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 D'ALCOI DE L'ANY 2020

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 d'una 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, las entitats locals han sigut un dels objectius més afectats per les recents onades de ciberatacs.

Atesa aquesta realitat, i en sintonia amb el seu pla estratègic actual, la Sindicatura de Comptes ha fet un treball de seguiment dels controls bàsics de ciberseguretat (CBCS) de l'Ajuntament d'Alcoi respecte a la situació mostrada en l'auditoria de l'any 2020.

## Conclusions

Encara que s'han fet 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.

L'índex de maduresa general dels CBCS mostra un valor del 58,8%, per la qual cosa l'Ajuntament ha d'adoptar mesures amb la finalitat d'aconseguir l'objectiu del 80%. A pesar de la millora experimentada des de l'índex de maduresa del 47,3% identificat en la nostra auditoria de 2020, el nivell d'efectivitat en els controls analitzats és insuficient. Hi ha possibilitats clares de millora per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en els controls que presenten deficiències significatives.

L'Ajuntament d'Alcoi té establida una acceptable governança de la ciberseguretat, però ha de reforçar el suport en forma de recursos pressupostaris dedicats a la seguretat de la informació.

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. Respecte de l'Esquema Nacional de Seguretat, l'Ajuntament ha d'atendre i solucionar les no conformitats identificades en l'auditoria de compliment realitzada l'any 2021. En relació amb la protecció de dades personals, l'Ajuntament ha d'elaborar el registre d'activitats de tractament i publicar-lo.

També hem efectuat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament, entre les quals aconsellem implantar de manera general en tots els sistemes de l'entitat el procediment aprovat existent per a la gestió d'usuaris amb privilegis d'administració, millorar i aprovar el procediment de seguretat elaborat per a la identificació i solució de vulnerabilitats, i aplicar de manera efectiva els principis i les mesures per al tractament de registres d'activitat que són detallats en el procediment de gestió d'usuaris aprovat.

**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 d'Alcoi de l'any 2020

**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, aquelles que d'acord amb l'ordenament jurídic siguen convenients per a assegurar adequadament el compliment dels principis financers, de legalitat, d'eficàcia, d'economia i de transparència, exigibles al sector públic, així com la sostenibilitat ambiental i la igualtat de gènere. D'altra banda, l'article 11 de la mateixa llei estableix que, en l'exercici de la seua funció fiscalitzadora, la Sindicatura de Comptes està facultada per a **verificar la seguretat i fiabilitat dels sistemes informàtics** que suporten la informació economicofinancera, comptable i de gestió.

En la guia d'auditoria GPF-OCEX 5311, "Ciberseguretat, seguretat de la informació i auditoria externa", del *Manual de fiscalització* de la Sindicatura de Comptes, es destaca la importància creixent que les qüestions relacionades amb la ciberseguretat estan adquirint en la gestió de les administracions públiques, raó per la qual els auditors públics els han de prestar cada vegada més atenció. En línia amb això, **en el Pla Estratègic de la Sindicatura de Comptes per al període 2019-2022 s'assenyala la ciberseguretat com una de les àrees d'alt risc i prioritàries per a dur a terme la tasca fiscalitzadora**.

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 18 de de juny de 2020 el Consell de la Sindicatura de Comptes va aprovar l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Alcoi, Exercici 2020. 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 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 prenen tot el sentit conceptes com la ciberresiliència i la ciberhigiene. Per ciberresiliència es pot entendre la capacitat d'una entitat per a evitar o resistir i recuperar-se d'un ciberatac en un temps

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

## 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 d'Alcoi. Exercici 2020.

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

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

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada dels huit CBCS revisats en l'auditoria de l'any 2020, 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 fet 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 el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconsegueix un **índex de maduresa general del 58,8%**, 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 no formalitzats documentalment.

Encara que l'Ajuntament ha atés de manera parcial les nostres recomanacions i l'índex de maduresa general ha millorat des del 47,3% identificat en la nostra auditoria de 2020, l'índex de maduresa actual continua sent insuficient per a garantir un grau adequat de seguretat i aconseguir el 80% requerit per l'ENS.

