

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'ALACANT DE L'ANY 2019**

Situació a 31 de desembre de 2021



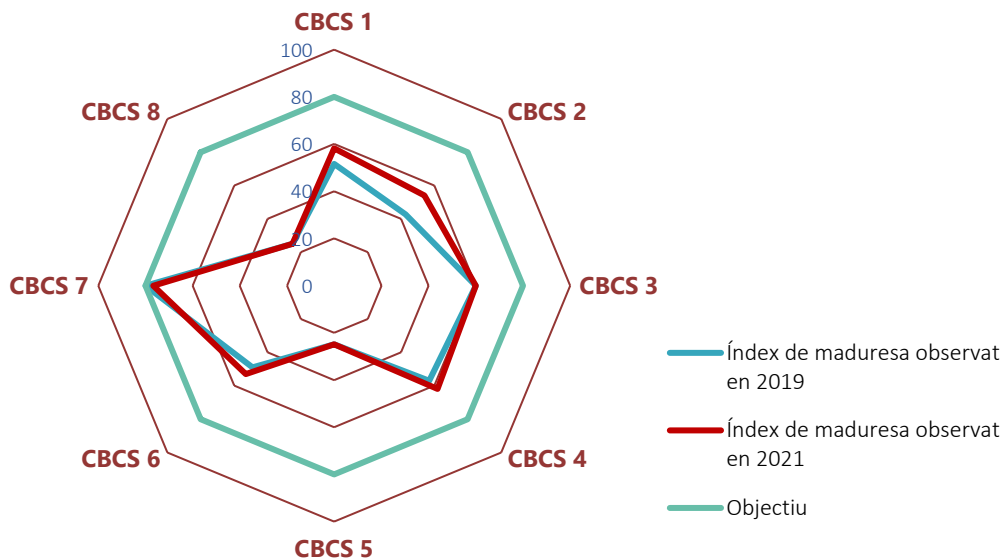
RESUM

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

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

Conclusions

Únicament s'han realitzat lleus progressos des de la nostra auditoria anterior i les nostres recomanacions només s'han atés parcialment. Per tant, l'índex de maduresa general dels controls bàsics de ciberseguretat mostra un valor del 51,7% (48,8% en 2019), per la qual cosa el nivell d'efectivitat en els controls analitzats continua sent insuficient i ha de millorar. Han d'implantar-se millores per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en aquells controls que presenten deficiències significatives.



L'Ajuntament d'Alacant no té establida una governança adequada de la ciberseguretat. Els òrgans superiors de l'Ajuntament, com a responsables del sistema de control, han de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.



Així mateix, la nostra revisió també ha posat de manifest un grau de compliment molt deficient quant a l'adequació a les normes legals relacionades amb la seguretat de la informació. L'informe assenyalava diversos aspectes sobre els quals s'ha d'actuar per a esmenar-los ràpidament. Pel que fa a l'Esquema Nacional de Seguretat, l'Ajuntament ha de realitzar la designació de les persones per als rols definits en la política de seguretat i constituir el comitè de seguretat de la informació.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament. Entre aquestes aconsellem finalitzar la implantació de solucions per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa, revisar i actualitzar tots els sistemes que es troben fora del període de suport i finalitzar i aprovar formalment el procediment per a gestió d'usuaris amb privilegis d'administració.

NOTA

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



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

Situació a 31 de desembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana



ÍNDEX (amb hipervincles)

1. Introducció	3
2. Responsabilitats dels òrgans superiors de l'Ajuntament en relació amb els controls de ciberseguretat	4
3. Responsabilitat de la Sindicatura de Comptes	4
4. Conclusions	5
5. Recomanacions i mesures per al compliment de la legalitat	8
Apèndix 1. Metodologia aplicada	18
Apèndix 2. Situació dels controls bàsics de ciberseguretat	35
Apèndix 3. Bones pràctiques destacables	44
Acrònims i glossari de termes	47
Tràmit d'al·legacions	49
Aprovació de l'Informe	50



1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

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

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

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 16 de gener de 2020 el Consell de la Sindicatura de Comptes va aprovar l'[Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Alacant, Exercici 2019](#). Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 fer un treball de seguiment de la situació dels controls bàsics de ciberseguretat d'aquest ajuntament i dels altres 14 ajuntaments analitzats.

La necessitat d'una adequada ciberhigiene

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

En aquests entorns actuals d'administració electrònica avançada prenen tot el sentit conceptes com la ciberresiliència i la ciberhigiene. Per ciberresiliència es pot entendre la capacitat d'una entitat per a evitar o resistir un ciberatac i per a recuperar-se'n en un temps



raonable per a continuar prestant els seus serveis. La ciberhigiene és un principi fonamental¹ 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'Alacant, exercici 2019.

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

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

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



sistemes que suporten el procés comptable-pessupostari, 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, així com també que planifiquem i executem l'auditoria amb la finalitat d'obtenir 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 obtenir 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

L'índex de maduresa general dels controls bàsics de ciberseguretat és insuficient i ha de millorar per a aconseguir els nivells exigits per l'ENS

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que l'**índex de maduresa general** en la gestió dels controls bàsics de ciberseguretat aconseguix un **51,7%**, 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.

