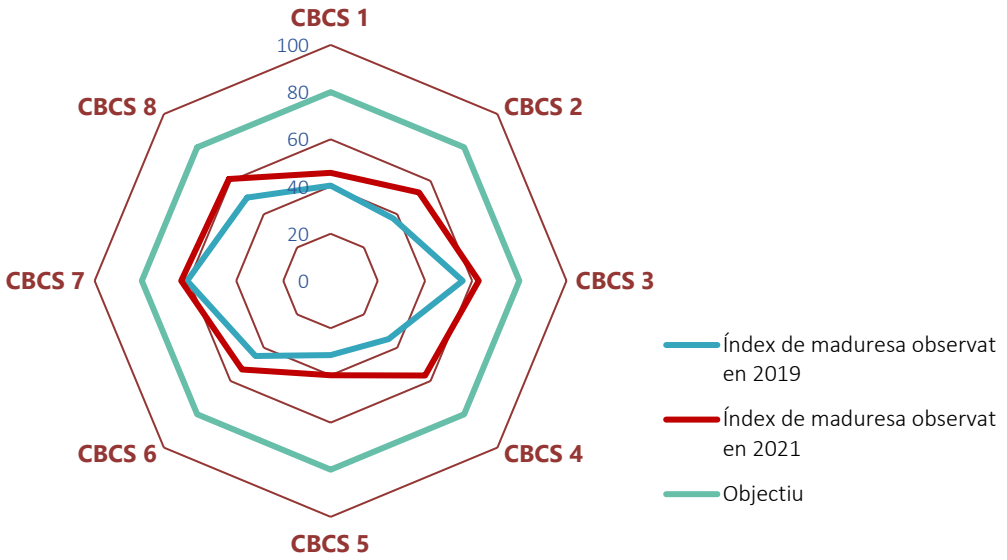
# RESUM

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.

Atesa aquesta realitat, i en sintonia amb el seu actual pla estratègic, la Sindicatura de Comptes ha fet un treball de seguiment dels controls bàsics de ciberseguretat (CBCS) de l'Ajuntament de Sagunt respecte a la situació que mostrava l'auditoria de l'any 2019.

## Conclusions

Encara que s'han fet progressos des de la nostra auditoria anterior i s'han atés parcialment algunes de les nostres recomanacions, l'índex de maduresa general dels controls bàsics de ciberseguretat, l'objectiu de la qual seria aconseguir un 80%, mostra un valor del 54,4% (44,5% en 2019), per la qual cosa el nivell d'efectivitat en els controls analitzats continua sent insuficient i ha de millorar per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en aquells controls que presenten deficiències significatives.




L'Ajuntament de Sagunt no té establida una adequada governança de la ciberseguretat, situació que ha de ser esmenada. Els òrgans de govern han d'aprovar normes i procediments en relació amb la seguretat de la informació aplicables a tota l'organització per igual.

La política de seguretat de l'Ajuntament ha de ser actualitzada i els rols definits en aquesta han d'exercir les seues funcions de manera efectiva. Cal que el comité de seguretat de la informació, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat, es reunisca regularment, a fi de conéixer l'estat de la seguretat de la informació de l'Ajuntament i prendre les decisions pertinents de manera oportuna.

Així mateix, la nostra revisió també ha posat de manifest un grau de compliment insuficient 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.

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, a més d'aprovar formalment procediments que descriguen les accions i controls implantats, recomanem la implantació de solucions per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa, actualitzar els sistemes obsolets, estendre l'ús de l'eina de gestió de vulnerabilitats, pedaços i actualitzacions a tots els equips de l'entitat i aplicar als administradors de sistemes el criteri de mínima funcionalitat.

**NOTA**

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

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

## Situació a 31 de desembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

## ÍNDEX (amb hipervincles)

# 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, les 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 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 5 de març de 2020 el Consell de la Sindicatura de Comptes va aprovar l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Sagunt, Exercici 2019. Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 fer 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

Addicionalment, 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 adquireixen tot el seu sentit conceptes com la ciberresiliència i la ciberhigiene. Per ciberresiliència es pot entendre la capacitat d'una entitat per a evitar o resistir un ciberatac i recuperar-se'n en un temps

raonable per a continuar prestant els seus serveis. La ciberhigiene és un principi fonamental[1] 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.

L'experiència patida per l'Ajuntament en 2021, que s'esmenta en l'apartat següent, és un clar exponent de la necessitat de reforçar els controls de seguretat en totes les institucions públiques i aconseguir el nivell de maduresa exigit per l'ENS.

## 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 realitzat 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 Sagunt. Exercici 2019.

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats, proporcionant una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la

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

informació i, si és el cas, formular recomanacions que contribuïsquen a esmenar les deficiències observades i a millorar els procediments de control.

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.

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 sustenten les conclusions i les recomanacions d'aquest informe.

# 4. CONCLUSIONS

## Encara que s'han realitzat progressos des de la nostra auditoria anterior i s'han atés parcialment les nostres recomanacions, l'índex de maduresa general dels controls bàsics de ciberseguretat és insuficient i ha de millorar per a aconseguir els nivells exigits per l'ENS

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que l'**índex de maduresa general** en la gestió dels controls bàsics de ciberseguretat aconsegueix un **54,4%**, 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.

Encara que l'Ajuntament ha atés de manera parcial les nostres recomanacions i l'índex de maduresa general ha millorat des del 44,5% de la nostra auditoria de 2019, l'índex de

maduresa actual continua sent insuficient per a garantir un adequat grau de seguretat i aconseguir el 80% requerit per l'ENS. La comparació dels resultats detallats amb els obtinguts l'any 2019 mostra una millora en tots els controls, si bé la millora ha sigut insuficient i cap aconsegueix l'objectiu del 80%, atés el baix grau d'atenció a algunes de les nostres recomanacions (vegeu apartat 5 següent).

Hi ha clares possibilitats de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació, particularment sobre aquells controls que presenten deficiències significatives i no arriben al nivell de maduresa N2 (CBCS 1 i CBCS 5). 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.

