SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SEGUIMENT DE LES RECOMANACIONS REALITZADES EN L'INFORME D'AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DE L'AJUNTAMENT DE VILA-REAL DE L'ANY 2020

Situació a 31 de desembre de 2021

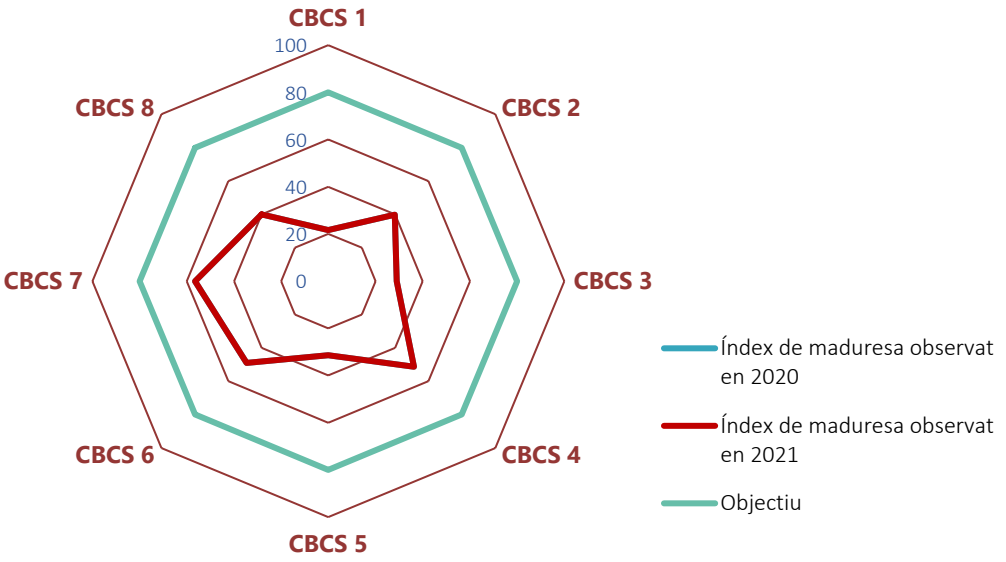
RESUM

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

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

Conclusions

No s'ha realitzat cap progrés per a millorar la ciberseguretat des de la nostra auditoria anterior i no s'ha atés cap de les nostres recomanacions per a això. Per tant, l'índex de maduresa general dels controls bàsics de ciberseguretat, l'objectiu dels quals seria aconseguir un 80%, mostra el mateix valor del 39,8% assenyalat en l'auditoria de l'any 2020, per la qual cosa el nivell d'efectivitat en els controls analitzats continua sent molt deficient i reflecteix un nivell de risc inacceptable per a una entitat pública de la importància de l'Ajuntament de Vila-real. L'entitat ha d'adoptar mesures urgents per a reconduir la situació i 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.



L'Ajuntament de Vila-real no té establida una estructura de governança de la ciberseguretat, tal com exigeix la normativa, i un sistema adequat de control intern. Aquesta situació ha de ser promptament esmenada i els òrgans superiors de l'Ajuntament, com a

responsables del sistema de control, han de reforçar de manera decidida el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

Així mateix, la nostra revisió també ha posat de manifest un grau de compliment insuficient quant a l'adequació a les normes legals relacionades amb la seguretat de la informació. L'informe assenyala diversos aspectes sobre els quals s'ha d'actuar per a esmenar-los ràpidament. Respecte de 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 els òrgans que s'hi descriuen.

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 implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa, identificar i actualitzar tots els sistemes que es troben fora del període de suport, situar les còpies de seguretat secundàries en un local correctament condicionat i finalitzar i formalitzar un procediment unificat per a la 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 conéixer el veritable abast del treball realitzat.

Informe de seguiment de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Vila-real de l'any 2020

Situació a 31 de desembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

L'article 6 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, inclou entre les seues funcions, a més de les referides al control extern de la gestió economicofinancera del sector públic valencià i dels seus comptes, 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 9 de juliol de 2020 el Consell de la Sindicatura de Comptes va aprovar l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Vila-real, Exercici 2020. Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 fer un treball de seguiment de la situació dels controls bàsics de ciberseguretat d'aquest ajuntament i dels altres 14 ajuntaments analitzats.

La necessitat d'una ciberhigiene adequada

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

En aquests entorns actuals d'administració electrònica avançada 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 o per a recuperar-se'n en un temps

raonable per a continuar prestant els seus serveis. La ciberhigiene és un principi fonamental[1] relacionat amb la seguretat de la informació i equival a establir mesures rutinàries senzilles per a minimitzar els riscos de les ciberamenaces. De manera anàloga al que ocorre amb la higiene personal, les bones pràctiques de ciberhigiene poden impulsar una major immunitat en les entitats que les apliquen, la qual cosa redueix el risc davant d'un ciberatac.

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

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022 hem realitzat el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Vila-real. Exercici 2020.

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

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 2020, relacionats amb les aplicacions i

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

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

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

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

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

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

4. CONCLUSIONS

No s'ha realitzat cap progrés per a millorar la ciberseguretat des de la nostra auditoria anterior i no s'ha atés cap de les nostres recomanacions per a aconseguir aquesta millora.

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

L'entitat ha d'adoptar mesures urgents per a reconduir la situació

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconsegueix un **índex de maduresa general del 39,8%**, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*; és a dir, els processos de control existeixen, però la gestió no està organitzada correctament.