L'Ajuntament únicament ha atés de manera parcial algunes de les nostres recomanacions i l'índex de maduresa general ha millorat lleument des del 48,8% identificat en la nostra auditoria de 2019. Per tant, l'índex de maduresa actual continua sent insuficient per a garantir un grau de seguretat adequat 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

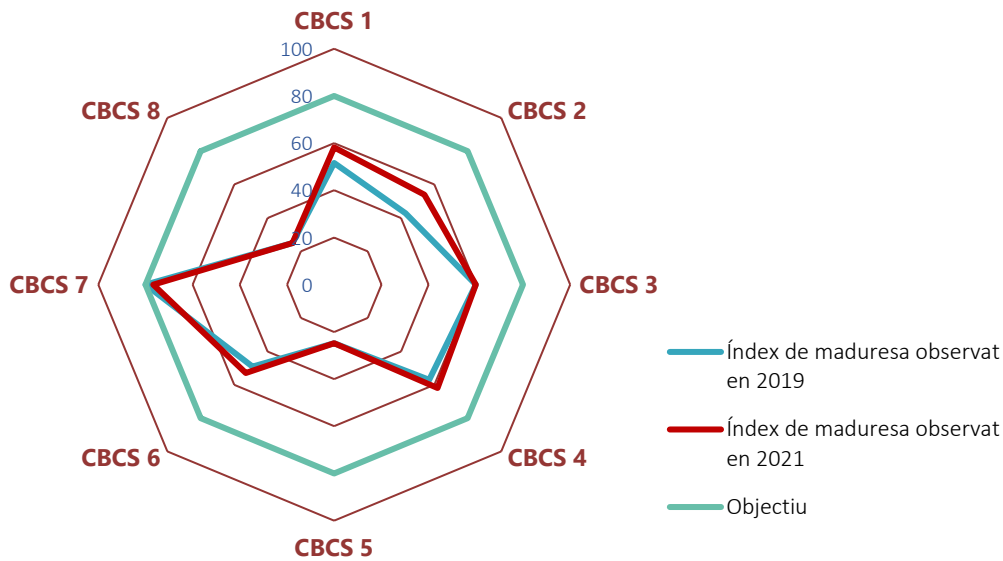
Control	2019			2021		
	Índex de maduresa	Nivell de maduresa	Índex de compliment	Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1 Inventari i control de dispositius físics	51,6%	N2	64,5%	58,2%	N2	72,8%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	42,8%	N1	53,5%	54,0%	N2	67,5%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	60,0%	N2	75,0%	60,0%	N2	75,0%
CBCS 4 Ús controlat de privilegis administratius	57,0%	N2	71,3%	61,9%	N2	77,4%
CBCS 5 Configuracions segures del programari i maquinari	24,8%	N1	30,9%	24,8%	N1	30,9%
CBCS 6 Registre de l'activitat dels usuaris	49,0%	N1	61,3%	53,0%	N2	66,3%
CBCS 7 Còpies de seguretat de dades i sistemes	80,0%	N3	100,0%	76,7%	N2	95,8%
CBCS 8 Compliment normatiu i governança de ciberseguretat	25,0%	N1	31,2%	25,0%	N1	31,2%
General	48,8%	N1	61,0%	51,7%	N2	64,6%

L'índex de compliment dels CBCS és del 64,6%, 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 61,0% del nostre informe anterior i la comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una lleu millora en quatre dels controls, una nul·la millora en tres CBCS i la regressió d'un. En conjunt, aquesta millora és insuficient atés el baix grau d'atenció a les nostres recomanacions (vegeu apartat 5 següent).

El nivell d'efectivitat en els controls analitzats continua sent 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 els controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 5 i CBCS 8). En l'apartat 5 es realitzen les recomanacions pertinents amb aquesta finalitat.

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

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



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

L'Ajuntament d'Alacant no té establida una governança adequada de la ciberseguretat, situació que ha de ser esmenada. A més, s'ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació

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

El compromís i conscienciació amb la ciberseguretat també s'ha d'estendre a la direcció² (tal com es defineix en el glossari al final d'aquest informe), que són els responsables d'articular i facilitar l'execució de les activitats establides per l'alta direcció en matèria de ciberseguretat.

D'altra banda, hem verificat que els gestors i responsables de la seguretat tenen una dedicació compartida entre múltiples competències i no disposen d'ocupació completa a la seguretat de la informació, de manera que aquesta dedicació resulta insuficient en un ens de la grandària i complexitat de l'Ajuntament d'Alacant. Aquesta mancança impedeix que el conjunt d'accions i mesures implantades puguin constituir-se com a processos

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



d'execució contínua i són percebudes com a accions puntuals, aïllades, la qual cosa dificulta l'establiment d'un sistema de gestió de la seguretat de la informació efectiu.

Aquests fets, al costat de les rellevants mancances identificades, com la falta d'activitat del comitè de seguretat de la informació, ens permet afirmar que l'Ajuntament d'Alacant no té establida una governança de la ciberseguretat adequada.

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

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

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

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

Per a esmenar les deficiències de control identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 4 anterior, reformulem les recomanacions que es van efectuar en l'auditoria de 2019, considerant si és el cas les millores realitzades des d'aquell moment. L'Ajuntament ha 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. Elaborar i aprovar formalment un procediment per a la gestió de l'inventari i el control de dispositius físics que reculli el procés complet, incloent-hi les revisions periòdiques de maquinari, actualitzant degudament l'inventari i incloent-hi les dates d'aquestes revisions.
2. Finalitzar la implantació de la solució adquirida per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

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

3. Aprovar formalment i implantar un procediment de gestió integral del programari de l'entitat, que ha d'incloure:



- Les directrius necessàries per a la creació i manteniment d'un inventari de programari complet i actualitzat.
 - Elaborar una llista de programari autoritzat en l'entitat i els procediments necessaris per a actualitzar-lo, incloent-hi les accions implantades actualment relacionades amb l'autorització i control de les instal·lacions.
 - Els controls actualment existents per a limitar la instal·lació i execució únicament al programari autoritzat.
 - La definició d'un pla de manteniment del programari que considere la totalitat del programari utilitzat a l'Ajuntament.
4. Revisar i actualitzar tots els sistemes que es troben fora del període de suport.

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

5. Formalitzar el procés implantat actualment de detecció de vulnerabilitats i ampliar-ne l'abast de manera que cobreixi el cicle complet de gestió contínua de vulnerabilitats: identificació i solució de vulnerabilitats per mitjà de les eines desplegades, 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, prioritats, responsables, solució, etc.