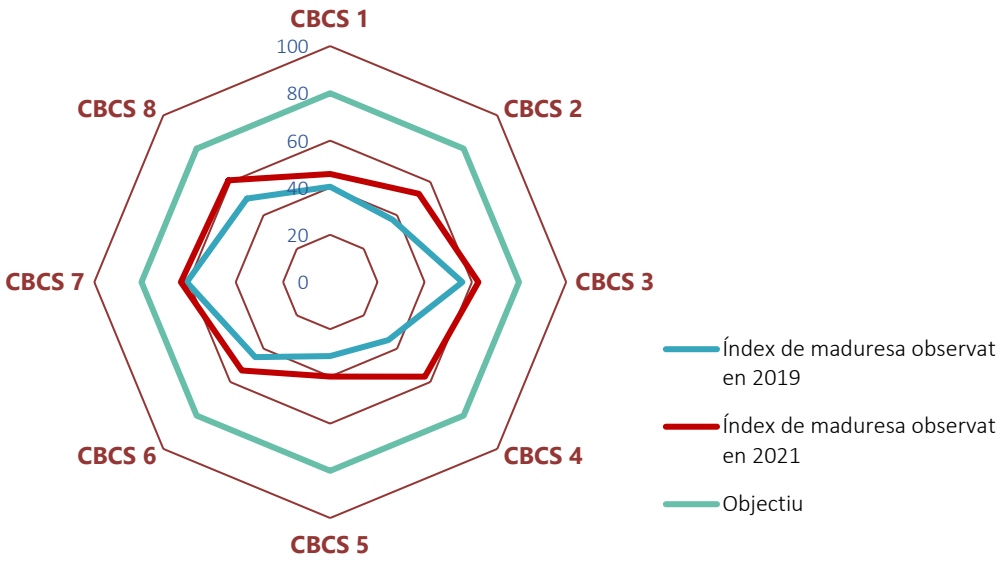
**Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat**

| Control | 2019 | | | 2021 | | |
|---|---|---|---|---|---|---|
| | Índex de maduresa | Nivell de maduresa | Índex de compli-ment | Índex de maduresa | Nivell de maduresa | Índex de compli-ment |
| **CBCS 1** Inventari i control de dispositius físics | *40,4%* | ***N1*** | *50,4%* | 45,8% | **N1** | 57,2% |
| **CBCS 2** Inventari i control de programari autoritzat i no autoritzat | *37,4%* | ***N1*** | *46,8%* | 53,0% | N2 | 66,3% |
| **CBCS 3** Procés continu d'identificació i solució de vulnerabilitats | *56,0%* | *N2* | *70,0%* | 62,8% | N2 | 78,5% |
| **CBCS 4** Ús controlat de privilegis administratius | *34,8%* | ***N1*** | *43,5%* | 56,7% | N2 | 70,9% |
| **CBCS 5** Configuracions segures del programari i maquinari | *31,4%* | ***N1*** | *39,2%* | 40,0% | **N1** | 50,0% |
| **CBCS 6** Registre de l'activitat dels usuaris | *45,0%* | ***N1*** | *56,3%* | 53,0% | N2 | 66,3% |
| **CBCS 7** Còpies de seguretat de dades i sistemes | *60,8%* | *N2* | *76,0%* | 63,3% | N2 | 79,2% |
| **CBCS 8** Compliment normatiu i governança de ciberseguretat | *50,0%* | *N2* | *62,5%* | 61,0% | N2 | 76,3% |
| General | 44,5% | ***N1*** | 55,6% | 54,4% | N2 | 68,1% |

L'índex de compliment dels CBCS és del 68,1%, 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%. Aquest índex ha millorat des del 55,6% del nostre informe anterior i la comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una lleugera millora en tots els controls.

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

**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 Sagunt no té establida una governança adequada de la ciberseguretat, situació que ha de ser esmenada. 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 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[2] (tal com es defineix 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.

Si bé hem pogut verificar l'existència d'un cert nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament i particularment dels responsables de les àrees implicades, hi ha mancances rellevants que impedeixen que la governança es puga considerar efectiva:

[2] *Prontuario de ciberseguridad para entidades locales*, Centre Criptològic Nacional i Federació Espanyola de Municipis i Províncies, abril 2021.

- La falta d'activitat del Comité de Seguretat, òrgan imprescindible per a coordinar la seguretat de la informació entre les diferents àrees de l'Ajuntament i dels rols clau, particularment el responsable de seguretat, les responsabilitats del qual es troben detallades i assignades en la política de seguretat, però no s'exerceixen de manera efectiva.

- La falta de recursos suficients, tant econòmics com de personal, en el departament TIC per a atendre la problemàtica de la seguretat de la informació.

És necessari, per tant, solucionar de manera urgent les mancances identificades, que tenen un impacte negatiu en el nivell de seguretat de la informació de l'Ajuntament, i atendre les recomanacions efectuades en aquest informe.

### El grau de compliment de la normativa relativa a la seguretat de la informació és insuficient

La revisió del compliment de legalitat en matèria relacionada amb la seguretat de la informació ha posat de manifest un insuficient nivell de compliment de la normativa. Hi ha incompliments significatius, que són assenyalats en l'apartat 5, sobre els quals s'ha d'actuar per a esmenar-los ràpidament.

## 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 les millores realitzades des de llavors. 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 s'han d'adoptar.

### 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 reculla el procés complet actualment implantat, incloent-hi les revisions periòdiques de maquinari, actualització de l'inventari i incloent-hi la periodicitat d'aquestes revisions.

2. Millorar els controls que permeten 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 que incloga les accions actualment implantades.

4. Revisar i actualitzar els sistemes que encara es troben fora del període de suport, especialment els lligats a processos crítics de l'entitat.

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

5. Aprovar formalment un procediment que descriga les accions dutes a terme per a la gestió de vulnerabilitats, des de la identificació fins a la solució, i que considere, a més de les accions ja establides, l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes, la priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.

6. Fer extensiu a tota l'organització l'ús de l'eina implantada per a la gestió unificada i automatitzada de pedaços de seguretat i actualitzacions.

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

7. Aprovar un procediment que incloga la gestió d'usuaris amb privilegis d'administració que aplique les mateixes directrius per a tots els sistemes de l'entitat i que establisca, a més de les pràctiques que ja es duen a terme en aquest control, la utilització, per cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de privilegis depenent de les tasques a realitzar.

## 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, 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 CCN.

   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 comprendre la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà de procediment manual o per mitjà 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, les còpies de seguretat, la 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. Actualitzar i aprovar formalment el procediment de còpies de seguretat, que descriga el conjunt de mesures implantades i detalle les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves planificades de restauració i els requisits de protecció de les còpies.

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

11. 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:

    - Emplenar la Instrucció Tècnica de Seguretat de l'Informe de l'Estat de la Seguretat, de la Secretaria d'Estat d'Administracions Públiques (Informe INES).
    - Realitzar les auditories de compliment 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.