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

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

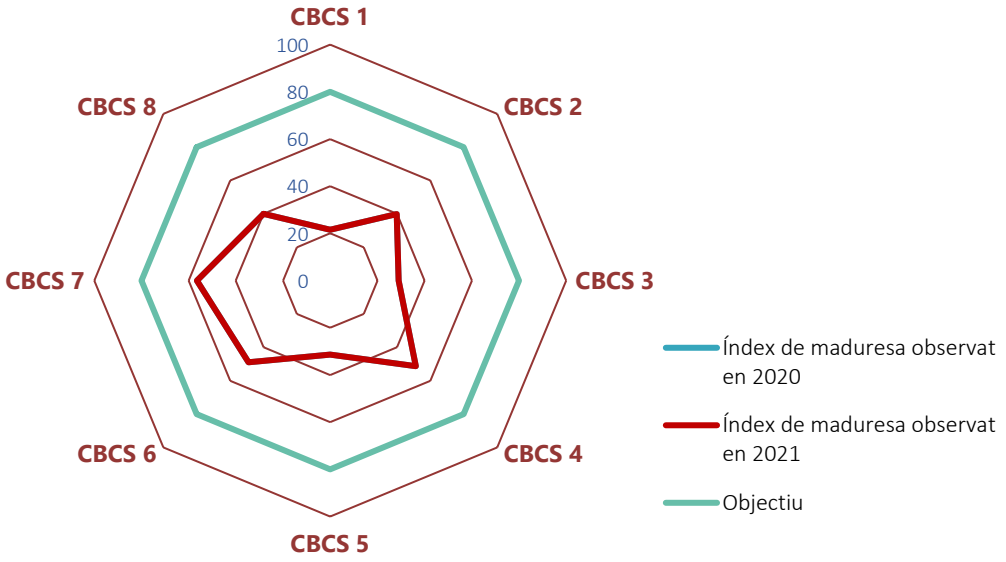
Control	2020			2021		
	Índex de maduresa	Nivell de maduresa	Índex de compli-ment	Índex de maduresa	Nivell de maduresa	Índex de compli-ment
CBCS 1 Inventari i control de dispositius físics	*21,6%*	***N1***	*27,0%*	*21,6%*	***N1***	*27,0%*
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	*39,8%*	***N1***	*49,7%*	*39,8%*	***N1***	*49,7%*
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	*29,0%*	***N1***	*36,2%*	*29,0%*	***N1***	*36,2%*
CBCS 4 Ús controlat de privilegis administratius	*51,3%*	***N2***	*64,1%*	*51,3%*	***N2***	*64,1%*
CBCS 5 Configuracions segures del programari i maquinari	*31,4%*	***N1***	*39,2%*	*31,4%*	***N1***	*39,2%*
CBCS 6 Registre de l'activitat dels usuaris	*49,0%*	***N1***	*61,3%*	*49,0%*	***N1***	*61,3%*
CBCS 7 Còpies de seguretat de dades i sistemes	*56,5%*	***N2***	*70,6%*	*56,5%*	***N2***	*70,6%*
CBCS 8 Compliment normatiu i governança de ciberseguretat	*40,0%*	***N1***	*50,0%*	*40,0%*	***N1***	*50,0%*
General	39,8%	***N1***	49,8%	39,8%	***N1***	49,8%

L'índex de compliment dels CBCS és del 49,8%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3 procés definit*. Aquest índex no ha millorat des del nostre informe anterior i la comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2020 no mostra cap millora en cap control, atés el grau nul d'atenció a les nostres recomanacions (vegeu apartat 5 següent).

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

D'una manera més sintètica i gràfica, la situació observada dels controls es reflecteix en el gràfic 1, tant en aquesta auditoria com en la realitzada l'any 2020. El gràfic no mostra la línia blava de 2020, ja que com que no s'ha millorat gens, aquesta línia està sota la línia roja de 2021.

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



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

L'Ajuntament de Vila-real no té establida una estructura de governança de la ciberseguretat, tal com exigeix la normativa i un sistema adequat de control intern.

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

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

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

Hem pogut verificar l'existència d'un insuficient nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament. No s'ha atés cap de les

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

nostres recomanacions i hem constatat la falta d'iniciatives per part de la corporació per a reconduir la situació.

Aquest fet, al costat de les rellevants mancances identificades, ens permet afirmar que la governança de la ciberseguretat de l'Ajuntament de Vila-real és pràcticament inexistent. Aquestes mancances són:

- La falta d'activitat de la Junta d'Administració Electrònica, Seguretat de la Informació i Transparència, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat, que ha d'incloure representació de les àrees de l'organització afectades.

- La inexistència de determinats rols clau en l'organització, com el responsable de seguretat de la informació. Considerem com a factor de risc crític la falta d'un responsable de seguretat del conjunt dels sistemes d'informació de l'Ajuntament, que vetle per l'aplicació homogènia de les mesures de seguretat de l'ENS en la totalitat dels sistemes de l'entitat i particularment en un entorn de sistemes descentralitzats.

- L'absència d'un marc normatiu (ús correcte d'equips, serveis, instal·lacions, usos indeguts, responsabilitats del personal) i procedimental (documents que detallen com es fan les tasques habituals, responsables, report de comportaments anòmals) únic per als cinc sistemes de l'Ajuntament, amb la finalitat de garantir una efectiva organització global de la seguretat de la informació.