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

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

6. Finalitzar i aprovar formalment el procediment en elaboració per a gestió d'usuaris amb privilegis d'administració, en el marc de desenvolupament del nou SGSI, de manera que establisca les directrius per a tots els sistemes de l'entitat i que incloga:
- L'eliminació de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió han de realitzar-se amb usuaris nominatius.
 - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.
 - La política d'autenticació que cal aplicar a aquest tipus de comptes.



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

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

Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de 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.

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

8. Finalitzar i aprovar formalment la normativa en elaboració per a auditoria i registre d'esdeveniments dels sistemes de manera 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, tal com es realitza per a determinats sistemes crítics.

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

9. Finalitzar i aprovar formalment el procediment en elaboració per a la gestió de còpies de seguretat, de manera que represente amb fidelitat el conjunt de mesures ja implantades per a la gestió de còpies de seguretat de dades i sistemes i que detalle addicionalment 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)

10. Implantar les mesures necessàries per a donar compliment a les disposicions del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de:
 - Realitzar la designació de les persones per als rols definits en la política de seguretat i la constitució i funcionament efectiu del Comitè de Seguretat de la Informació.
 - Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriuen.
 - Realitzar les auditories de compliment previstes en l'article 34 del Reial Decret 3/2010.



- Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.
11. En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que estableix l'RGPD i la Llei Orgànica 3/2018. En particular ha de:
- 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 als articles 32.2 i 35 de l'RGPD.
 - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.
 - Planificar i executar auditories en matèria de protecció de dades.
12. Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.

Priorització de les recomanacions

A fi que es puguem establir accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial que cal mitigar i cost estimat de la implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2019, adaptant la relació risc/cost de cada recomanació i considerant les millores realitzades des de la revisió anterior. No s'hi inclouen els punts 10 a 12 anteriors, ja que són mesures de compliment obligat.

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





Actuacions en curs

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

Enumerem a continuació les actuacions que es troben en execució i que per la seua rellevància s'han de destacar en l'Informe:

- Actualment existeix un procés selectiu per a la incorporació de cinc noves places de personal tècnic en informàtica de l'Ajuntament. Aquestes incorporacions milloraran les capacitats del servei d'informàtica i s'ha previst la finalització del procés selectiu durant l'any 2022.
- L'entitat disposa d'una eina d'escaneig actiu de vulnerabilitats, que té previst explotar i gestionar de manera activa per mitjà de les noves incorporacions de personal que s'han esmentat.
- En 2022 s'han projectat diferents accions relacionades amb l'adequació a l'ENS que estaven pendents d'implementar en el moment de la revisió:
 - Aprovació i publicitat de la nova política de seguretat de la informació.
 - Constitució del Comité Municipal de Seguretat de la Informació i assignació de responsabilitats. La nova política de seguretat de la informació defineix la seua composició, funcions, responsabilitats i règim de funcionament.
 - Revisió i aprovació de la normativa i procediments de seguretat.
- S'han projectat l'any 2022 diferents accions relacionades amb actuacions tecnològiques i de ciberseguretat que es troben en diferents graus d'execució:
 - Adhesió de l'Ajuntament d'Alacant al Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana. Finançament a càrrec dels fons europeus Next Generation articulats per mitjà del Pla de Recuperació, Transformació i Resiliència.
 - Construcció d'un nou CPD i renovació tecnològica, incloent-hi la renovació d'electrònica de xarxa i dels sistemes d'emmagatzematge, virtualització i servidors de base de dades.
 - Actuacions de sistemes relacionats amb la seguretat, incloent-hi el desplegament complet del sistema NAC i eines de monitoratge i centralització de logs.



- S'ha iniciat una reorganització dels recursos humans relacionats amb la seguretat de la informació. S'ha realitzat la provisió del lloc de cap del Departament de Desenvolupament de Seguretat Tecnològica.

Seguiment de recomanacions anteriors

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

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



Quadre 2. Seguiment de recomanacions

Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>1</p> <p>Integrar en l'actual sistema d'inventari una eina de descobriment automàtic d'elements, en cas de viabilitat tècnica.</p> <p>Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.</p>	<p>L'entitat disposa d'una normativa aprovada que recull parcialment el procés d'inventariat, no obstant això, aquesta normativa ha quedat desactualitzada.</p> <p>S'ha implantat una eina de protecció d'<i>endpoint</i> que realitza el descobriment i inventari automàtic de determinats elements de maquinari, incloent-hi equips d'usuari i servidors.</p> <p>S'ha instal·lat una eina específica per al control dels dispositius físics de xarxa.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>2</p> <p>Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.</p>	<p>Es troba en fase d'implantació un sistema NAC (<i>network access control</i>) desplegat totalment per al control de dispositius sense fils i en fase de proves en els altres dispositius corporatius.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>3</p> <p>Aprovar formalment i implantar un procediment de gestió integral del programari de l'entitat, que ha d'incloure:</p> <ul style="list-style-type: none"> - L'inventari de programari. S'han d'establir les directrius necessàries per a la creació i manteniment d'un inventari de programari complet i actualitzat. Per a implantar-lo s'aconsella l'ús d'eines que permeten automatitzar aquest procés. - Llista de programari autoritzat en l'entitat i els procediments necessaris per a actualitzar-lo, incloent-hi les accions implantades actualment relacionades amb l'autorització i control de les instal·lacions: - La definició d'un pla de manteniment del programari que considere la totalitat del programari utilitzat, incloent-hi tant el gestionat per mitjà de licitacions i clàusules contractuals com la resta de programari utilitzat a l'Ajuntament. 	<p>S'ha implantat una eina de protecció d'<i>endpoint</i> que realitza l'inventari automàtic del programari instal·lat en els equips gestionats, servidors i ordinadors personals amb sistema operatiu Windows. A més, l'eina bloqueja el programari no conegut pel fabricant i permet instal·lar, desinstal·lar i actualitzar programari de manera programada.</p> <p>S'apliquen de manera puntual polítiques per a limitar l'execució de programes, tant en el directori actiu com per mitjà de regles del tallafoc.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<ul style="list-style-type: none"> - Controls a implantar per a limitar la instal·lació i execució solament al programari autoritzat. 			
<p>4 Revisar i actualitzar tots els sistemes que es troben fora del període de suport.</p>	Sense variació.	No aplicada	Es manté la redacció.
<p>5 Formalitzar el procés implantat actualment de detecció de vulnerabilitats i ampliar-ne l'abast de manera que cobrisca el cicle complet de gestió contínua de vulnerabilitats: identificació i solució de vulnerabilitats, incloent-hi l'anàlisi prèvia a l'entrada en producció dels sistemes, la prioritització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats, identificant dates, prioritat, responsable, solució, etc.</p> <p>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.</p>	<p>L'Ajuntament ha iniciat determinats canvis, particularment tecnològics, però aquests no són significatius respecte a la gestió de vulnerabilitats que es realitzava en la revisió anterior.</p> <p>L'Ajuntament ha desplegat l'eina microCLAUDIA del CCN als equips i sistemes per a protecció contra codi nociu de tipus <i>ransomware</i>, però aquest fet no es considera en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021.</p> <p>S'ha instal·lat una eina per a l'escaneig de vulnerabilitats en els sistemes, però aquesta eina no s'explota per falta de personal encarregat de la seua aplicació.</p>	No aplicada	S'actualitza la redacció feta en 2019.
<p>6 Formalitzar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga:</p> <ul style="list-style-type: none"> - L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió hauran de realitzar-se amb usuaris nominatius. - La política d'autenticació a aplicar a aquesta mena de comptes. - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes. 	<p>S'han eliminat els usuaris administradors per defecte de determinats sistemes crítics de la corporació.</p> <p>S'ha implantat autenticació per mitjà de certificat digital per a l'accés a la VPN dels usuaris en la modalitat de teletreball.</p> <p>S'ha implantat l'autenticació de doble factor per a l'accés a determinats sistemes des de l'exterior de la xarxa corporativa.</p>	Aplicada parcialment	S'actualitza la redacció feta en 2019.