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**

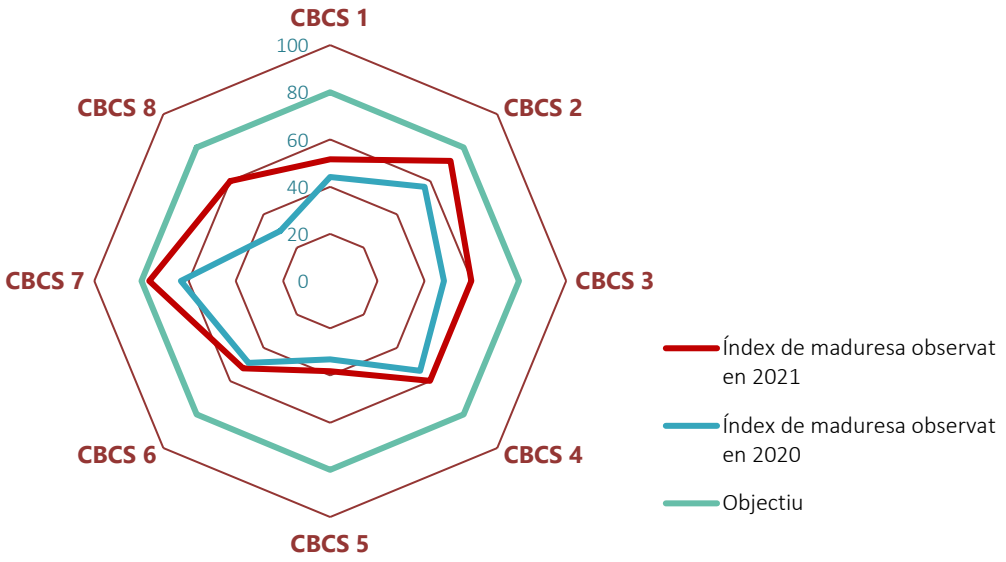
| Control | 2020 | | | 2021 | | |
|---|---|---|---|---|---|---|
| | Índex de maduresa | Nivell de maduresa | Índex de complí-ment | Índex de maduresa | Nivell de maduresa | Índex de complí-ment |
| **CBCS 1** Inventari i control de dispositius físics | *44,1%* | ***N1*** | *55,1%* | 51,6% | N2 | 64,5% |
| **CBCS 2** Inventari i control de programari autoritzat i no autoritzat | *56,5%* | ***N2*** | *70,6%* | 72,0% | N2 | 90,0% |
| **CBCS 3** Procés continu d'identificació i solució de vulnerabilitats | *48,2%* | ***N1*** | *60,3%* | 59,8% | N2 | 74,7% |
| **CBCS 4** Ús controlat de privilegis administratius | *53,8%* | ***N2*** | *67,3%* | 59,8% | N2 | 74,7% |
| **CBCS 5** Configuracions segures del programari i maquinari | *33,2%* | ***N1*** | *41,5%* | 38,2% | **N1** | 47,8% |
| **CBCS 6** Registre de l'activitat dels usuaris | *49,0%* | ***N1*** | *61,3%* | 52,3% | N2 | 65,4% |
| **CBCS 7** Còpies de seguretat de dades i sistemes | *63,3%* | ***N2*** | *79,2%* | 76,7% | N2 | 95,8% |
| **CBCS 8** Compliment normatiu i governança de ciberseguretat | *30,0%* | ***N1*** | *37,5%* | 60,0% | N2 | 75,0% |
| General | 47,3% | ***N1*** | 59,1% | 58,8% | N2 | 73,5% |

L'índex de compliment dels CBCS és del 73,5%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*. Aquest índex ha millorat des del 59,1% del nostre informe anterior. La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2020 mostra una millora en tots els controls, si bé ha sigut insuficient i cap aconsegueix l'objectiu, atés el baix grau d'atenció a les nostres recomanacions (vegeu l'apartat 5 següent).

A pesar de la millora experimentada, el nivell d'efectivitat en els controls analitzats és insuficient i hi ha possibilitats clares de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació, i particularment sobre el control, que presenta deficiències significatives i no aconsegueix el nivell de maduresa N2 (CBCS 5). En l'apartat 5 es realitzen les recomanacions pertinents amb aquesta finalitat.

D'una manera més sintètica i gràfica, la situació observada dels controls es reflecteix en el gràfic 1, tant en aquesta auditoria com en la realitzada l'any 2020.

**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 d'Alcoi té establida una governança acceptable de la ciberseguretat, però ha de reforçar el suport en forma de recursos 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.

Hem pogut verificar l'existència d'aquest compromís amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament, la qual cosa, juntament amb l'existència d'uns processos de gestió adequats, ens permet afirmar que la governança de ciberseguretat presenta un nivell acceptable.

No obstant això, resulta necessari impulsar de manera proactiva iniciatives per a millorar la ciberhigiene i la ciberresiliència. Particularment, s'ha d'incrementar el suport en forma de recursos pressupostaris que permeten donar compliment als objectius en matèria de seguretat, incloent-hi el desenvolupament de projectes i la implantació de sistemes necessaris per a l'establiment i millora dels controls de ciberseguretat.