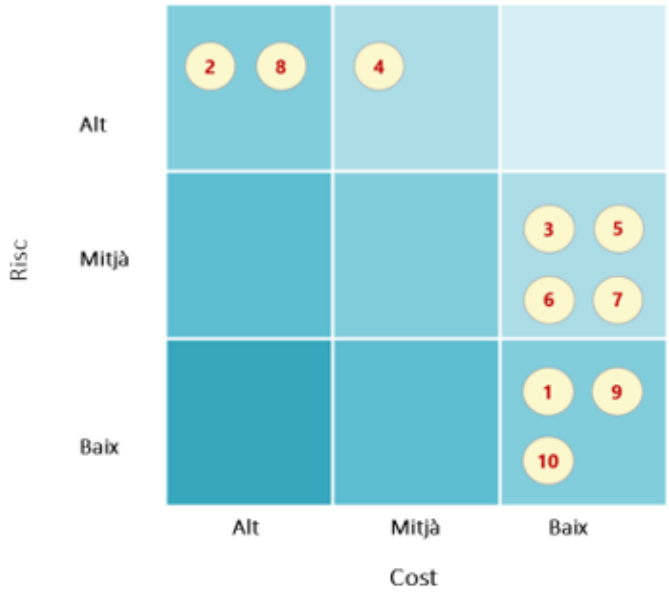
12. En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de:

    - 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 puguen 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 que cal mitigar** i **cost estimat de la implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2019, adaptant la relació risc/cost de cada recomanació i considerant les millores realitzades des de la revisió anterior. No s'hi inclouen els punts 11 i 12 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, una ha sigut atesa, huit ho han sigut parcialment i quatre no s'han atés.

## 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 |
|---|---|---|---|---|
| **1** | Aprovar formalment un procediment per a la gestió de l'inventari i el control d'actius físics que reculla el procés complet actualment implantat, incloent-hi les revisions periòdiques de maquinari, actualitzant degudament l'inventari i incloent-hi la periodicitat d'aquestes revisions. | L'Ajuntament no ha aprovat un procediment a aquest efecte. Encara que s'han realitzat algunes accions relacionades amb aquest control, com l'actualització del programari que gestiona l'inventari de dispositius físics i la incorporació d'alguns edificis a la xarxa corporativa, aquestes accions no atenen l'essencial de la nostra recomanació. | **No aplicada** | Es manté la redacció de 2019. |
| **2** | Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa. | El departament d'informàtica ha treballat en la desconnexió de preses de xarxa de les zones públiques o comunes; no obstant això, no hi ha un mecanisme robust de control en aquest aspecte. També s'ha implantat una solució per a la fortificació dels equips d'usuari atenent criteris de seguretat dels *endpoints*.<br><br>Les mesures implantades per a aquest control no s'han formalitzat en un procediment aprovat. | **Aplicada parcialment** | S'actualitza la redacció de 2019. |
| **3** | Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que tinga en compte:<br>- L'elaboració de llistes de programari autoritzat (llistes blanques) i la realització de revisions periòdiques de programari.<br>- La implantació de les mesures tècniques que impedisquen la instal·lació i execució del programari no autoritzat.<br>- 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. | L'Ajuntament ha implantat determinades mesures per a esmenar les deficiències detectades, com l'eliminació dels usuaris administradors dels equips client o el bloqueig d'aplicacions en el perímetre de la xarxa.<br><br>No obstant això, les mesures implantades no han sigut recollides en un procediment aprovat formalment. | **Aplicada parcialment** | S'actualitza la redacció de 2019. |
| **4** | Revisar i actualitzar tots els sistemes que es troben fora del període de suport. | Encara que s'han actualitzat gran part dels sistemes que es trobaven fora del període de suport, continuen existint sistemes crítics obsolets. Això suposa una deficiència greu que afecta tot el sistema d'informació. | **Aplicada parcialment** | S'actualitza la redacció de 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 |
|---|---|---|---|---|
| **5** | Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:<br>- La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i les accions actualment establides de seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat.<br>- La priorització actualment implantada basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades. | L'Ajuntament ha desplegat el sistema microCLAUDIA per a la provisió de vacunes davant de codi nociu de tipus *ransomware*, i l'eina CARMEN, que monitora els fluxos de dades per a la identificació d'amenaces persistents avançades.<br>El departament TIC ha desplegat un sistema EDR que identifica vulnerabilitats en els equips amb agent de xarxa instal·lat, encara que en el moment de la revisió únicament es disposa de 100 llicències de prova.<br>S'ha implantat una eina de cibervigilància que proporciona múltiples serveis, entre els quals es troba la gestió de vulnerabilitats i pedaços o el monitoratge de filtracions de dades. | **Aplicada parcialment** | S'actualitza la redacció feta en 2019. |
| **6** | Utilitzar eines que permeten la gestió unificada i automatitzada de pedaços de seguretat i altres actualitzacions. | Encara que s'ha implantat un sistema EDR que realitza la gestió de pedaços i actualitzacions, en el moment de la revisió únicament disposava de 100 llicències de prova. | **Aplicada parcialment** | S'actualitza la redacció de 2019. |
| **7** | Aprovar 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:<br>- 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 han de realitzar-se amb usuaris nominatius.<br>- Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.<br>- 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).<br>- La política d'autenticació a aplicar a aquest tipus de comptes. | El departament ha eliminat els permisos d'administració per als usuaris que no requereixen aquests privilegis, han solucionat la incidència detectada en l'aplicació de gestió tributària i enfortit la política de contrasenyes.<br>No obstant això, hi ha possibilitats de millora per a aconseguir el nivell exigit per l'ENS, com ara la utilització de diferents nivells de privilegis per part dels administradors, que les accions dutes a terme s'estenguen a tots els sistemes o l'aprovació d'una política de gestió d'usuaris administradors que detalle aquestes accions. | **Aplicada parcialment** | S'actualitza la redacció de 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 |
|---|---|---|---|---|
| **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 i que s'aplique a la totalitat dels sistemes de l'Ajuntament. 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 CCN (com ja s'està fent per a un subconjunt dels actius de l'entitat).<br><br>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 d'incloure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, per mitjà d'un procediment manual o d'eines automatitzades de monitoratge de la configuració. | Encara que s'han realitzat accions relacionades amb la configuració segura de sistemes –com el control d'accés d'equips en el tallafoc o l'exigència de les certificacions de l'ENS en les solucionés i empreses contractades–, l'Ajuntament no disposa d'un procediment aprovat per la corporació que descriga la gestió de configuracions i canvis en els sistemes crítics de l'entitat. | **Aplicada parcialment** | Es manté la redacció. |
| **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, la 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. | El servei de directori d'usuaris en el núvol compta amb un sistema de registre d'accions dels usuaris.<br><br>L'Ajuntament ha implantat eines oferides pel CSIRT-CV i CCN-CERT que alerten de les anomalies detectades en la xarxa corporativa. A més, està en fase d'integració amb el vSOC del CSIRT-CV.<br><br>No obstant això, no es disposa d'un procediment que descriga el tractament de *logs* d'auditoria que incloga els aspectes necessaris. | **No aplicada** | Es manté la redacció. |
| **10** | Actualitzar i aprovar formalment el procediment existent per a la gestió de les còpies de seguretat de dades i sistemes, que definisca, com a mínim, les dades i els sistemes afectats, la periodicitat de les còpies, les ubicacions, els responsables, les proves de restauració i els requisits de protecció de les còpies. | El departament ha millorat el sistema de còpies per mitjà de l'adquisició d'un nou maquinari i la contractació de serveis en el núvol.<br><br>No obstant això, no es realitzen proves de restauració planificades dels sistemes crítics ni el procediment està aprovat per la direcció. | **Aplicada parcialment** | S'actualitza la redacció de 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 |
|---|---|---|---|---|
| **11** | 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:<br>- Emplenar la Instrucció Tècnica de Seguretat de l'Informe de l'Estat de la Seguretat, de la Secretaria d'Estat d'Administracions Públiques (Informe INES).<br>- Realitzar les auditories de compliment previstes en l'article 34 del Reial Decret 3/2010.<br>- 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. | Sense variació en 2021. | **No aplicada** | Es manté la redacció. |
| **12** | En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix per l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de:<br>- Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.<br>- Planificar i executar auditories de compliment en matèria de protecció de dades. | Sense variació en 2021. | **No aplicada** | Es manté la redacció. |
| **13** | Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre. | S'ha realitzat l'auditoria del registre de factures de l'exercici 2021. | **Aplicada** | S'elimina la recomanació de 2019. |