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>7 Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN.</p> <p>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, bé per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració.</p>	<p>Sense variació.</p>	<p>No aplicada</p>	<p>Es manté la redacció.</p>
<p>8 Aprovar formalment un procediment per al tractament de <i>logs</i> d'auditoria de l'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels <i>logs</i>. Per a la revisió de <i>logs</i> és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.</p>	<p>S'ha implantat una eina per a la gestió dels <i>logs</i> en el projecte "Alacant es mou" en col·laboració amb Red.es.</p> <p>L'Ajuntament centralitza els <i>logs</i> de l'electrònica de xarxa en una eina específica, però no realitza una revisió de <i>logs</i> d'auditoria de manera sistemàtica.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>9 Realitzar proves periòdiques de recuperació, regides mitjançant un procediment que siga adequadament aprovat o bé incloent aquestes proves en la política de gestió de còpies de seguretat existent. Aquest procediment ha de definir, com a mínim, periodicitat de les proves, abast i personal necessari.</p>	<p>L'entitat disposa d'una normativa aprovada que recull parcialment el procés de realització de còpies de seguretat, no obstant això, aquesta normativa ha quedat desactualitzada i no representa la realitat del control.</p> <p>S'ha implantat una nova eina per a la gestió de còpies de seguretat. S'ha inclòs en aquesta gestió la realització de còpies del correu electrònic i les dades de les aplicacions ofimàtiques.</p>	<p>No aplicada</p>	<p>S'actualitza la redacció feta en 2019.</p>



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de:</p> <ul style="list-style-type: none"> - Realitzar la designació de les persones per als rols definits en la política de seguretat i constitució dels òrgans que s'hi descriuen. <p>10 - Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriuen.</p> <ul style="list-style-type: none"> - Realitzar les auditories de compliment previstes en l'article 34 del Reial Decret 3/2010. - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS de 13 d'octubre de 2016 	<p>S'ha desenvolupat una nova política de seguretat i un marc normatiu i procedimental, però es troben pendents d'aprovació.</p>	<p>No aplicada</p>	<p>Es matisa la redacció del primer guió de la recomanació.</p>
<p>En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i en la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de:</p> <ul style="list-style-type: none"> - Nomenar un DPD d'acord amb el que es preveu en l'article 37.1.a de l'RGPD. <p>11 - 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.</p> <ul style="list-style-type: none"> - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD. - Planificar i executar auditories en matèria de protecció de dades. 	<p>Sense variació en 2021.</p> <p>S'ha realitzat la designació del DPD al maig de 2022.</p> <p>Encara que aquest fet no és considerat en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021, sí que ho tenim en compte per a actualitzar la nostra recomanació.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>12 Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.</p>	<p>Sense variació.</p>	<p>No aplicada</p>	<p>Es manté la redacció.</p>



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 de què són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials –i en molts casos, reals– tant econòmiques com en la prestació dels serveis públics.

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

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

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

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 INES³ 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 romanguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan implementades correctament.

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

³ 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'Alacant, exercici 2019, i obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això n'hem avaluat tant el disseny⁴ com l'eficàcia operativa⁵ per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport. També hem revisat el compliment de la normativa bàsica relativa a la seguretat de la informació.

Així mateix hem formulat recomanacions que contribuïsquen a esmenar les deficiències observades i a millorar els procediments de control, tenint en consideració les millores introduïdes des de la nostra auditoria anterior.

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

Abast

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

- CBCS 1 Inventari i control de dispositius físics
- CBCS 2 Inventari i control de programari autoritzat i no autoritzat
- CBCS 3 Procés continu d'identificació i solució de vulnerabilitats
- CBCS 4 Ús controlat de privilegis administratius
- CBCS 5 Configuracions segures del programari i maquinari
- CBCS 6 Registre de l'activitat dels usuaris
- CBCS 7 Còpies de seguretat de dades i sistemes
- CBCS 8 Compliment normatiu i governança de ciberseguretat

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

⁴ L'avaluació del disseny d'un control implica la consideració per l'auditor de si el control, de manera individual o en combinació amb altres controls, és capaç de previndre de manera eficaç, o de detectar i corregir, la materialització dels riscos previstos. És a dir, és capaç de complir l'objectiu de control.