### 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 nivell insuficient de compliment de la normativa. Hi ha incompliments significatius, que s'assenyalen 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 2020, 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. Actualitzar i millorar el procediment aprovat per a la gestió de l'inventari i el control d'actius físics de manera que reculla, amplie i represente amb fidelitat el conjunt de mesures implantades en la pràctica.

2. Implantar les solucions 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. Actualitzar i millorar el procediment aprovat per a la gestió de l'inventari i el control de programari de manera que reculla, amplie i represente amb fidelitat el conjunt de mesures implantades en la pràctica. Addicionalment, recomanem aprovar formalment el pla anual de manteniment preventiu i predictiu existent i la llista de programari autoritzat inclosa en aquest.

4. La recomanació de l'informe de 2020 s'ha implementat.

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

5. Millorar i aprovar el procediment de seguretat elaborat per a la identificació i solució de vulnerabilitats, de manera que incloga la priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats, identificant dates, prioritat, responsable, solució, etc.

Per a la millora dels processos existents d'identificació de vulnerabilitats es proposa l'ús d'eines d'escaneig i la realització de tests de penetració.

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

6. Implantar de manera general en tots els sistemes de l'entitat el procediment aprovat existent per a la gestió d'usuaris amb privilegis d'administració, i específicament:

   - L'eliminació dels usuaris no nominatius amb privilegis administratius dels sistemes. Totes les activitats de gestió hauran de realitzar-se amb usuaris nominatius.

   - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, l'ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.

   - La utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes nominatius 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).

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

7. Ampliar i implantar de manera efectiva en tots els sistemes de l'entitat el procediment existent de configuració segura dels sistemes. 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. I fer extensiva a tots els sistemes de l'entitat la gestió d'aquestes guies per mitjà de les eines disponibles per a la gestió de fluxos de treball.

   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 a través d'eines automatitzades de monitoratge de la configuració.

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

8. Aplicar de manera efectiva els principis i mesures per al tractament de registres d'activitat detallats en el procediment de gestió d'usuaris, i particularment els referits a la retenció, protecció i centralització de registres d'activitat.

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

9. Millorar el procediment formalment aprovat per a la gestió de còpies de seguretat de dades i sistemes, de manera que detalle com a mínim les dades i sistemes afectats, la

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

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

Hi ha diversos aspectes sobre els quals l'Ajuntament ha d'actuar per a esmenar les deficiències identificades:

10. Per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat, l'Ajuntament ha d'atendre i solucionar les no conformitats identificades en l'auditoria de compliment de l'ENS realitzada l'any 2021 i, posteriorment, publicar en la seu electrònica les certificacions 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.

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

    - Elaborar el registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la LO 3/2018.

    - Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.

    - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.

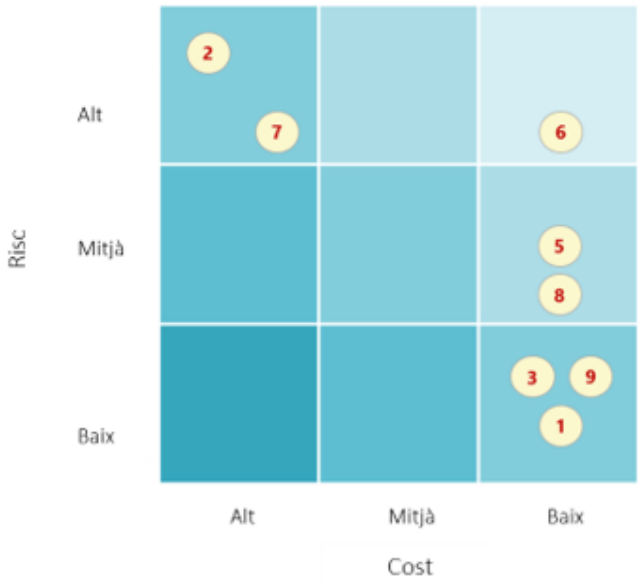
    - Planificar i executar auditories de compliment en matèria de protecció de dades.

12. L'incompliment assenyalat en l'informe de 2020 s'ha esmenat.

## 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 2020, adaptant la relació risc/cost de cada recomanació i considerant les millores realitzades des de la revisió anterior. No s'hi inclouen els punts 10 i 11 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 2020.