- La inacció de la corporació davant els riscos identificats, a pesar que l'alta direcció ha sigut coneixedora d'aquests riscos a través del Ple, al qual es va elevar l'informe de la Sindicatura de Comptes de l'exercici 2020, i de les recomanacions efectuades per empreses especialitzades en seguretat de la informació contractades per la corporació, que indiquen la necessitat de disposar d'un pla director de ciberseguretat i del compliment de l'ENS.

- La falta de personal i de dotació pressupostària suficient per a atendre la problemàtica de la seguretat de la informació.

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

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

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

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

Per a esmenar les deficiències de control identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 4 anterior, reiterem bàsicament les recomanacions que es van efectuar en l'auditoria de 2020, ja que no s'ha realitzat cap millora des de llavors. L'Ajuntament haurà de dedicar els esforços i recursos necessaris per a esmenar les deficiències pendents.

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

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

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

   A l'hora de garantir un nivell d'actualització adequat de l'inventari, és aconsellable donar prioritat a l'ús d'eines per a la detecció i actualització automàtica dels elements del sistema d'informació davant de procediments manuals.

2. Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

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

3. Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga:

   - L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques de programari.

   - La definició d'un pla de manteniment de la totalitat del programari utilitzat a l'Ajuntament.

4. Identificar 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. Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:

   - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i les accions

actualment establides de seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat.

- La priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.

6. Implantar eines que permeten la gestió unificada i automatitzada de pedaços de seguretat i altres actualitzacions.

7. Optimitzar l'explotació de la informació proporcionada per la sonda del CCN,[3] incloent-hi els avisos proporcionats en el procés de resolució de vulnerabilitats.

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

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

   - L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió han de realitzar-se amb usuaris nominatius.

   - 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.

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

9. 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.[4]

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

[3] Centre Criptològic Nacional.

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

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

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

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

11. Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.

12. Situar les còpies de seguretat localitzades en el node secundari de la xarxa municipal en el local correctament condicionat per a aquest fi disponible en el mateix edifici.

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

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

    - Designar les persones per als rols definits en la política de seguretat i constitució dels òrgans que s'hi descriguen.

    - Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriguen.

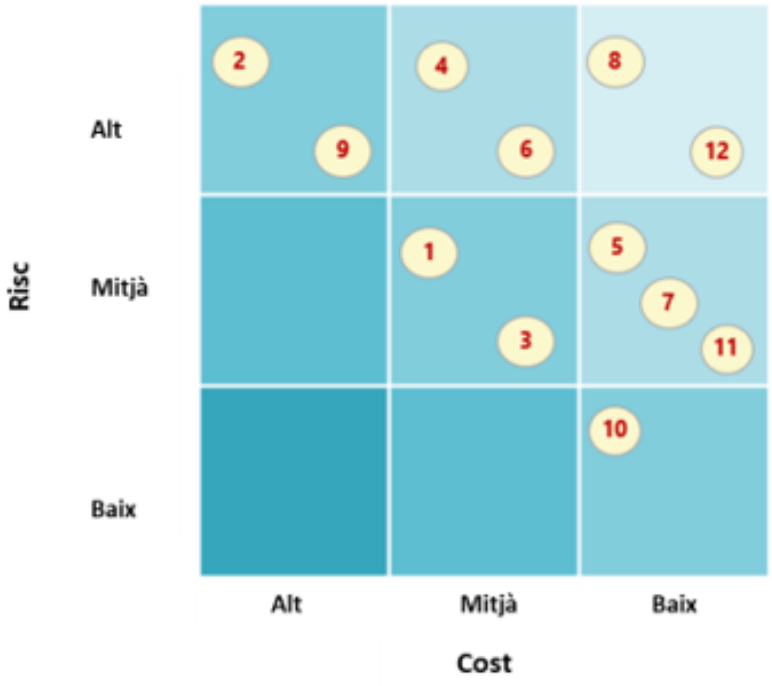
    - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.

14. En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular, ha d'aplicar la totalitat de mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.

Priorització de les recomanacions

A fi que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial a mitigar** i **cost estimat de la implantació**. Aquest gràfic segueix igual respecte a l'informe de 2020, considerant que no s'ha realitzat cap millora des de llavors. No s'hi inclouen els punts 13 i 14 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 algunes actuacions en matèria de ciberseguretat que atendrien parcialment algunes de les recomanacions anteriors. La implantació efectiva d'aquestes actuacions tindrà un impacte positiu, encara que molt limitat, en el nivell de ciberseguretat de l'entitat. Aquestes actuacions són:

- Actualització de determinats components del sistema de còpies. Entre les actuacions planificades es troba:
  - la substitució de l'equipament que es troba fora de servei, la licitació del qual ha sigut iniciada i inclou els serveis de suport tècnic i manteniment del nou equipament.
  - l'actualització de determinats components del sistema de còpies, en fase d'estudi, a fi de millorar el temps de còpia i proporcionar restauracions més de confiança amb major rapidesa.
- Desplegament de serveis i eines proporcionats pel CSIRT-CV, com a part del Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana, i l'adquisició i desplegament de solucions finançades per mitjà dels fons europeus Next Generation EU.

Seguiment de recomanacions anteriors

Hem realitzat un seguiment de les recomanacions efectuades en l'informe d'auditoria de l'any 2020.

Tal com es mostra en el quadre 2, de les recomanacions realitzades en aquell informe, no se n'ha atés cap.