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



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

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

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

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls a 31 de desembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe, ja que fins a aquell moment s'ha admés qualsevol evidència disponible. Per tant, amb caràcter general l'Informe reflecteix la situació en aquell moment, ja que és freqüent que, des que s'inicia el treball de camp, determinades deficiències observades i assenyalades als gestors siguin esmenades i són considerades d'aquesta manera en les conclusions i en els indicadors.

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

Metodologia

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

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

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



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

La guia pràctica de fiscalització dels OCEX 5313

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

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS. No obstant això, atesa l'amplitud de l'ENS, que està format per 75 mesures de seguretat, per a la seua inclusió en els CBCS es va seleccionar una sèrie limitada de controls. Per a triar els més rellevants es va atendre el marc conceptual establert per la prestigiosa organització Center for Internet Security (CIS),⁶ que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. L'avantatge principal 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 establerts en l'ENS i en l'RGPD.

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

Atés que l'ENS és de compliment obligat per a tots els ens públics, s'ha tingut especial cura que la metodologia d'auditoria dels controls bàsics de ciberseguretat estiguera plenament alineada amb l'ENS. Aquesta alineació facilita 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 referències de l'ENS següents:

⁶ Center for Internet Security, <www.cisecurity.org>.



Quadre 3. Els CBCS i l'ENS

Control	Mesura de seguretat de l'ENS*
CBCS 1 Inventari i control de dispositius físics	op.exp.1
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	op.exp.1 op.exp.2
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	mp.sw.2 op.exp.4
CBCS 4 Ús controlat de privilegis administratius	op.acc.4 op.acc.5
CBCS 5 Configuracions segures del programari i maquinari	op.exp.2 op.exp.3
CBCS 6 Registre de l'activitat dels usuaris	op.exp.8 op.exp.10
CBCS 7 Còpies de seguretat de dades i sistemes	mp.info.9
CBCS 8 Compliment 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) assenyala⁷ que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen" i reduir els ciberriscos.⁸

Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.⁹

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

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

⁸ Segons experts citats en l'informe [DOD Needs to Take Decisive Actions to Improve Cyber Hygiene](#) de la US Government Accountability Office (2020), fins al 90% dels ciberatacs podrien evitar-se implantant mesures de ciberhigiene adequades.

⁹ Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices*, 2017.



Quadre 4. Punts d'acció d'ENISA

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

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

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

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

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



Quadre 5. Els CBCS i els seus subcontrols

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



Control	Objectiu del control	Subcontrol	
CBCS 5 Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors	Establir, implantar i gestionar la configuració de seguretat, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de previndre atacs a través de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6 Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels logs d'auditoria)	Recollir, gestionar i analitzar logs d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de logs d'auditoria	El log d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
		CBCS 6-2: Emmagatzematge de logs: retenció i protecció	Els logs es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de logs	Els logs de tots els sistemes són revisats periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels logs d'auditoria, de manera que se'n facilite la revisió.
		CBCS 6-4: Monitoratge i correlació	L'entitat disposa d'un SIEM (<i>security information and event management</i>) o una eina d'anàlisi 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 es mostra en el quadre següent:

Quadre 6. Avaluació dels subcontrols

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

Controls

Per a determinar la situació global de cada control de ciberseguretat hem utilitzat el **model de nivell de maduresa** dels processos de control d'acord amb el que s'estableix en la GPF-



OCEX 5313, que al seu torn està basada en la *Guia de seguretat CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 7. Nivells de maduresa

Nivell	Índex	Descripció
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. <i>L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depèn de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depèn de tindre personal d'alta qualitat.</i>
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. <i>L'eficàcia del procés depèn de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredecible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.</i>
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. <i>Es disposa d'un catàleg de processos que es manté actualitzat. Aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant dels incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor d'allò desconegut (o no planificat).</i> <i>L'èxit és més que bona sort: es mereix.</i> <i>Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2 i que sí que es gestiona en el nivell 3.</i>
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. <i>Es disposa d'un sistema de mesures i mètriques per a conèixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.</i> <i>En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.</i>
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. <i>El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.</i> <i>S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, utilitzant-se com a indicadors en la gestió de la millora dels processos.</i> <i>En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes a base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.</i>



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

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

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

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

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

- a) Aconseguir els seus objectius.
- b) Protegir els actius al seu càrrec.
- c) Complir les seues obligacions diàries de servei.
- d) Respectar la legalitat vigent.
- e) Respectar els drets de les persones.

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

Confidencialitat	És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.
Integritat	És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, assegurant que no se n'ha produït l'alteració, pèrdua o destrucció, ja siga de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.
Disponibilitat	Es tracta de la capacitat d'un servei, un sistema o una informació de ser accessible i utilitzable pels usuaris o processos autoritzats quan aquests ho requerisquen.



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

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

Una informació o un servei es poden veure afectats en una o més de les seues dimensions de seguretat. Cada dimensió de seguretat afectada s'adscriurà a un dels nivells següents: BAIX, MITJÀ o ALT.

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

- a) Un sistema d'informació serà de categoria ALTA si alguna de les seues dimensions de seguretat aconseguix el nivell ALT.
- b) Un sistema d'informació serà de categoria MITJANA si alguna de les seues dimensions de seguretat aconseguix el nivell MITJÀ, i cap aconseguix un nivell superior.
- c) Un sistema d'informació serà de categoria BÀSICA si alguna de les seues dimensions de seguretat aconseguix el nivell BAIX, i cap aconseguix un nivell superior.

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

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:¹⁰

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

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

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

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



Indicadors globals

A l'efecte de l'ENS, la guia CCN-STIC-824 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 aconseguït per un organisme respecte del conjunt de controls de ciberseguretat.
- L'**índex de compliment** analitza igualment el nivell de maduresa aconseguït, però en relació amb l'exigència aplicable en cada cas, tenint en compte la categoria del sistema. És a dir, compara l'índex de maduresa amb el nivell mínim exigít per a aquesta categoria en l'ENS, que en aquesta auditoria és N3 (80%) per a tots els casos.