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

## Actuacions en curs

Encara que no s'han tingut en compte en el càlcul dels indicadors mostrats en l'apartat 4, hem verificat que en el moment de finalització del treball de camp de l'auditoria s'han iniciat o planificat actuacions en matèria de ciberseguretat en diversos àmbits que atendrien algunes de les recomanacions anteriors. Aquestes actuacions es troben alineades amb els objectius de l'Ajuntament per a l'adequació a l'ENS i algunes s'han iniciat a conseqüència de les recomanacions realitzades en l'auditoria de l'any 2020. La implantació efectiva d'aquestes actuacions tindrà un impacte positiu en el nivell de ciberseguretat de l'entitat i per la seua rellevància s'han de destacar en l'Informe.

L'Ajuntament es troba en procés de desplegament de la tecnologia i els mitjans necessaris per a implantar un centre d'operacions de ciberseguretat. El projecte inclou l'ús 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, i l'adquisició i desplegament de solucions finançades a través dels fons europeus Next Generation EU.

Està prevista la implantació, entre altres, de les solucions del Centre Criptològic Nacional:

- LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces), eina per a la gestió de ciberincidents en les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat.

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

- CLAUDIA, solució d'*endpoint*[2] integrada amb l'eina CARMEN que permet tindre una visió més completa del que ocorre dins d'una xarxa.

- GLORIA, plataforma per a la gestió d'incidents i amenaces de ciberseguretat a través de tècniques de correlació complexa d'incidències (SIEM).

- 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.

- MicroCLAUDIA, que ja es troba desplegada en l'organització i que proporciona protecció contra codi nociu de tipus *ransomware*.[3]

[2] Un punt final o *endpoint* és un dispositiu informàtic remot que es comunica a través d'una xarxa a la qual està connectat. Es refereix típicament a dispositius utilitzats com ara ordinadors d'escriptori, portàtils, telèfons intel·ligents, tauletes o dispositius d'Internet de les coses.

[3] Un segrestador, *ransomware,* és un tipus de programa nociu que restringeix l'accés a determinades parts o arxius del sistema operatiu infectat i demana un rescat a canvi de llevar aquesta restricció.

## 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, incloent-hi el calendari per a les revisions periòdiques de maquinari i l'actualització de l'inventari. | S'ha elaborat i aprovat un procediment per a inventariar actius. No obstant això, el procediment es troba desactualitzat, no té el detall necessari i no representa amb fidelitat el control implantat en la realitat.<br>S'han millorat els processos d'inventari i gestió d'actius per mitjà d'un ús adequat de les eines disponibles. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |
| **2** | Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa. | Sense variació. | **No aplicada** | Es manté la redacció. |
| **3** | Elaborar i aprovar formalment un procediment per a la gestió integral del programari de l'entitat que preveja:<br>- L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques de programari.<br>- La definició d'un pla de manteniment de la totalitat del programari utilitzat, d'acord amb el que s'especifica en el procediment aprovat per al manteniment d'actius de maquinari i programari. | S'ha elaborat i aprovat un procediment per a inventariar actius. No obstant això, el procediment es troba desactualitzat, no té el detall necessari i no representa amb fidelitat el control implantat en la realitat.<br>S'han millorat els processos d'inventari i gestió d'actius per mitjà d'un ús adequat de les eines disponibles.<br>S'ha elaborat i aprovat un procediment de gestió de manteniment. I un pla anual de manteniment preventiu i predictiu, que inclou una llista blanca d'aplicacions, però li falta l'aprovació formal.<br>S'ha elaborat i aprovat una normativa d'ús de recursos que especifica les limitacions respecte a l'ús de programari no autoritzat. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |
| **4** | Revisar i actualitzar tots els sistemes que es troben fora del període de suport. | S'han actualitzat els sistemes que es trobaven fora del període de suport. | **Aplicada** | S'elimina la recomanació feta en 2020. |

| | 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 o incloure en algun dels procediments de seguretat el procés d'identificació i solució de vulnerabilitats, incloent-hi 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, identificant dates, prioritat, responsable, solució, etc.<br><br>Per a la millora dels processos existents d'identificació de vulnerabilitats es proposa l'ús d'eines d'escaneig i la realització de tests de penetració. | S'ha elaborat un procediment per a la identificació i solució de vulnerabilitats, però no s'ha aprovat formalment.<br><br>S'ha millorat de manera general la gestió de la resolució de vulnerabilitats identificades per mitjà de l'ús de les eines disponibles per a la gestió de fluxos de treball. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |
| **6** | Implantar en tots els sistemes de l'entitat un procediment de gestió d'usuaris amb privilegis d'administració, que almenys preveja:<br><br>- L'eliminació, sempre que siga possible des del punt de vista tècnic, dels usuaris no nominatius amb privilegis administratius dels sistemes. Totes les activitats de gestió s'han de realitzar amb usuaris nominatius.<br>- Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, l'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 nominatius 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). | S'han realitzat millores respecte a l'ús de comptes d'usuaris nominatius no compartits en els sistemes i s'han eliminat o substituït comptes d'usuaris d'administració per defecte. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |

| | 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 |
|---|---|---|---|---|
| **7** | Ampliar i implantar de manera efectiva en tots els sistemes de l'entitat el procediment existent de configuració segura dels sistemes. 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.<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 de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració. | S'han millorat les plantilles de configuració dels equips d'usuari i la gestió de la seua aplicació, per mitjà de l'ús de les eines disponibles per a gestió de fluxos de treball. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |
| **8** | Aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte. | S'ha aprovat un procediment de gestió d'usuaris que especifica el control de registres d'activitat en els sistemes de l'entitat. No obstant això, aquest procediment no s'ha implantat completament en l'entitat i únicament se n'apliquen determinats aspectes. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |
| **9** | Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies. | S'ha elaborat i aprovat un procediment per a la gestió de còpies de seguretat. No obstant això, aquest no té el detall necessari i no descriu amb fidelitat el control implantat.<br>S'han aplicat mesures de protecció addicionals sobre les còpies de seguretat existents.<br>S'ha millorat la gestió de proves de recuperació, per mitjà de l'ús d'eina de gestió de fluxos de treball. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |
| **10** | 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: | S'ha renovat el marc documental per al compliment de l'ENS, incloent-hi política de seguretat, normativa i procediments. | **Aplicada parcialment** | S'actualitza la redacció feta en 2020. |

| | 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 |
|---|---|---|---|---|
| | - Realitzar les auditories 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. | S'ha realitzat una auditoria per a verificar el grau de compliment i adaptació a l'ENS. | | |
| **11** | 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:<br>- Elaborar el registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.<br>- Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.<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 en matèria de protecció de dades. | Sense variació. | **No aplicada** | Es manté la redacció. |
| **12** | Dur a terme l'auditoria del registre de factures exigida 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 feta en 2020. |

# APÈNDIX 1
# Metodologia aplicada

## Introducció

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

Les entitats locals, i els ajuntaments en particular, no són alienes a aquesta problemàtica de la ciberseguretat en la seua pròpia 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.

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

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

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

## Objectiu de l'auditoria

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022, el nostre objectiu ha sigut realitzar el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Alcoi. Exercici 2020, així com obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això hem avaluat tant el seu disseny[5] com la seua eficàcia operativa[6] 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 2020, 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 a 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

[5] L'avaluació del disseny d'un control implica la consideració per l'auditor 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.

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

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

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

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

## Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls a 31 de desembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe, ja que fins llavors ha sigut admesa 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 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),[7] que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. L'avantatge principal d'aquests controls 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

Com 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 a la Sindicatura la realització de les auditories de ciberseguretat 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 següents referències de l'ENS:

[7] 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[8] 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", reduint els ciberriscos.[9]

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.[10]

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.

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

[9] 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.

[10] 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 les quals s'especifica amb el màxim detall els aspectes comprovats en cada control.

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

| Control | Objectiu del control | Subcontrol | |
|---|---|---|---|
| **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 estàndards 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 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 es basen en la *Guía de seguridad 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'ha 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 als quals està exposat, sota el criteri del principi de proporcionalitat.

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[11]

| 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%.**

[11] *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 preveu 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 la seua aplicació als CBCS, ja que permeten dur a terme un resum de l'estat de les mesures de seguretat dels ens auditats:

- L'**índex de maduresa** sintetitza, en tant per cent, el nivell de maduresa 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.[12]

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.**[13]

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.

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

[13] 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.[14] L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació[15] que ha de materialitzar-se en aspectes com ara:

- D'acord amb l'article 11 del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat, ha de formular-se la **política de seguretat de la informació (PSI) que ha de ser aprovada pel titular de l'òrgan superior** de l'entitat. Aquesta PSI s'ha de difondre entre la totalitat dels membres de l'organització, com també, si és el cas, a proveïdors i tercers.

- Assignar els rols i responsabilitats en matèria de seguretat de la informació. Els òrgans superiors de l'entitat han de nomenar el **responsable de la informació** (que pot tractar-se d'una persona o un òrgan col·legiat), el **responsable del servei** (que pot ser el mateix que l'anterior), el **responsable de la seguretat** i el **responsable del sistema**.

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

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

  La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,[16] 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 adequadament planificades.