Quadre 2. Seguiment de recomanacions

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
1	Aprovar formalment un procediment per a la gestió de l'inventari i el control d'actius físics que reculla el procés complet, incloent-hi les revisions periòdiques de maquinari, actualitzant degudament l'inventari i incloent-hi les dates d'aquestes revisions. A l'hora de garantir un nivell d'actualització adequat de l'inventari, és aconsellable donar prioritat a l'ús d'eines per a la detecció i actualització automàtica dels elements del sistema d'informació davant de procediments manuals.	L'inventari d'ordinadors portàtils i impressores, que gestiona l'empresa que proporciona el manteniment es trobava finalitzat i actualitzat en el moment de la revisió, 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	**No aplicada**	Es manté la redacció.
2	Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.	Sense variació.	**No aplicada**	Es manté la redacció.
3	Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga: - L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques de programari. - La definició d'un pla de manteniment de la totalitat del programari utilitzat a l'Ajuntament.	Sense variació.	**No aplicada**	Es manté la redacció.
4	Identificar i actualitzar tots els sistemes que es troben fora del període de suport.	Sense variació.	**No aplicada**	Es manté la redacció.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
5	Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents: - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i les accions actualment establides de seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat. - La priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.	Sense variació.	**No aplicada**	Es manté la redacció.
6	Implantar eines que permeten la gestió unificada i automatitzada de pedaços de seguretat i altres actualitzacions.	Sense variació.	**No aplicada**	Es manté la redacció.
7	Optimitzar l'explotació de la informació proporcionada per la sonda del CCN, incloent-hi els avisos proporcionats en el procés de resolució de vulnerabilitats.	Sense variació.	**No aplicada**	Es manté la redacció.
8	Formalitzar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga: - L'eliminació, 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. - 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.	Sense variació.	**No aplicada**	Es manté la redacció.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
9	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 d'incloure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà de procediment manual o d'eines automatitzades de monitoratge de la configuració.	Sense variació.	**No aplicada**	Es manté la redacció.
10	Aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat d'usuari 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.	Sense variació.	**No aplicada**	Es manté la redacció.
11	Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.	La cabina de discos que realitza les còpies de seguretat es troba fora de servei i sense contracte de manteniment, per la qual cosa no es realitzen còpies de seguretat per mitjà d'aquest sistema No obstant això, per a compensar la pèrdua de servei produïda per l'avaria, es realitzen noves còpies de seguretat dels sistemes crítics de l'entitat. Aquestes còpies són emmagatzemades en dispositius de tipus NAS (*network attached storage*) i es troben desconnectades de la xarxa municipal.	**No aplicada**	Es manté la redacció.
12	Situar les còpies de seguretat localitzades en el node secundari de la xarxa municipal en el local correctament condicionat per a aquest fi disponible en el mateix edifici.	Sense variació.	**No aplicada**	Es manté la redacció.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
13	Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de: - Designar les persones per als rols definits en la política de seguretat i constitució dels òrgans que s'hi descriguen. - Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriguen. - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.	Sense variació.	**No aplicada**	Es manté la redacció.
14	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 d'aplicar la totalitat de mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.	Sense variació.	**No aplicada**	Es manté la redacció.

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 tot tipus d'amenaces 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 INES[5] del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs es mantinguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan implementades correctament.

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

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

Objectiu de l'auditoria

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022, el nostre objectiu ha sigut realitzar el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Vila-real. Exercici 2020, i obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això n'hem avaluat tant el disseny[6] com l'eficàcia operativa[7] per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport. També hem revisat el compliment de la normativa bàsica relativa a la seguretat de la informació.

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

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada dels huit CBCS revisats en l'auditoria de l'any 2020, relacionats amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interés general.

Abast

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

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

Atesa la naturalesa de l'objecte material a revisar –la gran amplitud, complexitat i diversitat dels sistemes d'informació d'un ens local de grans dimensions– ha sigut necessari delimitar i concretar quins sistemes s'havien d'analitzar. En aquest sentit, hem analitzat les aplicacions que suporten els processos de gestió comptable i pressupostària i la gestió tributària i recaptadora, així com els controls que tenen implantats.

[6] 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.

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

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

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

L'abast específic d'aquest treball de seguiment de recomanacions ha estat condicionat per l'organització funcional de l'Ajuntament. Tal com s'estableix en el "Document de seguretat dels sistemes d'informació i d'administració electrònica de l'Ajuntament de Vila-real", l'Ajuntament disposa de sistemes centralitzats gestionats pel Servei de Noves Tecnologies (SNT) i sistemes descentralitzats, gestionats de manera autònoma pels serveis corresponents sense control de l'SNT. Aquesta norma estableix que els responsables dels sistemes descentralitzats han de gestionar determinats processos de seguretat, com:

- l'inventari de maquinari i programari
- la gestió d'usuaris i privilegis administratius
- la realització de còpies de seguretat

Els sistemes descentralitzats són:

- El Servei Municipal d'Esports
- La Policia Local
- El servei de telecomunicacions
- Els serveis públics municipals

Hi ha, per tant, determinats processos de seguretat sobre els sistemes descentralitzats la responsabilitat dels quals no està definida (tots excepte els tres indicats prèviament), circumstància que representa un factor de risc addicional.

Aquest treball únicament ha comprés la revisió de recomanacions sobre els sistemes centralitzats. Per tant, els controls i processos de seguretat no revisats no han sigut considerats a l'efecte de puntuació de cada un dels CBCS, encara que considerem que la seua valoració no tindria un efecte positiu sobre els indicadors obtinguts.