Governança de ciberseguretat

A l'efecte d'aquest treball, s'entén per governança de la seguretat de la informació i les comunicacions o de ciberseguretat (termes que utilitzem de manera indistinta en aquest informe) el conjunt de responsabilitats i activitats realitzades per l'alta direcció amb l'objectiu de proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconsegueixen els objectius, verificar que el risc es gestiona adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una forma responsable.¹¹

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

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

És més que una mera qüestió tècnica, per la qual cosa **exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització.**¹²

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

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

¹² Vegeu l'apartat 66 d'[Anàlisis núm. 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE](#) del Tribunal de Comptes Europeu.



La implicació dels òrgans superiors és, potser, el factor més important per a la implantació amb èxit d'un sistema de gestió de la seguretat de la informació o de ciberseguretat.¹³ L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació,¹⁴ que ha de materialitzar-se en aspectes com ara:

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

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

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

La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,¹⁵ que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat, i és la màxima autoritat en l'organització respecte a les decisions de seguretat que afecten els sistemes que manegen informació o presten algun servei. La seua composició ha de constar en la PSI.

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

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

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

¹³ [Guía de iniciación a actividad profesional. Implantación de sistemas de gestión de la seguridad de la información \(SGSI\) según la norma ISO 27001](#), Col·legi Oficial d'Enginyers de Telecomunicació.

¹⁴ [UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información](#), apartat 3.4.

¹⁵ [Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC](#), CCN, gener de 2021.



Seguiment de les recomanacions

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

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

Quadre 8. Situació de les recomanacions

Totalment o substancialment aplicada	Si l'ens fiscalitzat ha adoptat les mesures correctores, raonables i proporcionades en l'esfera de les seues competències, que permeten considerar que la recomanació ha produït 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 complert 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 complert 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 puguin adoptar les mesures correctores que consideren necessàries. En aquest informe els resultats es mostren de manera sintètica.



APÈNDIX 2

Situació dels controls bàsics de ciberseguretat



CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

Hem verificat que l'Ajuntament ha implantat determinades millores per a l'inventari i el control de dispositius físics. L'entitat disposa d'una normativa aprovada que recull parcialment el procés d'inventari. No obstant això, aquesta normativa ha quedat desactualitzada, no representa la realitat del control i serà substituïda per un procediment que es troba en elaboració.

L'Ajuntament manté l'ús d'una aplicació pròpia per a l'inventari i el control de dispositius físics que no s'ha modificat des de l'auditoria anterior. Addicionalment, l'Ajuntament ha implantat una eina de protecció d'*endpoint* que realitza el descobriment i inventariat automàtic d'elements de maquinari, equips d'usuari i servidors, que cobreix tot el parc instal·lat en la xarxa corporativa amb sistema operatiu Windows. Els sistemes Linux no disposen d'agent de descobriment automàtic, de manera que aquests equips no són recollits per l'eina.

Si bé no s'ha implantat un procés de revisió periòdica, quan l'eina de descobriment automàtic detecta un canvi de maquinari (modificació o baixa), aquest canvi és reportat, revisat i reflectit en l'aplicació manual pròpia.

Per a l'electrònica de xarxa, que s'ha renovat recentment, l'Ajuntament disposa d'un sistema propietari del fabricant que permet la gestió i inventari dels equips.

Encara que l'Ajuntament disposa de diferents inventaris que, de manera conjunta, formen l'inventari complet del maquinari de l'entitat, aquest control no és efectiu en totes les circumstàncies, ja que continua sense disposar-se d'un procediment que regule les baixes d'equips i, en conseqüència, hi ha equips retirats que continuen apareixent en l'inventari.

L'eina per a l'inventari i gestió de la xarxa inclou funcionalitats NAC (*network access control*) que limiten l'accés d'equips no autoritzats. Aquesta funcionalitat està totalment desplegada per al control dels equips sense fils i en fase de proves pilot per a la connexió cablejada dels dispositius corporatius d'empleats municipals i per a l'accés a internet de ciutadans des de les instal·lacions municipals.

Hi ha cert nivell de control sobre l'inventari i el control d'actius físics, i la valoració global aconsegueix un **índex de maduresa del 58,2%**, que es correspon amb un **nivell N2 de maduresa, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establerts o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 1 del 72,8%**.



La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 51,6%. Per tant, s'ha produït una millora de 6,6 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 pugui 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 fet canvis que milloren la gestió de programari autoritzat que observem en l'auditoria anterior.

L'Ajuntament ha desplegat, tant en servidors com en equips d'usuaris, una eina de protecció d'*endpoint* que realitza l'inventari automàtic del programari instal·lat en els equips gestionats amb sistema operatiu Windows. A més, l'eina permet instal·lar, desinstal·lar i actualitzar programari de manera programada.

L'entitat disposa d'una normativa aprovada, "Normes generals d'utilització dels recursos i sistemes d'informació de l'Ajuntament d'Alacant", que, si bé es troba pendent d'actualització en el marc de desenvolupament del nou SGSI, prohibeix la instal·lació de programari no autoritzat.

S'han implantat mesures puntuals per al bloqueig de programari específic no autoritzat per mitjà de polítiques en el directori actiu i a través de l'aplicació de regles concretes en el tallafoc. A més, l'eina de protecció d'*endpoint* bloqueja el programari que potencialment tinga alguna vulnerabilitat o siguen aplicacions no conegudes pel fabricant.

Respecte al manteniment i suport del fabricant del programari desplegat, no s'han realitzat millores en aquest període. Hi ha un procés efectiu per a l'actualització periòdica i manteniment de determinats sistemes crítics de l'entitat, però no s'han actualitzat tots els sistemes que es trobaven fora del període de suport en l'auditoria anterior.