- Decidir els criteris de valoració 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.

[14] *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.

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

[16] *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 d'Alcoi. Exercici 2020.

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 els seus 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'hi inclouen en aquesta categoria les recomanacions que, encara que acceptades o fins i tot aplicades i corregides per l'ens fiscalitzat, necessitarien obligatòriament alguna prova addicional per a contrastar el que ha manifestat l'ens fiscalitzat que excedeixen l'abast previst en el treball. |

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

## Comunicació i confidencialitat

Ens comuniquem amb els responsables de l'entitat en relació, entre altres qüestions, amb l'abast i el moment de realització de l'auditoria planificats i les constatacions significatives de l'auditoria, com també amb qualsevol deficiència significativa dels controls interns que identifiquem en el transcurs 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 ha elaborat i aprovat formalment un procediment que detalla el procés per a la gestió de l'inventari d'actius. No obstant això, el procediment es troba desactualitzat, no té el detall necessari i no representa amb fidelitat el control implantat en la realitat.

La gestió de l'inventari ha sigut millorada per l'explotació adequada de l'eina de gestió de fluxos de treball i *ticketing*, que inclou, a més d'un inventari d'actius físics i programari, la relació entre actius, la gestió de canvis, la realització periòdica de tasques preventives i l'elaboració d'informes d'indicadors per a la direcció.

No s'han implantat mesures tècniques addicionals per a restringir l'accés de dispositius físics no autoritzats. No obstant això, s'han iniciat gestions i s'han analitzat solucions per a la licitació d'un sistema NAC per a control d'accés a la xarxa.

Existeix cert nivell de control sobre l'inventari i el control d'actius físics, i la seua valoració global aconsegueix un **índex de maduresa del 51,6%**, 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 1 del 64,5%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 44,1%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 7,5 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 ha elaborat i aprovat formalment un procediment que detalla el procés per a la gestió de l'inventari del programari. No obstant això, el procediment es troba

desactualitzat, li falta el detall necessari i no representa amb fidelitat el control implantat en la realitat.

L'inventari de programari es manté correctament actualitzat per mitjà de diverses eines que proporcionen i faciliten diferents controls de seguretat posteriors. Algunes d'aquestes eines no es trobaven disponibles en el treball de revisió anterior i hem verificat que han sigut desplegades i explotades adequadament.

L'Ajuntament disposa d'un pla anual de manteniment preventiu i predictiu que, encara que no està formalment aprovat, facilita, juntament amb altres processos implantats, una gestió adequada de manteniments i llicències. A més, hem verificat que s'han actualitzat els sistemes que es trobaven fora del període de suport.

S'han implantat nous processos efectius per al control sobre programari no autoritzat, incloent-hi la realització de revisions periòdiques, la gestió de les quals es troba adequadament automatitzada per mitjà de les eines disponibles. Si bé es disposa d'una normativa aprovada que descriu les limitacions de l'ús de programari no autoritzat, aquesta no detalla completament el control implantat.

Hi ha un cert nivell de control sobre l'inventari i control del programari autoritzat, que aconsegueix un **índex de maduresa del 72,0%**, 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 90,0%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 56,5%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 15,5 punts en l'índex de maduresa del control.

## 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

L'Ajuntament ha elaborat un procediment que inclou el detall necessari sobre el control implantat i sobre els actius que s'han inclòs en el control. No obstant això, aquest procediment no es troba formalment aprovat.

A més, hem verificat que s'han millorat els processos de gestió per mitjà de l'ús adequat de les eines disponibles per a gestió de fluxos de treball. També s'han millorat els mecanismes d'identificació de vulnerabilitats per mitjà de la incorporació d'eines específiques, que s'utilitzen de manera puntual davant determinades situacions.

L'Ajuntament ha implantat l'eina microCLAUDIA del Centre Criptològic Nacional. Hem verificat que s'ha instal·lat adequadament en els sistemes Windows de la corporació i es realitzen els corresponents desplegaments de vacunes davant de codi nociu. Addicionalment es troben en fase de desplegament diverses eines del Centre Criptològic Nacional, en el marc del Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana, que proporcionen capacitat d'identificació en perímetre d'amenaces persistents avançades i detecció d'amenaces en *endpoint*.

Hi ha un cert nivell de control sobre la gestió de vulnerabilitats, i la valoració global del control presenta un **índex de maduresa del 59,8%**, 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 74,7%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 48,2%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora d'11,6 punts en l'índex de maduresa del control.