Àmbit temporal

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

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

Metodologia

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

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

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

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

La guia pràctica de fiscalització dels OCEX 5313

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

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS. No obstant això, atesa l'amplitud de l'ENS, que està format per 75 mesures de seguretat, per a la seua

inclusió en els CBCS es va seleccionar una sèrie limitada de controls. Per a triar els més rellevants es va atendre el marc conceptual establit per la prestigiosa organització Center for Internet Security (CIS),[8] que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. L'avantatge principal és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant ciberatacs al voltant del 85%. Si s'implementen els vint controls el risc es pot reduir un 94%.

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

Com que l'ENS és de compliment obligat per a tots els ens públics, s'ha tingut especial cura que la metodologia d'auditoria dels controls bàsics de ciberseguretat estiguera plenament alineada amb l'ENS. Aquesta alineació facilita a la Sindicatura la realització de les auditories de ciberseguretat i coadjuva a la implantació de l'ENS en els ens auditats, ja que pràcticament tots els subcontrols o controls detallats que verifica la Sindicatura els requereix l'ENS. D'aquesta manera, els huit controls bàsics de ciberseguretat presenten una correspondència (no exacta) amb les referències de l'ENS següents:

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.

[8] Center for Internet Security, <www.cisecurity.org>.

Els CBCS com a mesures de ciberhigiene

L'European Union Agency for Cybersecurity (ENISA) assenyala[9] 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.[10]

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.[11]

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

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.

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

[10] 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.

[11] Carnegie Mellon University *Software* Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* <https://resources.sei.cmu.edu/asset_files/presentation/2017_017_001_508771.pdf>, 2017.

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

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

Quadre 5. Els CBCS i els seus subcontrols

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

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

Avaluació dels resultats del treball

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

Subcontrols

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

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

Quadre 6. Avaluació dels subcontrols

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

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. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. *L'eficàcia del procés depén de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.*
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. *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).* *L'èxit és més que bona sort: es mereix.* *Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2 i que sí que es gestiona en el nivell 3.*
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. *Es disposa d'un sistema de mesures i mètriques per a conéixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.* *En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.*
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. *El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.* *S'estableixen objectius quantitatius de millora, 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.* *En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes a base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.*

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

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

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

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

Autenticitat	És la propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.
Traçabilitat	És la propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

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

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

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

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

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

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

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[12]

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

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

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

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

Indicadors globals

A l'efecte de l'ENS, la guia CCN-STIC-824 preveu una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics. Aquests indicadors han sigut adaptats per a la seua aplicació als CBCS, ja que permeten dur a terme un resum de l'estat de les mesures de seguretat dels ens auditats:

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

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

Governança de ciberseguretat

A l'efecte d'aquest treball, s'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'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una forma responsable.[13]

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

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

És més que una mera qüestió tècnica, per la qual cosa **exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització.**[14]

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.

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

[14] Vegeu l'apartat 66 d'*Análisis núm. 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE,* del Tribunal de Comptes Europeu.

La implicació dels òrgans superiors és, potser, el factor més important per a la implantació amb èxit d'un sistema de gestió de la seguretat de la informació o de ciberseguretat.[15] L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació,[16] que s'ha de materialitzar en aspectes com ara:

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

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

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

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

  La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,[17] que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat, i és la màxima autoritat en l'organització respecte a les decisions de seguretat que afecten els sistemes que manegen informació o presten algun servei. La seua composició ha de constar en la PSI.

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

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

- Decidir els criteris d'acceptació del risc i els nivells acceptables de risc.

- Dirigir les revisions periòdiques de la PSI i vetlar per la realització de les auditories internes de seguretat.

[15] *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.

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

[17] *Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC*, CCN, gener de 2021.

Seguiment de les recomanacions

En aquest treball s'ha realitzat el seguiment de les recomanacions recollides en l'apartat 6 de l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Vila-real. Exercici 2020.

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

Quadre 8. Situació de les recomanacions

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

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

Comunicació i confidencialitat

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

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

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

APÈNDIX 2

Situació dels controls bàsics de ciberseguretat

CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

L'Ajuntament no ha fet canvis significatius respecte de l'inventari i control de dispositius físics que observem en la revisió anterior.

La normativa de seguretat aprovada per la Junta d'Administració Electrònica, Seguretat de la Informació i Transparència de l'Ajuntament de Vila-real (JAESIT) recull l'obligació dels responsables de la informació de cada sistema descentralitzat de realitzar l'inventari dels elements de maquinari que componen aquests sistemes, però el procediment no ha sigut desenvolupat ni aprovat en aquest període.

El Servei de Noves Tecnologies (SNT) disposa de dos inventaris de gestió manual per a l'administració de determinats actius: un inventari d'elements del CPD, que és una eina crítica d'administració i es manté correctament actualitzat; i un inventari d'ordinadors portàtils i impressores que gestiona l'empresa externa que proporciona el manteniment, inventari que es trobava en fase final d'implantació a 31 de desembre de 2021 i ha sigut completat en el moment de la revisió.

D'altra banda, no s'ha implantat un control robust que impedisca la connexió de dispositius físics no autoritzats als sistemes d'informació des de la revisió anterior.

El nivell de control sobre l'inventari i el control d'actius físics és insuficient, i la valoració global aconsegueix un **índex de maduresa del 21,6%,** que es correspon amb un **nivell N1 de maduresa *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 1 del 27,0%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

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

Situació del control

L'Ajuntament no ha fet canvis significatius respecte a l'inventari i control de programari autoritzat que vam observar en la revisió anterior.