## Actuacions en curs

Encara que no s'han tingut en compte en el càlcul dels indicadors que es mostren 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. 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 planificades o en execució i que per la seua rellevància han de ser destacades:

- L'eina EDR utilitzada per a la gestió de pedaços i actualitzacions està en fase de licitació. Durant el treball de revisió únicament es disposava de 100 llicències de prova. Aquesta eina millorarà diversos dels controls de seguretat analitzats.

- L'Ajuntament està en fase de licitació d'un projecte per a l'adequació i compliment del nou ENS, projecte subvencionat amb els fons Next Generation EU, en el qual s'inclourà l'elaboració i aprovació de procediments de control sobre els diferents sistemes d'informació.

- Desplegament de serveis i eines proporcionats pel CSIRT-CV, com a part del Pla de Xoc de Ciberseguretat per a les entitats locals de la Comunitat Valenciana. Té previst el desplegament de:

    - CARMEN, solució desenvolupada amb l'objectiu d'identificar el compromís de la xarxa d'una organització per part d'amenaces persistents avançades (APT).

    - LUCIA (Llista Unificada de Coordinació d'Incidents i Amenaces), eina per a la gestió de ciberincidents.

    - SAT-INET (Sistema d'Alerta Primerenca d'Internet), servei desenvolupat i implantat per l'Equip de Resposta davant Incidents de Seguretat de la Informació del Centre Criptològic Nacional (CCN-CERT) per a la detecció en temps real de les amenaces i incidents.

# APÈNDIX 1
# Metodologia aplicada

## Introducció

Cada vegada un major nombre d'aspectes de la gestió pública es realitza 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 tot tipus provinents del ciberespai, majors riscos de ciberseguretat i s'han multiplicat els incidents de seguretat de què 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-ne l'impacte, i també respondre i recuperar-se d'incidents.

Encara 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[3] 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 implementades correctament.

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.

## 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

[3] Informe Nacional de l'Estat de Seguretat dels Sistemes de les TIC del CCN.

i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Sagunt. Exercici 2019, i obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això n'hem avaluat tant el disseny[4] com l'eficàcia operativa[5] per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport. També hem revisat el compliment de la normativa bàsica relativa a la seguretat de la informació.

Així mateix, hem formulat recomanacions que contribuïsquen a esmenar les deficiències observades i a millorar els 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 aplicacions que suporten els processos de gestió comptable i pressupostària i la gestió tributària i recaptadora, així com els controls que tenen implantats.

[4] 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.

[5] L'auditor comprova que el control existeix i que l'entitat l'està utilitzant.

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

- 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 siguen esmenades i són considerades d'aquesta manera en les conclusions i en els indicadors.

Addicionalment, 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'obtindre 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 es pot consultar en el nostre web. Per a major 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 establit per la prestigiosa organització Center for Internet Security (CIS),[6] que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. L'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 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 establits 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 els requereix l'ENS. D'aquesta manera, els huit controls bàsics de ciberseguretat presenten una correspondència (no exacta) amb les referències següents de l'ENS:

[6] Center for Internet Security, <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

L'European Union Agency for Cybersecurity (ENISA) assenyala[7] 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.[8]

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.[9]

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 prioritaris recomanats per ENISA com a bones pràctiques de ciberhigiene.

[7] *Review of Cyber Hygiene Practices*, ENISA, desembre de 2016. Vegeu la pàgina 14.

[8] 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 de ciberhigiene adequades.

[9] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices*, 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 ciberhigiene adequada.

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.

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

Utilitzem els controls bàsics de ciberseguretat com a criteris d'auditoria o criteris 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 què 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 | |
|---|---|---|---|
| **CBCS 1** Inventari i control de dispositius físics | Gestionar activament tots els 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. |
| **CBCS 2** Inventari i control de programari autoritzat | Gestionar activament tot el programari en els sistemes, de manera que només es puga instal·lar i executar programari autoritzat. | CBCS 2-1: Inventari de 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. |
| **CBCS 3** Procés continu d'identificació i solució de vulnerabilitats | Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants. | CBCS 3-1: Identificació de vulnerabilitats | Existeix un procés per a identificar les vulnerabilitats dels components del sistema que assegura que aquestes són identificades en temps oportú. |
| | | CBCS 3-2: Priorització | Les vulnerabilitats identificades són analitzades i prioritzades per a la resolució atenent el risc que suposen per a la seguretat del sistema. |
| | | CBCS 3-3: Resolució de vulnerabilitats | Es realitza un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que es resolen en el temps previst en el procediment. |
| | | CBCS 3-4: Pedaços | L'entitat disposa de procediments i eines que permeten aplicar els pedaços de seguretat publicats pels fabricants en un temps raonable. |
| **CBCS 4** Ús controlat de privilegis administratius | Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'ús i configuració de privilegis administratius en ordinadors, xarxes i aplicacions. | CBCS 4-1: Inventari i control de comptes d'administració | Els privilegis d'administració estan limitats adequadament i l'entitat disposa d'un inventari de comptes d'administració que facilita el correcte control. |
| | | CBCS 4-2: Canvi de contrasenyes per defecte | Les contrasenyes per defecte dels comptes que no s'utilitzen o són estàndard es canvien abans de l'entrada en producció del sistema. |
| | | CBCS 4-3: Ús dedicat de comptes d'administració | Els comptes d'administració només es realitzen per a les tasques que són estrictament necessàries. |
| | | CBCS 4-4: Mecanismes d'autenticació | Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes. |
| | | CBCS 4-5: Auditoria i control | L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades. |