## 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

Hem analitzat les accions que realitza l'Ajuntament per al control dels comptes d'administració i hem verificat que, si bé hi ha determinades mesures per al control de comptes d'administració i han sigut establides en un procediment formalment aprovat, aquestes no es troben implantades de manera homogènia en tots els sistemes.

S'han identificat millores quant a l'ús d'usuaris nominatius no compartits en els sistemes de l'entitat, específicament en els sistemes de virtualització i de seguretat perimetral.

A més, hem verificat que s'han eliminat o substituït els usuaris per defecte de part dels sistemes, en un procés de revisió que s'està executant en el moment de realització de l'auditoria.

Hi ha cert nivell de control sobre els comptes amb privilegis administratius, per la qual cosa la valoració global del control existent aconsegueix un **índex de maduresa del 59,8%**, 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 4 del 74,7%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 53,8%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 6 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 el control implantat per l'Ajuntament per a la configuració segura d'aplicacions i dispositius i hem verificat que es troba parcialment establit en un procediment formalment aprovat, però no s'han implantat totes les mesures que s'hi descriuen ni el procés s'ha fet extensiu a tots els sistemes de l'entitat.

S'han realitzat millores respecte a les plantilles de configuració i la gestió de la seua aplicació per mitjà de l'ús de les eines disponibles per a gestió de fluxos de treball, particularment sobre les plantilles de configuració d'equips d'usuari.

La valoració global del control existent sobre les configuracions segures és que l'organització aconsegueix un **índex de maduresa del 38,2%**, 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 47,8%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 33,2%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 5 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

Hem analitzat les accions aplicades per l'Ajuntament per al registre de l'activitat dels seus usuaris en els diferents sistemes i hem verificat que s'ha aprovat un procediment de gestió d'usuaris que especifica el control de registres d'activitat en els sistemes de l'entitat.

Aquest procediment especifica la informació que cal emmagatzemar, els requisits de retenció i protecció i els sistemes afectats pel control. No obstant això, hem verificat que aquest procediment no s'ha implantat completament en l'entitat i únicament se n'apliquen determinats aspectes.

No s'han fet altres canvis organitzatius o tècnics per a la resta del control. Sí que hem pogut verificar que s'han analitzat solucions i s'han iniciat les gestions necessàries per a la futura licitació d'un sistema SIEM i la provisió d'un servei vSOC.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 52,3%**, 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 6 del 65,4%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 49,0%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 3,3 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 elaborat i aprovat un procediment sobre la gestió de còpies de seguretat de dades i sistemes. No obstant això, el procediment no té el detall i maduresa necessaris i no descriu amb fidelitat el control implantat.

Hem verificat que s'han establit millores respecte a la realització de proves de recuperació, que es realitzen de manera periòdica i la seua execució i revisió es troba gestionada per mitjà de tasques periòdiques establides en l'eina disponible per a gestió de fluxos de treball.

A més, s'han establit polítiques de còpia desconnectades addicionals, que per la seua naturalesa contribueixen a incrementar el nivell de protecció d'aquestes.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 76,7%**, 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 7 del 95,8%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 63,3%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 13,4 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 adequada governança de ciberseguretat.

### Situació del control

#### Compliment de l'ENS

Des de la revisió realitzada l'any 2020, l'Ajuntament ha realitzat les accions següents que han millorat el nivell de compliment exigit pel Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica:

- El dia 22 de juny de 2021, el Ple municipal va acordar l'actualització i aprovació de la política, normativa i procediments de seguretat de la informació, d'acord amb l'Esquema Nacional de Seguretat.
- S'han elaborat i aprovat versions actualitzades de la declaració d'aplicabilitat i el pla d'adequació.
- S'ha emplenat i remés anualment l'Informe de l'Estat de la Seguretat (Informe INES).
- S'ha realitzat l'any 2021 una auditoria de compliment, prevista en l'article 34.

A pesar de les iniciatives anteriors, hi ha mancances que s'han d'esmenar, en particular no s'ha implantat la totalitat de les mesures de seguretat i accions previstes en la declaració d'aplicabilitat i el pla d'adequació, que han sigut planificades en un projecte organitzat en fases la finalització de les quals s'ha establit per a març de 2023. En conseqüència, no s'ha certificat el compliment de l'ENS.

#### Compliment de l'RGPD

Quant al compliment en matèria de protecció de dades personals, des de la revisió realitzada l'any 2020 l'Ajuntament no ha realitzat accions que hagen millorat el nivell de compliment de les exigències de l'RGPD.

En conseqüència, continuen vigents les mancances identificades i les recomanacions realitzades en l'informe precedent.