Hi ha cert nivell de control sobre l'inventari i control de programari autoritzat, que aconsegueix un **índex de maduresa del 54,0%**, 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 67,5%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 42,8%, que es correspon amb un nivell de maduresa N1, *inicial/ad hoc*. Per tant, s'ha produït una millora d'11,2 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 iniciat determinats canvis tecnològics, però aquests no són significatius respecte a la gestió de vulnerabilitats que es realitzava en la revisió anterior o no se n'ha finalitzat l'aplicació.

Els responsables del sistema continuen subscrits a les llistes de correu de comunicació i seguiment de vulnerabilitats que realitza el CCN-CERT i INCIBE per a l'anàlisi, notificació i seguiment d'aquelles vulnerabilitats més crítiques i que impacten en les tecnologies que utilitzen. Aquestes incidències són registrades en un gestor de tasques propi per a fer-ne el seguiment i resolució, tal com es va verificar en la revisió anterior.

L'entitat està iniciant el desplegament de l'eina microCLAUDIA del CCN en tots els sistemes i equips, eina que proporciona protecció contra codi nociu de tipus *ransomware*. En el moment de la revisió aquesta mesura es troba en una fase inicial del desplegament sobre el parc informàtic de l'Ajuntament.

L'Ajuntament utilitza una eina per a la gestió centralitzada de pedaços de seguretat i actualitzacions en equips d'usuari i servidors.

L'entitat ha desplegat una eina per a l'escaneig de vulnerabilitats en tots els sistemes de l'Ajuntament. Aquesta eina escaneja els sistemes i mostra en una consola el seu estat global. Les operacions d'escaneig es realitzen per mitjà d'una tasca programada i automàtica o a través d'un escaneig dirigit a una màquina sospitosa concreta. No obstant això, aquest sistema no s'explota en l'actualitat a causa de la falta de recursos de personal per a configurar-lo i implantar-lo.

Hi ha un cert nivell de control sobre la gestió de vulnerabilitats, de manera que la valoració global del control aconsegueix un **índex de maduresa del 60,0%**, 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 3 del 75,0%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 60,0%. Per tant, no s'ha produït cap progrés, ja que les millores previstes no han entrat en funcionament.



CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

L'Ajuntament ha implantat algunes millores per a l'inventari i el control dels comptes d'usuaris administradors.

Les accions de l'Ajuntament formen part d'un procés parcialment definit en les "Normes generals d'utilització dels recursos i sistemes d'informació de l'Ajuntament d'Alacant". No obstant això, aquesta normativa no es troba implantada de manera general per a tots els sistemes de l'entitat, ha quedat desactualitzada i serà substituïda per un SGSI que es troba en elaboració.

Hem verificat que s'han eliminat els usuaris administradors per defecte de determinats sistemes crítics de la corporació. A més, s'han millorat els mecanismes d'autenticació per a l'accés a sistemes crítics, com els accessos per VPN per mitjà de certificats digitals dels usuaris en la modalitat de teletreball com a resultat del confinament per COVID-19, o l'ús de doble factor d'autenticació per a l'accés a determinats sistemes des de l'exterior de la xarxa corporativa.

Hi ha un cert nivell de control sobre els comptes amb privilegis administratius. La valoració global del control aconsegueix un **índex de maduresa del 61,9%**, 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 d'aquest CBCS 4 del 77,4%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 57,0%, que es correspon amb un nivell de maduresa N2. Per tant, s'ha produït una millora de 4,9 punts en l'índex de maduresa del control.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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



Situació del control

L'Ajuntament ha realitzat determinats canvis en el control, però aquests no són significatius respecte a la configuració segura dels sistemes que vam observar en la revisió anterior.

Hem analitzat les accions realitzades a l'Ajuntament per al control de configuracions segures dels equips i aplicacions i hem verificat que, encara que es realitzen accions que impliquen l'aplicació d'una configuració de seguretat en els sistemes, aquesta és insuficient i no existeix un procediment formalment aprovat a aquest efecte.

La valoració global del control existent sobre les configuracions segures és que l'organització aconsegueix un **índex de maduresa del 24,8%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està organitzada correctament. Això representa un **índex de compliment del CBCS 5 del 30,9%**.

La situació del control no ha variat respecte de l'informe realitzat l'any 2019.

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 els procediments aplicats a l'Ajuntament per al control de l'activitat dels usuaris en els sistemes i hem verificat que hi ha controls en funcionament relacionats amb aquestes activitats que s'apliquen de manera informal i no existeix un procediment aprovat a aquest efecte. No obstant això, sí que s'ha desenvolupat una normativa d'auditoria i registre d'esdeveniments dels sistemes que es troba pendent d'aprovació.

S'ha implantat una eina per a la gestió dels *logs* d'auditoria en el projecte "Alacant es mou" en col·laboració amb Red.es. en una xarxa segmentada de la general de l'Ajuntament.

L'Ajuntament té centralitzats els *logs* de l'electrònica de xarxa en una eina específica, però no realitza una revisió de *logs* d'auditoria de manera sistemàtica, sinó que aquesta es limita a casos en què existeix una necessitat concreta.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 53,0%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 6 del 66,3%**.



La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 49,0%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 4 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 la recuperació de la informació en temps oportú.

Situació del control

Hem analitzat les accions de l'Ajuntament per a la realització de còpies de seguretat de dades i sistemes i hem observat que formen part d'un procés que es troba correctament definit i executat. Aquest procés es troba formalment recollit en les "Normes generals d'utilització dels recursos i sistemes d'informació de l'Ajuntament d'Alacant". No obstant això, aquesta normativa ha quedat desactualitzada, no representa la realitat del control i serà substituïda per un procediment que es troba en elaboració. Aquesta desactualització limita la maduresa del control, atés que el procés ja no es troba correctament formalitzat, circumstància que ha perjudicat lleugerament la valoració de l'índex de maduresa.