Si bé la responsabilitat de l'inventariat de programari es troba establida en la normativa de seguretat vigent, l'Ajuntament no ha aprovat un procediment que reculla les mesures de seguretat sobre l'inventari i control de programari que s'han d'aplicar.

L'Ajuntament virtualitza la totalitat de les aplicacions municipals centralitzades. L'inventari de programari és el catàleg d'aplicacions de l'eina de virtualització. La gestió d'usuaris i drets d'accés a aquestes aplicacions es realitza per mitjà d'un procés adequat que inclou la revisió i aprovació de permisos i que es troba recollit en un procediment que no ha sigut aprovat.

D'altra banda, es va evidenciar l'existència d'un elevat nombre d'equips amb sistemes operatius fora del període de suport del fabricant, particularment servidors, que no s'han actualitzat a versions adequades en aquest període, fet que suposa un greu risc per al sistema d'informació.

La gestió del llicenciament i el manteniment d'aplicacions comercials la realitza l'SNT per mitjà d'un procés adequat i gestionable, però no està formalitzat en procediment aprovat.

El treball anterior no va incloure en el seu abast l'anàlisi de l'inventari de programari dels sistemes descentralitzats, per la qual cosa no hem realitzat cap revisió sobre aquests sistemes en aquest treball.

Hi ha un nivell insuficient de control sobre l'inventari i control de programari autoritzat, de manera que l'**índex de maduresa és del 39,8%**, que es correspon amb un **nivell de maduresa *N1,* inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la gestió no està organitzada correctament. Això representa un **índex de compliment del CBCS 2 del 49,7%**.

No s'ha produït cap millora respecte de la nostra auditoria anterior.

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

Objectiu del control

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

Situació del control

L'Ajuntament no ha fet canvis significatius respecte al procés d'identificació i solució de vulnerabilitats que vam observar en la revisió anterior.

Sobre la gestió de vulnerabilitats realitzada per l'Ajuntament en el treball anterior es va observar que s'efectuaven algunes accions a fi d'identificar i remeiar vulnerabilitats, però aquestes accions no s'han implantat de manera efectiva en tots els sistemes, ni s'han establit en un procediment aprovat.

La identificació i solució de vulnerabilitats únicament es realitzava sobre determinats sistemes inclosos en el nostre abast, bé de manera manual per mitjà de la cerca i resolució d'unes certes vulnerabilitats crítiques, bé per part de tercers per mitjà de contractes de manteniment de determinats sistemes. Aquesta gestió no s'ha estés a la resta de sistemes de l'Ajuntament. El procés de priorització i resolució d'aquestes vulnerabilitats es gestiona de manera informal i no s'ha inclòs en un procediment aprovat.

Hi ha, per tant, determinats sistemes sobre els quals no s'ha establit cap tipus d'acció per a la identificació i solució de vulnerabilitats, fet que constitueix una important deficiència de control.

Sobre l'aplicació de pedaços i actualitzacions de seguretat, de manera general, únicament s'apliquen de manera sistemàtica sobre determinats sistemes l'actualització dels quals s'estableix en contractes de manteniment amb tercers. Per a la resta de sistemes, i particularment per als sistemes Windows, no s'ha implantat un procés de control sobre els pedaços i actualitzacions, mancança que pot suposar un risc greu per a la seguretat dels sistemes de l'entitat.

Per als sistemes descentralitzats que no són gestionats per l'SNT, no es van verificar les mesures implantades en el treball anterior. Per tant, no s'ha realitzat cap revisió atés que es troba fora de l'abast del treball.

El nivell de control és insuficient i la valoració global sobre aquest control aconsegueix un **índex de maduresa del 29,0%,** que es correspon amb un **nivell de maduresa *N1, inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està organitzada correctament. Això representa un **índex de compliment del CBCS 3 del 36,2%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

L'Ajuntament no ha fet canvis significatius respecte a l'ús controlat de privilegis administratius que observem en la revisió anterior.

La responsabilitat de la gestió d'usuaris està establida en la normativa de seguretat i es diferencia entre sistemes centralitzats, gestionats per l'SNT, i sistemes descentralitzats, gestionats pels mateixos responsables dels sistemes. Es van identificar en la revisió anterior determinades mesures efectives per al control de comptes d'administració, però aquestes mesures no s'han detallat formalment en un procediment aprovat i no es troben implantades de manera homogènia en tots els sistemes.

La gestió de l'assignació de privilegis administratius en els sistemes inclosos en l'abast de la fiscalització es realitza amb diferent grau d'efectivitat depenent del sistema. A més, no s'aplica una política d'autenticació homogènia en tots els sistemes o la política aplicada no és robusta en tots els casos.

No s'ha corregit l'ús de comptes d'administració no nominatius en determinats sistemes, la qual cosa impedeix la traçabilitat de les accions en cas d'incidents i constitueix la deficiència més significativa detectada en aquest control.

S'ha confirmat l'existència d'identificadors diferenciats per a un mateix usuari, depenent del tipus de tasca que calga exercir en el sistema, a fi de limitar l'ús d'identificadors amb privilegis administratius en les tasques que no en requereixen un.

Sobre la gestió d'usuaris administradors en els sistemes descentralitzats, no hem realitzat cap revisió addicional sobre els sistemes descentralitzats que es van analitzar en el treball anterior.