| Control | Objectiu del control | Subcontrol | |
|---|---|---|---|
| **CBCS 5** Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors | Establir, implantar i gestionar la configuració de seguretat, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de previndre atacs a través 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. |
| **CBCS 6** Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria) | Recollir, gestionar i analitzar *logs* d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac. | CBCS 6-1: Activació de *logs* d'auditoria | El *log* d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs. |
| | | CBCS 6-2: Emmagatzematge de *logs*: retenció i protecció | Els *logs* es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats. |
| | | CBCS 6-3: Centralització i revisió de *logs* | Els *logs* de tots els sistemes són revisats periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels *logs* d'auditoria, de manera que se'n facilite la revisió. |
| | | CBCS 6-4: Monitoratge i correlació | L'entitat disposa d'un SIEM (*security information and event management*) o una eina d'analítica de *logs* per a realitzar correlació i anàlisi de *logs*. |
| **CBCS 7** Còpia de seguretat de dades i sistemes | Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú. | CBCS 7-1: Realització de còpies de seguretat | L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema. |
| | | CBCS 7-2: Realització de proves de recuperació | Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica, i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament. |
| | | CBCS 7-3: Protecció de les còpies de seguretat | Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmeses a través de la xarxa. |
| **CBCS 8** Compliment 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 que mostra el quadre següent:

**Quadre 6. Avaluació dels subcontrols**

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

### 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 |
|---|---|---|
| **N0 Inexistent** | 0 | El control no s'està aplicant en aquest moment. |
| **N1 Inicial / ad hoc** | 10 | El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat.<br>*L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.* |
| **N2 Repetible, però intuïtiu** | 50 | Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives.<br>*L'eficàcia del procés depén 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 impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.* |
| **N3 Procés definit** | 80 | Els processos estan estandarditzats, documentats i comunicats amb accions formatives.<br>*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).*<br>*L'èxit és més que bona sort: es mereix.*<br>*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.* |
| **N4 Gestionat i mesurable** | 90 | La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix.<br>*Es disposa d'un sistema de mesures i mètriques per a conéixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.*<br>*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.* |
| **N5 Optimitzat** | 100 | Se segueixen bones pràctiques en un cicle de millora contínua.<br>*El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.*<br>*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.*<br>*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.* |

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 aconsegueix el nivell ALT.

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

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

La categoria d'un sistema d'informació, en matèria de seguretat, modula l'equilibri entre la importància de la informació que maneja, dels serveis que presta i l'esforç de seguretat requerit, en funció dels riscos 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:[10]

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

Els sistemes auditats en aquest informe 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 aconsegueixen el nivell mínim d'exigència requerit en l'ENS, que en aquest cas és *N3, procés definit,* i un índex de maduresa del 80%.**

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

## Indicadors globals

A l'efecte de l'ENS, la guia CCN-STIC-824 planteja una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics. Aquests indicadors han sigut adaptats per a aplicar-los 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 aconseguit per un organisme respecte del conjunt de controls de ciberseguretat.

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

## 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'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una forma responsable.[11]

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**.[12]

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.

[11] Vegeu el glossari de la Information Systems Audit and Control Association (ISACA).

[12] Vegeu l'apartat 66 d'*Análisis 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.[13] L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació,[14] 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, així com, 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,[15] 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 capacitació.

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

- 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.

[13] *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.

[14] *UNE-EN ISO/IEC 27001 Tecnologia de la informació. Tècniques de seguretat. Sistemes de gestió de la seguretat de la informació*, apartat 3.4.

[15] *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 Sagunt. 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**

| | |
|---|---|
| **Totalment o substancialment aplicada** | 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 complit raonablement. A més, s'ha obtingut evidència suficient que acredita les mesures adoptades. |
| **Aplicada parcialment** | 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 complit raonablement. |
| **No aplicada** | 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. |
| Sense validesa en el marc actual | 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. |
| No verificada | 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 que conté 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 de l'auditoria.

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 puguen 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 tinguen accés a la xarxa.

## Situació del control

L'Ajuntament no disposa d'un procediment formalment aprovat per al manteniment i la gestió de l'inventari de dispositius físics.

L'eina per a la gestió de l'inventari del maquinari s'ha actualitzat i permet noves funcionalitats sobre els dispositius amb agent de xarxa instal·lat, com ara la gestió de llicències, a més de ser l'eina de *ticketing* del departament TIC.

Una de les millores més significatives ha sigut la implantació d'un programari d'EDR per a la gestió centralitzada de llocs de treball que permet, entre altres coses, control d'aplicacions, actualitzacions i pedaços, etc. No obstant això, durant la nostra revisió, l'Ajuntament únicament disposava de 100 llicències de prova, encara que es tenia prevista l'ampliació d'aquestes llicències i la incorporació d'un sistema (MDM) per a la gestió de dispositius mòbils.

Respecte al control d'accés de dispositius físics a la xarxa corporativa, el departament d'informàtica ha realitzat determinades accions encaminades a millorar, encara que de manera limitada, la situació assenyalada en la nostra auditoria anterior:

- Revisió de totes les preses de xarxa en zones comunes o d'accés públic, deshabilitant les preses sense ús o innecessàries.

- Implantació de mesures que impedeixen l'accés de dispositius a la xarxa basades en els requisits de seguretat dels *endpoint*, encara que únicament afecta equips que es connecten a la xarxa des de l'exterior.

- Integració a la xarxa corporativa de diferents edificis, la qual cosa permet ampliar les dependències sobre les quals s'apliquen controls.

Encara que l'Ajuntament ha realitzat determinades accions per a corregir les deficiències detectades en la nostra auditoria anterior, no s'han aplicat mesures efectives que garantisquen un control robust sobre el dispositiu de maquinari, com ara la implantació d'un servidor de validació per a l'accés de dispositius a la xarxa o controls per a un altre tipus de dispositius (mòbils, dispositius extraïbles, etc.).

Existeix un insuficient nivell de control sobre l'inventari i el control d'actius físics, i la seua valoració global aconsegueix un **índex de maduresa del 45,8%**, que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o

la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 1 del 57,2%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 40,4%, per tant, s'ha produït una lleu millora de 5,4 punts en l'índex de maduresa del control.

## CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

### Objectiu del control

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

### Situació del control

L'Ajuntament manté correctament actualitzat l'inventari programari a través de la mateixa eina utilitzada per a l'inventari d'actiu de maquinari. Aquesta eina EDR detecta i realitza un inventari automàtic del programari dels dispositius amb agent de xarxa i permet la gestió centralitzada de pedaços i actualitzacions. No obstant això, aquesta nova eina únicament es troba desplegada en 100 equips de prova, encara que han licitat més llicències a fi d'ampliar-ne l'ús a tota l'organització.

Durant el nostre treball d'auditoria realitzat en 2019 es va observar un determinat nombre d'equips amb programari fora del període de suport del fabricant, cosa que suposava un greu risc per a tot el sistema d'informació. Durant aquest treball hem observat que el departament TIC ha realitzat un esforç per a esmenar aquesta deficiència actualitzant i homogeneïtzant el parc d'equips d'usuari. També s'ha revisat el microprogramari de l'electrònica de xarxa i del tallafoc, i s'ha verificat que està correctament actualitzat. No obstant això, continua havent-hi sistemes obsolets (sense suport del fabricant, actualitzacions o pedaços) que alberguen alguns dels processos crítics de l'entitat, tal com es descriu en el control següent.

L'Ajuntament no disposa d'un pla de manteniment per a la gestió integral de programari. Les necessitats per a l'actualització de llicències, contractacions i l'adquisició de solucions es van cobrint per mitjà d'informes de necessitat emesos pel departament TIC que són aprovats per la direcció.

El Departament TIC ha elaborat una llista blanca d'aplicacions autoritzades, però aquesta llista no s'ha aprovat formalment.

L'organització no té establit un sistema de bloqueig d'aplicacions no permeses; no obstant això, el control s'ha millorat des del nostre treball d'auditoria anterior. S'han aplicat mesures compensatòries que proporcionen una certa efectivitat al control, com ara l'eliminació de privilegis d'administració dels usuaris sobre les seues màquines i l'aplicació de regles de tallafoc per a impedir les connexions de les aplicacions fora de la xarxa.

Encara que l'Ajuntament ha realitzat accions encaminades a la millora del control sobre el programari, aquestes no estan establides en un procediment aprovat formalment.

El nivell de control sobre l'inventari i control de programari autoritzat aconsegueix un **índex de maduresa del 53,0%**, 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 2 del 66,3%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 37,4%, per tant, s'ha produït una millora de 15,6 punts en aquest índex.

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

### Objectiu del control

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

### Situació del control

Hem verificat que, encara que l'Ajuntament no ha aprovat un procediment que descriga les accions dutes a terme per a la gestió de vulnerabilitats, sí que s'han realitzat diverses accions per a millorar aquesta gestió.

Una de les millores en aquest control ha sigut la implantació d'una aplicació EDR, que permet la identificació de vulnerabilitats, a més de la gestió centralitzada d'actualitzacions i pedaços en els sistemes amb agent de xarxa instal·lat. No obstant això, com ja hem assenyalat, únicament disposen de 100 llicències de prova en la data del treball de revisió. El departament ha licitat un contracte per a estendre les llicències a tots els equips de l'organització.

Les actualitzacions i pedaços de l'electrònica de xarxa o el tallafoc s'apliquen de manera manual i hem comprovat que es realitza de manera periòdica. A més, una de les bones pràctiques dutes a terme pel departament d'informàtica és la creació de *tickets* amb alertes periòdiques en l'eina de *ticketing* per a la revisió i actualització del microprogramari de l'electrònica de xarxa.

El departament ha dut a terme el desplegament de la solució del CCN-CERT microCLAUDIA en tots els equips de la xarxa. També han desplegat la solució CARMEN, oferida pel CCN-CERT i gestionada pel CSIRT-CV, que alerta per mitjà d'informes periòdics d'anomalies en la xarxa. Els tècnics del departament d'informàtica apliquen mesures concordes amb els resultats d'aquests informes.

Finalment, l'Ajuntament ha implantat una eina de vigilància digital que rastreja la xarxa a la recerca de filtracions de dades de l'organització. El departament TIC monitora i realitza les notificacions o correccions pertinents dels incidents de seguretat detectats.

Encara que el control ha millorat, continua havent-hi possibilitats de millora que li garantirien major efectivitat, com l'ús d'eines d'escaneig de vulnerabilitats, auditories de *hacking* ètic, l'actualització de sistemes sense suport o la documentació de totes les accions dutes a terme des de la identificació fins a la resolució de vulnerabilitats crítiques en un procediment aprovat per la corporació.

A més, la deficiència més significativa ha sigut l'existència, tal com s'ha descrit en el control de programari, de determinats sistemes lligats a processos crítics de l'Ajuntament que estan fora del seu període de suport amb el fabricant (programari de virtualització, aplicació de gestió de la informació economicofinancera, sistemes del CPD), fet que ha sigut notificat pel departament TIC a la direcció, però no ha sigut esmenat. No tindre suport del fabricant implica no rebre actualitzacions funcionals, ni pedaços de seguretat sobre les vulnerabilitats detectades, la qual cosa suposa un risc greu que posa en perill tot el sistema d'informació.

Hi ha cert nivell de control sobre la gestió de vulnerabilitats, i la valoració global del control és d'un **índex de maduresa del 62,8%**, 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 3 del 78,5%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 56,0%, per tant, s'ha produït una millora de 6,8 punts en aquest indicador.

## 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 té aprovat un procediment que descriga la gestió d'usuaris amb privilegis d'administració sobre els diferents sistemes i aplicacions. No obstant això, han dut a terme determinades accions per a corregir les deficiències detectades en aquest control.

Una de les deficiències greus detectada durant la nostra auditoria anterior va ser l'assignació a tots els usuaris de privilegis d'administració sobre els seus equips. Hem verificat que s'han deshabilitat aquests permisos a tots els usuaris que no els necessiten. A més, s'han creat comptes d'administració sobre els equips d'usuari que únicament són utilitzats pel personal del departament TIC per a tasques de manteniment.

Una altra de les incidències greus reportades va ser l'existència d'usuaris amb perfils d'administració en l'aplicació de gestió tributària. Hem pogut verificar que la situació va ser notificada a l'empresa contractada i esmenada.

A més de les correccions anteriors, el departament ha realitzat una revisió dels usuaris amb privilegis d'administració sobre el domini, eliminant els usuaris genèrics i creant usuaris nominatius que identifiquen de manera inequívoca el personal que està fent tasques d'administració. No obstant això, els membres del departament no disposen d'usuaris amb diferents nivells de privilegis en funció del tipus de tasca a realitzar.