L'Ajuntament ha implantat una nova eina per a la gestió de còpies de seguretat. S'ha inclòs en aquesta gestió la realització de còpies del correu electrònic i les dades de les aplicacions ofimàtiques. L'emmagatzematge de les còpies de les dades ofimàtiques es realitza per mitjà dels serveis d'un proveïdor *cloud*.

L'Ajuntament no realitza proves de recuperació planificades de les còpies de seguretat realitzades, destinades a garantir les capacitats de recuperació d'aquesta informació en cas de necessitat.

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 2019 mostrava un índex de maduresa del 80,0%, que es correspon amb un nivell de maduresa *N3, procés definit*. Per tant, s'ha produït un empitjorament de 3,3 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 2019, l'Ajuntament no ha realitzat accions que hagen millorat el nivell de compliment exigít 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.

L'any 2019 es va adjudicar un projecte d'assistència tècnica per a donar compliment a l'Esquema Nacional de Seguretat, Reglament General de Protecció de Dades (RGPD) i Esquema Nacional d'Interoperabilitat. Aquest projecte va permetre el desenvolupament d'una nova política de seguretat i un marc normatiu i procedimental, que es troben pendents d'aprovació. Aquest projecte no es troba en execució en l'actualitat per falta de mitjans humans per a dur-lo a terme.

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

Compliment de l'RGPD

Quant al compliment en matèria de protecció de dades personals, des de la revisió realitzada l'any 2019, l'Ajuntament ha realitzat la designació del DPD al maig de 2022.

Encara que aquest fet no és considerat en el càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021, sí que el tenim en compte per a actualitzar la nostra recomanació per considerar-se complida en aquest punt.

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió no es modifica respecte a l'informe emés l'any 2019 i l'Ajuntament aconsegueix un **índex de maduresa del 25,0%**, que es correspon amb un **nivell de maduresa N1**, que indica que hi ha incompliments significatius generalitzats de la normativa i hi ha aspectes que s'han de millorar.

Governança de ciberseguretat

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



Si bé en l'auditoria hem observat l'existència d'un cert nivell de compromís i conscienciació amb la ciberseguretat per part dels gestors i responsables de les àrees implicades, hi ha mancances rellevants que indiquen que la governança és deficient i que hi ha un insuficient nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament i de la direcció. Les mancances més rellevants identificades, que impedeixen l'establiment d'un sistema de gestió de la seguretat de la informació (SGSI) efectiu, són les següents:

- L'existència d'un marc normatiu, incloent-hi la política de seguretat de la informació (PSI), i procedimental formalment aprovat però desactualitzat, que no representa la realitat de la institució.
- La falta d'activitat del Comité de Seguretat, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat i que ha d'incloure representació de les àrees de l'organització afectades.
- La falta d'activitat dels rols clau en l'organització, com el responsable de seguretat, a causa de l'acumulació de competències no directament relacionades amb la seguretat de la informació que impedeixen el seu desenvolupament efectiu. A més, els nomenaments i responsabilitats han quedat desactualitzats.
- La inexistència d'una cultura de seguretat en l'organització i de conscienciació respecte a la responsabilitat sobre aquesta per part de la direcció i l'alta direcció que siga clarament identificable per tot el personal.

No obstant això, s'han identificat alguns aspectes positius de cara al futur atés que s'han iniciat projectes per a donar compliment als requisits de l'Esquema Nacional de Seguretat. Aquestes accions han proporcionat com a resultat l'elaboració d'una política de seguretat actualitzada i un nou marc normatiu i procedimental, que es troben pendents d'aprovació. No obstant això, aquests projectes i iniciatives no tenen la deguda continuïtat per falta de recursos humans suficients fins a la data de finalització del treball de camp, circumstància que l'Ajuntament espera esmenar amb la cobertura de diversos llocs tècnics que s'estava realitzant en el moment de redactar aquest informe, tal com s'ha assenyalat en l'apartat "Actuacions en curs" de l'epígraf 5.

Resulta, per tant, necessària la solució urgent de les mancances identificades, que tenen un impacte negatiu en el nivell de seguretat de la corporació. En aquest sentit, els òrgans de govern tenen la responsabilitat de liderar i ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat. I la direcció és responsable de l'execució de les activitats establides en matèria de ciberseguretat.



APÈNDIX 3

Bones pratiques 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.

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

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

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

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

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

Desenvolupament i explotació de l'eina de ticketing i gestió de fluxos de treball en determinats processos de l'entitat

L'entitat ha desenvolupat i desplegat una eina d'inventari d'actius, *ticketing* i gestió de fluxos de treball que s'ha integrat amb determinats sistemes i processos interns d'una manera particularment efectiva.



La funcionalitat més rellevant de l'eina, des del punt de vista de la seguretat, és 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 revisió de pedaços i actualitzacions de determinats sistemes crítics.
- El seguiment d'altres i baixes d'empleats, gestió dels seus comptes d'usuari i equipament informàtic, coordinat automàticament amb recursos humans per mitjà de l'aplicació.
- La revisió periòdica de comptes d'usuaris i privilegis en determinats sistemes crítics.



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, el secretari general, l'interventor general, 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 en consonància amb els objectius de l'organització. Als efectes d'aquest informe li donem el mateix significat que a *governança de la seguretat de la informació*.

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i descriuen: a) l'ús correcte d'equips, serveis i instal·lacions; b) el que es considerarà ús indegut, i c) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conèixer-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 de Modernització i Noves Tecnologies i amb els responsables del Servei de Noves Tecnologies, Innovació i Informàtica, 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, 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 20 de juliol de 2022, va aprovar aquest informe d'auditoria.



Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Informe seguiment recomanacions cbcs Ajuntament Alacant en 2019 - SEFYCU 3409615

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



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

Codi Segur de Verificació (CSV): KUAA XDVF ZDFC HYCX QNNZ

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

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

Empremta del
document per a la
persona firmant

Text de la firma

Dades addicionals de la firma



Vicent Cucarella Tormo
Síndic Major

Firma electrònica - ACCV - 26/07/22 08:21
VICENT CUCARELLA TORMO