Existeix un cert nivell de control sobre els comptes amb privilegis administratius, però hi ha possibilitats de millora. La valoració global del control indica d'un **índex de maduresa del 51,3%,** que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment d'aquest CBCS 4 del 64,1%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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

Situació del control

L'Ajuntament no ha fet canvis significatius respecte a les configuracions segures de programari i maquinari que vam observar en la revisió anterior. Hem verificat que no s'ha aprovat formalment un procediment des de la nostra auditoria anterior. Encara que l'entitat aplica configuracions de seguretat en determinats sistemes, aquestes accions no són suficients per a assegurar l'efectivitat del control.

Si bé es disposa de plantilles per a la configuració de determinats dispositius, aquestes no tenen caràcter de fortificació ni la seguretat per defecte és el seu objecte.

Hi ha, per tant, un nivell deficient de control en l'aplicació de configuracions segures en dispositius i programari, per la qual cosa s'hauran de dedicar esforços i recursos per a millorar-la. La valoració global del control aconsegueix un **índex de maduresa del 31,4%,**

que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està organitzada correctament. Això representa un **índex de compliment del CBCS 5 del 39,2%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

L'Ajuntament no ha fet canvis significatius respecte al registre de l'activitat dels usuaris que vam observar en la revisió anterior.

En l'auditoria anterior s'analitzaren les accions de l'Ajuntament per al control de l'activitat dels usuaris en els sistemes i, encara que es disposa de certes mesures relacionades, hem constatat que en aquest període no s'han establit formalment en un procediment escrit i aprovat.

Hem verificat que el registre d'activitat es troba activat en els sistemes inclosos en l'abast de la revisió, si bé es continua mantenint la configuració per defecte que defineix el fabricant.

L'Ajuntament disposa de dos sistemes per a la gestió centralitzada de registres d'activitat de determinats actius, la qual cosa suposa una millora de la configuració bàsica per defecte dels *logs* d'auditoria. No obstant això, aquestes eines no integren tots els sistemes rellevants des del punt de vista de la ciberseguretat i la revisió d'aquests registres d'activitat es realitza de manera informal, no procedimentada.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 49,0%,** que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 6 del 61,3%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

Utilitzar processos i eines per a realitzar 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

L'Ajuntament realitza diverses accions per al control de les còpies de seguretat de les dades i sistemes. La responsabilitat de la realització de còpies de seguretat es troba establida en la normativa de seguretat vigent i el procés es troba correctament definit i implantat, però no s'ha recollit en un procediment aprovat formalment.

Les polítiques de còpia aplicades als sistemes situats en els servidors centrals de l'Ajuntament s'han desenvolupat d'acord amb les necessitats identificades des del mateix SNT i s'apliquen de manera efectiva. No obstant això, el resultat dels treballs de còpia es revisa per mitjà d'un procés manual que no es troba adequadament definit i gestionat.

S'ha confirmat que l'SNT realitza de manera sistemàtica proves de recuperació planificades com a part d'un procés de proves en entorn de preproducció per a la implantació de nous sistemes i gestió de canvis. Aquestes proves de preproducció permeten la comprovació de còpies de seguretat de sistema crítiques, i es documenten adequadament.

Així mateix, les mesures implantades per a la protecció de les còpies de l'SNT es poden considerar eficaces. No obstant això, tal com es va identificar en la revisió anterior, les còpies de seguretat, situades en un edifici que actua com a node secundari de la xarxa municipal, estan emplaçades en un local que no disposa de totes les condicions d'adequació física requerides.

Durant la realització del treball de revisió ens han indicat que la cabina de discos que realitza les còpies de seguretat està fora de servei i sense contracte de manteniment, per la qual cosa no es realitzen còpies de seguretat addicional per mitjà d'aquest sistema.

Com a mesura compensatòria, es realitzen setmanalment còpies de seguretat desconnectades de la xarxa en dispositius de tipus NAS (*network attached storage*) dels sistemes crítics dependents de l'SNT que és responsabilitat del Departament d'informàtica, a fi de disposar d'una còpia de seguretat addicional. Una vegada realitzada la còpia en el dispositiu NAS, es desconnecta de la xarxa i, una vegada verificada la seua integritat, es guarda en un lloc segur.

En cas de ser infectat el sistema per un virus de tipus *ransomware*, el sistema de còpies setmanal desconnectat permet restaurar el sistema afectat amb una pèrdua màxima de dades d'una setmana.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 56,5%**, 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 70,6%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT

Objectiu del control

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

Situació del control

Compliment de l'ENS

Des de la revisió realitzada l'any 2020, l'Ajuntament no ha realitzat accions que hagen millorat el nivell de compliment exigit pel Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

A més, no s'han designat determinats rols i responsabilitats en seguretat de la informació, particularment el responsable de seguretat de la informació, deficiència crítica en un entorn de sistemes descentralitzats.

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, continua vigent el nomenament del DPD i la seua notificació a l'Agència Espanyola de Protecció de Dades.

No s'ha realitzat cap auditoria en matèria de protecció de dades en què s'especifiquen les mesures tècniques i organitzatives que s'han adoptat per a donar compliment a les obligacions de la legislació vigent

Compliment de la legalitat del registre de factures

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

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió no es modifica respecte a l'informe emés l'any 2020, de manera que l'Ajuntament aconsegueix un **índex de maduresa del 40,0%**, que es correspon amb un **nivell de maduresa *N1, inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 8 del 50,0%**. No s'ha produït cap millora respecte de la nostra auditoria anterior.

Governança de ciberseguretat

L'Ajuntament de Vila-real no té establida una estructura de governança de la ciberseguretat, tal com exigeix la normativa i un adequat sistema de control intern.

Els òrgans superiors de l'Ajuntament 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.