Encara que la política d'autenticació o de contrasenyes no està formalment aprovada, s'han enfortit els mecanismes d'autenticació augmentant-ne la complexitat. A més, l'Ajuntament ha forçat a canviar les contrasenyes a tots els usuaris en determinades ocasions en què s'han detectat possibles vulneracions de seguretat a l'Ajuntament.

El departament TIC manté un inventari de les aplicacions que requereixen usuaris amb privilegis d'administració, però afirma que són els responsables dels departaments els qui gestionen els usuaris i permisos.

Hi ha un cert nivell de control sobre els comptes amb privilegis administratius. La valoració global del control presenta un **índex de maduresa del 56,7%**, 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 4 del 70,9%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 34,8%, per tant, s'ha produït una millora de 21,9 punts en l'índex de maduresa del control.

## 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

Hem analitzat les accions realitzades a l'Ajuntament per al control de configuracions segures dels diferents dispositius i aplicacions i hem verificat que, encara que hi ha certes accions en aquest control, les millores són limitades i no existeix un procediment formalment aprovat que descriga els passos que cal seguir per a aplicar configuracions segures als sistemes de l'entitat.

Una de les millores dutes a terme és l'ús de l'opció GlobalProtect del tallafoc que impedeix la connexió dels equips que no s'han configurat d'acord amb uns criteris de seguretat

definits pel departament TIC. Aquesta opció s'ha millorat durant el període de teletreball ocasionat per la pandèmia.

A més, hem verificat que el departament d'informàtica incorpora en les seues licitacions l'obligatorietat, per a les empreses o solucions que es contracten, d'incorporar les corresponents certificacions de seguretat de l'ENS. Per a la contractació d'aplicacions s'exigeixen configuracions basades en les guies de seguretat de les TIC del CCN-CERT.

Encara que algunes de les accions descrites estan relacionades amb la configuració segura de sistemes i aplicacions, el control és únicament efectiu de manera parcial, atés que no es disposa d'un sistema per al monitoratge de canvis no autoritzats en les configuracions o repositoris per a gestió de versions de les configuracions dels sistemes crítics.

La valoració global del control existent sobre les configuracions segures és que l'organització aconsegueix un insuficient **índex de maduresa del 40,0%**, que es correspon amb un **nivell de maduresa *N1, inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 50,0%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 31,4%, per tant, s'ha produït una millora de 8,6 punts en l'índex de maduresa del control.

## 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

L'Ajuntament no ha aprovat un procediment que descriga el tractament dels *logs* d'auditoria que incloga aspectes com els sistemes afectats, la informació que es reté, el període de retenció, les còpies de seguretat, la gestió de drets d'accés als registres o les revisions i responsables d'aquests registres.

L'Ajuntament té el servei de directori d'usuaris desplegat en el núvol, solució que incorpora un complet sistema de registres d'auditoria.

Les eines vistes en controls anteriors (vigilància digital, gestor d'actualitzacions, inventari) i les eines desplegades del CSIRT-CV i CCN-CERT inclouen aspectes relacionats amb aquest control, atés que incorporen registres que, encara que no són registres d'auditoria sinó esdeveniments en temps real, són analitzats i revisats per tercers. A més, l'Ajuntament es troba en fase d'integració amb el vSOC del CSIRT-CV.

L'Ajuntament no disposa d'un recol·lector d'esdeveniments que permeta la revisió centralitzada i incloga els sistemes més crítics de l'entitat.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 53,0%**, 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 6 del 66,3%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 45,0%, per tant, s'ha produït una millora de 8 punts en l'índex de maduresa del control.

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

### Objectiu del control

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

### Situació del control

L'Ajuntament ha millorat el sistema de còpies vist en la nostra auditoria anterior. No obstant això, no ha aprovat un procediment destinat a aquest efecte, aspecte especialment rellevant en aquest control.

El departament TIC ha realitzat dues millores que han permés evolucionar des del seu sistema anterior de còpies. D'una banda, han integrat una nova solució per a albergar les dades de la còpia de seguretat de manera xifrada i immutable, impedint l'alteració de la informació per part de qualsevol procés de sistema o usuari. D'altra banda, han contractat un nivell addicional de còpies de seguretat en el núvol.

Una de les bones pràctiques dutes a terme pel departament d'informàtica és la creació de *tickets* que funcionen com a recordatoris periòdics per a la revisió de còpies de seguretat.

Encara que el departament afirma realitzar proves de restauració de les còpies de diferents sistemes, aquestes restauracions no són planificades ni documentades, ni estan establides en un document formalment aprovat.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 63,3%**, 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 79,2%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 60,8%, per tant, s'ha produït una lleu millora de 2,5 punts en l'índex de maduresa del control.

# 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 governança de ciberseguretat adequada.

## Situació del control

### Compliment de l'ENS

L'Ajuntament no ha realitzat les accions recomanades durant la nostra revisió de 2019, realitzades a fi de complir el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica. En conseqüència, continuen vigents les mancances identificades i les recomanacions realitzades en l'informe precedent.

### Compliment de l'RGPD

Quant al compliment en matèria de protecció de dades personals, des de la revisió realitzada l'any 2019 l'Ajuntament afirma haver aplicat determinades mesures per a protegir les dades de caràcter personal i que ha adaptat el DPD d'alguns sistemes a la normativa vigent. No obstant això, no s'ha aportat documentació sobre aquest tema.

### Compliment de la legalitat del registre de factures

S'ha aportat l'auditoria de sistemes exigida per la Llei 25/2013, de 27 de desembre.

### Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat ha posat de manifest que hi ha un grau insuficient de compliment de la normativa. L'**índex de maduresa és del 61,0%**, que es correspon amb un **nivell de maduresa N2,** que indica que existeixen incompliments significatius de la normativa i hi ha aspectes que s'han de millorar.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 50,0%, que es correspon amb un nivell de maduresa *N2*. Per tant, s'ha produït una millora d'11 punts en l'índex de maduresa del control.

### Governança de ciberseguretat

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

Si bé en l'auditoria hem observat cert nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament i particularment dels

responsables de les àrees implicades, hi ha mancances rellevants que indiquen que la governança no es pot considerar efectiva.

Les mancances més rellevants identificades i que dificulten l'establiment d'un adequat sistema de gestió de la seguretat de la informació (SGSI) són les següents:

- La política de seguretat de la informació (PSI) està formalment aprovada però està desactualitzada i no reflecteix la realitat de la institució.

- La inexistència de procediments de seguretat formalment assumits per l'organització i que s'apliquen de manera homogènia a totes les seues àrees.

- La falta d'activitat del Comité de Seguretat, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat, que ha de reunir-se periòdicament i assumir un caràcter proactiu en la presa de totes les decisions que afecten la seguretat de la informació.