### Compliment de la legalitat del registre de factures

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

### Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió ha millorat respecte a l'informe emés l'any 2020 i l'Ajuntament aconsegueix un **índex de maduresa del 60,0%**, que es correspon amb un **nivell de maduresa N2**, que indica que encara hi ha incompliments significatius de la normativa i aspectes que s'han de millorar.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 30,0%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora substancial de 30,0 punts en l'índex de maduresa del control.

### Governança de ciberseguretat

L'Ajuntament d'Alcoi té establida una governança acceptable de la seguretat de la informació.

Hem pogut verificar l'existència d'aquest compromís amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament, la qual cosa, juntament amb l'existència d'uns adequats processos de gestió, ens permet afirmar que la governança de ciberseguretat presenta un nivell acceptable. Els aspectes fonamentals identificats que sustenten aquesta afirmació són:

- L'existència d'una política de seguretat de la informació aprovada, que constitueix el conjunt de directrius i principis que representen el compromís de l'entitat respecte a la protecció dels actius d'informació de l'Ajuntament.

- La definició i nomenament de rols, i la creació d'òrgans de govern de la seguretat de la informació, particularment el responsable de seguretat i el comité de seguretat TIC.

- El compromís amb la gestió i el compliment de requisits legals fonamentals relacionats amb la seguretat de la informació.

- L'atenció, encara que de manera parcial, de les necessitats de recursos humans per mitjà de la creació de places addicionals per al Departament d'Informàtica i Noves Tecnologies. La provisió d'aquests recursos, si bé no satisfà completament les necessitats respecte a la gestió dels sistemes d'informació i de la seguretat d'aquests, sí que facilitarà la distribució de tasques i responsabilitats, cosa que permetrà als tècnics responsables i gestors de la seguretat incrementar i optimitzar la seua dedicació a l'establiment efectiu d'un sistema de seguretat de la informació (SGSI).

- L'articulació de projectes, en el context d'utilització dels fons Next Generation EU, que tenen com a objecte promoure la seguretat de la informació, eliminar les mancances més rellevants identificades i aconseguir el compliment normatiu.

No obstant això, els òrgans superiors de l'Ajuntament han de reforçar l'actual nivell de suport i compromís amb la seguretat dels sistemes d'informació, a fi d'aconseguir els nivells de maduresa dels controls requerits per l'ENS i solucionar les deficiències identificades.

# 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 han sigut identificats o revisats 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 tinga 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.

## Explotació de l'eina de ticketing i gestió de fluxos de treball en determinats processos de l'entitat

L'entitat ha desplegat una eina de *ticketing* i gestió de fluxos de treball que ha sigut integrada amb determinats sistemes i processos interns d'una manera particularment efectiva.

Les implementacions i funcionalitats més rellevants de l'eina són:

- La categorització dels actius d'informació. S'ha desenvolupat la taxonomia completa d'elements del sistema d'informació de l'entitat i tots els actius s'han classificat d'acord amb aquesta taxonomia; això ha facilitat l'aplicació de controls que són dependents de la naturalesa de l'actiu.

- La identificació d'interdependències entre els actius d'informació, la qual cosa facilita l'aplicació de processos de control posteriors.

- La gestió de canvis en actius i sistemes d'informació de l'entitat, que es troba suportada per l'inventariat adequat d'actius i l'establiment d'interdependències i que ha facilitat les avaluacions d'impacte dels canvis gestionats.

- La generació d'informes de disponibilitat i altres indicadors departamentals, la qual cosa facilita la presa de decisions i la millora dels processos de control, aspecte imprescindible per a l'establiment de controls de maduresa N4 (Gestionat i mesurable) o superiors.

- L'establiment de tasques i controls preventius periòdics, la qual cosa assegura l'execució correcta de tasques i controls per part del personal del departament. Entre aquests controls es troben:

  - La realització de proves de restauració de còpies de seguretat
  - La revisió d'inventari d'actius i programari instal·lat.
  - La revisió de pedaços i actualitzacions.
  - La revisió de credencials d'usuari.
  - La realització d'accions de conscienciació.

# 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 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.

**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, i els funcionaris directors del departament TIC i els caps d'àrea o servei.

**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 descriuran: *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 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.

**Política de seguretat de la informació:** Es 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.

# TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que es preveu en la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'informe d'auditoria es va discutir amb el regidor delegat responsable d'Innovació, Indústria i Activitats, Societat Digital i amb el cap del Departament d'Informàtica i Noves Tecnologies, 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, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*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 l'exercici 2021, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

Una vegada 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, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*h* del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 25 de maig de 2022, va aprovar aquest informe d'auditoria.