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 permeten afirmar que la governança de la ciberseguretat de l'Ajuntament de Vila-real és pràcticament inexistent** i que hi ha un **nivell insuficient de compromís** i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament. Les mancances més rellevants identificades són les següents:

- La falta d'activitat de la Junta d'Administració Electrònica, Seguretat de la Informació i Transparència, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat, que ha d'incloure representació de les àrees de l'organització afectades.

  Aquesta circumstància ocasiona la falta de coordinació i comunicació entre els diferents responsables dels sistemes d'informació que hi ha a l'Ajuntament.

- La inexistència de determinats rols clau en l'organització, com el responsable de seguretat de la informació. A causa de l'organització funcional dels sistemes d'informació a l'Ajuntament, diferenciats en sistemes centralitzats i descentralitzats, considerem com a factor de risc crític la falta d'un responsable de seguretat del conjunt dels sistemes d'informació de l'Ajuntament, que vetle per l'aplicació homogènia de les mesures de seguretat de l'ENS en la totalitat dels sistemes de l'entitat i particularment en un entorn de sistemes descentralitzats.

- Absència d'un marc normatiu i procedimental únic per als cinc sistemes de l'Ajuntament. No s'ha desenvolupat el marc normatiu (ús correcte d'equips, serveis, instal·lacions, usos indeguts, responsabilitats del personal) i procedimental (documents que detallen com es fan les tasques habituals, responsables, report de comportaments anòmals) requerit en l'ENS per a garantir una organització global efectiva de la seguretat de la informació.

  Aquesta situació repercuteix negativament en la valoració dels controls, atés que la ineficiència de controls en qualsevol de les àrees repercuteix en el risc i la valoració global del control.

- La inacció de la corporació davant els riscos identificats, encara que l'alta direcció és coneixedora d'aquests riscos a través del Ple en el qual es va elevar l'informe publicat per la Sindicatura de Comptes sobre els controls bàsics de ciberseguretat de l'Ajuntament de Vila-real de l'exercici 2020, i de les recomanacions efectuades per

empreses especialitzades en seguretat de la informació contractades per la corporació, en què indiquen la necessitat de disposar d'un pla director de ciberseguretat i del compliment de l'Esquema Nacional de Seguretat.

- La falta d'atenció a mancances rellevants o situacions de risc sobrevingudes, a causa de la falta de personal i de dotació pressupostària per al seu tractament.

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.

Alguna mesura parcial i insuficient s'ha adoptat recentment, tal com s'ha assenyalat anteriorment.

APÈNDIX 3
Bones pràctiques destacables

Introducció

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

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

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

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

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

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

Entorn de preproducció

L'Ajuntament disposa d'un entorn de preproducció que es troba explotat de manera particularment efectiva. Aquest entorn és utilitzat en diversos controls i subcontrols de seguretat, especialment els següents:

- Gestió de canvis. L'Ajuntament utilitza l'entorn de preproducció per a l'execució de diversos processos relacionats amb la gestió de canvis en sistemes existents, incloent-

hi actualitzacions crítiques, i la posada en operació de nous sistemes. La gestió realitzada inclou tasques relatives a diversos subcontrols, entre els quals es troben:

- La realització de proves de testatge dels canvis en aplicacions i sistemes. Incloent-hi la realització de proves unitàries i proves d'integració.
- L'ús d'entorns per a proves separats de producció, per a limitar o eliminar l'afecció a l'entorn de producció de possibles problemes en la fase de proves.
- L'aprovació de l'usuari en les proves de testatge, per a validar els canvis realitzats.
- El registre exhaustiu de canvis i sol·licituds, per a facilitar la traçabilitat i seguiment del procés de canvi.

- Proves de recuperació de còpies de seguretat. Com a part del procés de realització de proves de testatge dels canvis en aplicacions i sistemes, es realitza de manera freqüent la recuperació completa i posada en operació de sistemes i components crítics, la qual cosa permet:
  - Verificar la viabilitat de les còpies existents.
  - La preparació i entrenament del personal relacionat amb la recuperació de dades i sistemes en cas d'incident de seguretat.
  - L'execució, de manera informal, de procediments per a la recuperació davant desastres.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

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

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

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

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

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

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

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

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

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i descriuen: *a*) l'ús correcte d'equips, serveis i instal·lacions; *b*) el que es considerarà ús indegut, i *c*) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular d'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: És un document d'alt nivell que defineix el que significa *seguretat de la informació* en una organització d'acord amb l'article 11 del Reial Decret 3/2010 i articula la gestió continuada de la seguretat. Ha de ser aprovada pel president o presidenta o la junta de govern d'una entitat local o el consell d'administració d'una societat. Ha d'estar accessible per a tots els membres de l'organització i redactada de manera senzilla, precisa i comprensible. Convé que siga breu, i que deixe els detalls tècnics per a altres documents més precisos que ajuden a dur a terme el que es proposa: normes de seguretat i procediments de seguretat.

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

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

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir amb el regidor responsable d'Innovació i noves tecnologies, amb el secretari i vicesecretari de l'Ajuntament i amb els responsables corresponents del Departament d'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, i de l'article 55.1.*c* del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'informe d'auditoria corresponent a 2021, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*h* del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 7 de setembre de 2022, va aprovar aquest informe d'auditoria.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe seguiment recomanacions CBCS Vila-real de l'any 2020 - SEFYCU 3480616

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 X9V2 AYA3 LZEK ZDKQ

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 - 13/09/22 07:34 VICENT CUCARELLA TORMO