- La falta d'activitat dels rols clau en l'organització, particularment el responsable de seguretat, les responsabilitats del qual es troben detallades i assignades en la política de seguretat, però no s'exerceixen de manera efectiva.

- Hi ha insuficiència de recursos econòmics i humans reportada pel departament TIC per a atendre:

    - La necessitat d'actualització de certs sistemes en el CPD o la situació del sistema economicofinancer.

    - La necessitat de cobrir les vacants existents de personal en el departament TIC.

No obstant això, s'han identificat determinats aspectes positius en la gestió de la ciberseguretat:

- Les activitats formatives i de conscienciació al personal de la corporació, que estan sent adequadament organitzades i gestionades i que estan reportant resultats positius, amb un alt grau d'acceptació per part del personal de l'Ajuntament.

- La investigació proactiva i l'ús de solucions innovadores per a la gestió o implantació de determinats controls de seguretat.

- 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, eliminar les mancances més rellevants identificades i aconseguir el compliment normatiu.

- L'esforç, per part dels responsables de les àrees relacionades, en la identificació de necessitats, requisits i la seua comunicació adequada a la corporació per mitjà d'informes de necessitat.

- L'existència d'una planificació estratègica d'actuacions en el marc de la ciberseguretat.

És urgent solucionar, per tant, les mancances identificades, ja que afecten de manera negativa el nivell de seguretat de la informació, i explotar les fortaleses existents, que facilitaran l'aplicació de mesures necessàries i de les recomanacions efectuades en aquest informe per a articular de manera efectiva l'SGSI de l'Ajuntament.

# APÈNDIX 3
## Bones pràctiques destacables

## Introducció

Amb caràcter general, si una entitat aconsegueix una valoració del 80% en l'índex de maduresa d'un control significa que està aplicant de manera raonable les bones pràctiques en matèria de seguretat de la informació establides en l'ENS o en les guies professionals corresponents, que se sintetitzen en el quadre 5 d'aquest informe. En un altre cas l'entitat ha d'adoptar mesures per a millorar la seua ciberseguretat i aconseguir aquesta meta.

Addicionalment a la valoració dels controls bàsics de ciberseguretat, és convenient destacar determinats aspectes, pràctiques, solucions tècniques o sistemes que s'han identificat o revisat durant la realització de l'auditoria i que destaquen en relació amb l'estat de l'art sobre una determinada matèria. Aquests aspectes proporcionen per la seua singularitat un coneixement addicional que facilita la interpretació, contextualització i avaluació dels resultats obtinguts en els procediments d'auditoria per a la valoració dels controls.

A més, atés el caràcter positiu dels aspectes considerats en aquest apartat, la seua identificació pot, en determinats casos, constituir la base de sinergies entre administracions públiques de la mateixa naturalesa i amb característiques similars, ja que es poden reproduir si es donen necessitats i problemàtiques comunes.

El criteri per a determinar si un aspecte és considerat bona pràctica destacable és l'existència d'una o diverses de les circumstàncies següents:

- solucions o sistemes especialment avançats o efectius des del punt de vista tecnològic,
- processos de gestió particularment madurs, i
- solucions o processos poc freqüents entre les entitats auditades, però de demostrada eficàcia davant de les necessitats de l'entitat, independentment de la seua complexitat o innovació.

Els aspectes destacats a continuació, en general, s'han considerat en l'avaluació dels CBCS. No obstant això, alguns no formen part dels CBCS tal com estan definits en la GPF-OCEX 5313, però els comentem per les raons indicades abans. Cal aclarir que l'existència d'aspectes concrets particularment rellevants no implica necessàriament que el control global dispose de la maduresa requerida, ja que la seua valoració inclou la consideració d'un conjunt d'aspectes tècnics, organitzatius i formals que s'han d'aconseguir individualment i en conjunt, amb un determinat nivell d'efectivitat i maduresa.

## Plataforma per a la gestió i dinamització de la conscienciació en la ciberseguretat

Un dels aspectes en què el departament TIC està fent un esforç notable ha sigut en la conscienciació dels treballadors de tota l'organització. Per a això, l'Ajuntament utilitza una plataforma des de la qual es programen diferents campanyes de conscienciació i accions de duració curta que es llancen als usuaris. Aquestes campanyes inclouen la difusió de notícies, exàmens, proves de *phishing*, etc.

Els resultats obtinguts són analitzats i permeten avaluar l'estat de conscienciació de l'entitat, emetent informes amb indicadors sobre el nivell de risc. L'eina té la capacitat de filtrar els resultats per àrees o fins i tot per usuaris.

L'ús d'aquest tipus d'eines a l'Ajuntament permet, d'acord amb els resultats obtinguts, augmentar de manera considerable la cultura de ciberseguretat de tots els membres de l'organització. A més, no es tracta d'un projecte executat en un moment puntual, sinó que està enfocat com un procés de millora contínua.

## Vigilància digital/Cibervigilància

L'Ajuntament ha implantat una eina de vigilància digital, un servei basat en robots que rastregen la xarxa a la recerca de filtracions d'informació de l'organització, i emeten alertes de les incidències detectades. Aquestes alertes són rebudes pels membres del departament TIC, que supervisen els informes generats i realitzen les accions pertinents.

Aquesta eina proporciona un indicador de l'estat de la ciberseguretat de l'entitat basat en l'anàlisi de diferents aspectes, com la fuga de dades o credencials, seguretat en el correu electrònic, anàlisi web o reputació IP, entre altres.

Aquest sistema de vigilància digital, juntament amb les alertes de les aplicacions implantades del CCN-CERT i CSIRT-CV, completen el sistema de detecció d'anomalies i incidències dins i fora de la xarxa.

# 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'alcaldessa 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'amenaces i rastreig d'informació sensible a través d'internet basat 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'informació i esdeveniments 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:**[16] Un sistema EDR, acrònim en anglés de *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. Als efectes 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 descriuen: *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 estarà a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, estarà 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.

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

**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 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 es proposa: normes de seguretat i procediments de seguretat.

**Procediments de seguretat:** Aborden tasques concretes, i indiquen què 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 de Noves Tecnologies de l'Ajuntament i amb el coordinador tècnic del Servei Municipal d'Informàtica i Comunicacions 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 18 d'octubre de 2022, va aprovar aquest informe d'auditoria.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

# Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

**Informe seguiment recomanacions CBCS Ajuntament Sagunt 2019 - SEFYCU 3562416**

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 ZANH AJZV NHE4 N7MC

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<br>Síndic Major | Firma electrònica - ACCV - 18/10/22 11:48<br>VICENT CUCARELLA TORMO |