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 PATERNA DE L'ANY 2019

Situació a 31 de desembre de 2021

RESUM

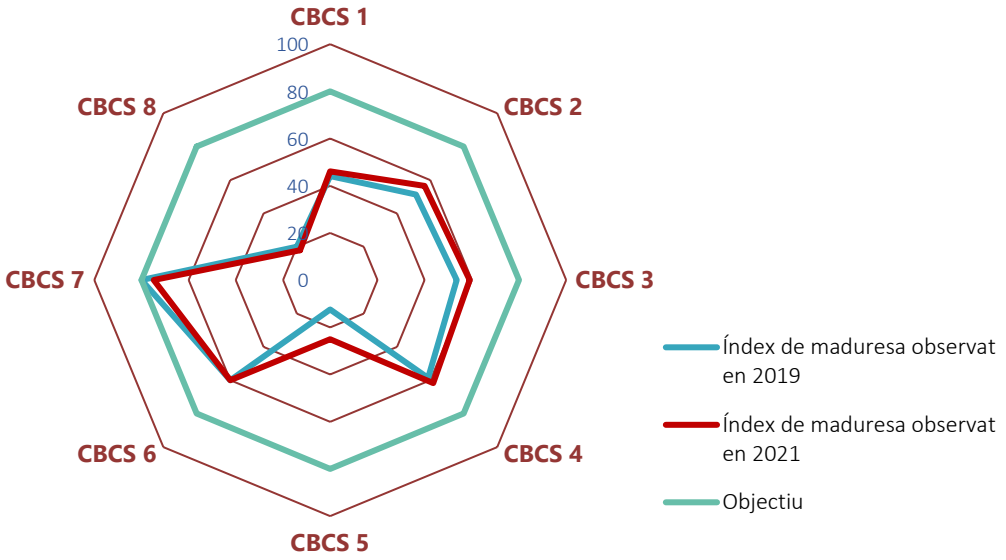
La transformació digital que estan experimentant totes les administracions públiques i la seua interconnexió a través de complexes xarxes informàtiques les exposa de manera cada vegada més intensa a amenaces provinents del ciberespai. Això origina un increment dels riscos associats als sistemes d'informació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

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

Conclusions

L'Ajuntament ha realitzat determinades accions des de la nostra auditoria anterior i s'han atés, encara que parcialment, algunes de les nostres recomanacions.

L'índex de maduresa general dels controls bàsics de ciberseguretat, l'objectiu dels quals seria aconseguir un 80%, mostra un valor del 50,2%, que suposa una escassa millora respecte del 47,5% recollit en la nostra auditoria de 2019, per la qual cosa el nivell d'efectivitat en els controls analitzats continua sent insuficient. L'Ajuntament ha d'adoptar les mesures necessàries per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en aquells controls que presenten deficiències significatives.



Hi ha un cert nivell de compromís i conscienciació amb la seguretat per part dels membres del departament TIC i dels òrgans superiors; no obstant això, diverses circumstàncies

indiquen que la governança de la ciberseguretat no pot considerar-se efectiva, una situació que s'ha d'esmenar.

Cal que el comité de seguretat de la informació, òrgan imprescindible per a la seua coordinació, es reunisca regularment a fi de conéixer l'estat de la seguretat de la informació de l'Ajuntament i prendre les decisions pertinents de manera oportuna. A més, els rols establits en la política de seguretat de l'Ajuntament han de definir-se correctament i exercir les seues funcions de manera efectiva.

Es necessària la implantació d'una cultura en matèria de ciberseguretat que afecte tots els nivells de l'organització i que ha de ser impulsada per la direcció en forma de plans estratègics que definisquen objectius i mesures concretes, incloent-hi plans periòdics de formació i conscienciació per als treballadors.

Així mateix, la nostra revisió també ha posat de manifest un grau molt deficient de compliment quant a l'adequació a les normes legals relacionades amb la seguretat de la informació, que ja es van identificar en el nostre treball de 2019 i no s'han corregit. L'informe assenyala els incompliments normatius sobre els quals s'ha d'actuar. En aquest sentit, l'Ajuntament ha adjudicat en 2022 un contracte per a esmenar aquests incompliments.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a corregir les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament, entre les quals, a més d'actualitzar els procediments de manera que descriguen les accions i controls implantats, recomanem la implantació de solucions per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa, actualitzar els sistemes obsolets, l'ús d'una eina de gestió centralitzada de vulnerabilitats, pedaços i actualitzacions i l'aplicació de seguretat per defecte a tots els sistemas i aplicacions crítiques de l'entitat.

NOTA

Aquest resum pretén ajudar a comprendre els resultats del nostre informe i facilitar la tasca als lectors i als mitjans de comunicació. Recomanem la lectura de l'informe complet 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 Paterna de l'any 2019

Situació a 31 de desembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

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

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

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

La necessitat d'una ciberhigiene adequada

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

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

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

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

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

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

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

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

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

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

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

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

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

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

4. CONCLUSIONS

Encara que s'han atés parcialment algunes recomanacions de la nostra auditoria anterior, l'índex de maduresa general dels controls bàsics de ciberseguretat continua sent insuficient i ha de millorar per a aconseguir els nivells establits per l'ENS.

L'Ajuntament té en marxa un conjunt de projectes que, si s'executen i gestionen adequadament, contribuiran a millorar els nivells de ciberseguretat dels seus sistemes d'informació.

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 50,2%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment.

Encara que l'Ajuntament ha atés de manera parcial les nostres recomanacions i l'índex de maduresa general ha millorat lleument des del 47,5% identificat en la nostra auditoria de 2019, l'índex de maduresa actual continua sent insuficient per a garantir un adequat grau de seguretat i aconseguir el 80% requerit per l'ENS.

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

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

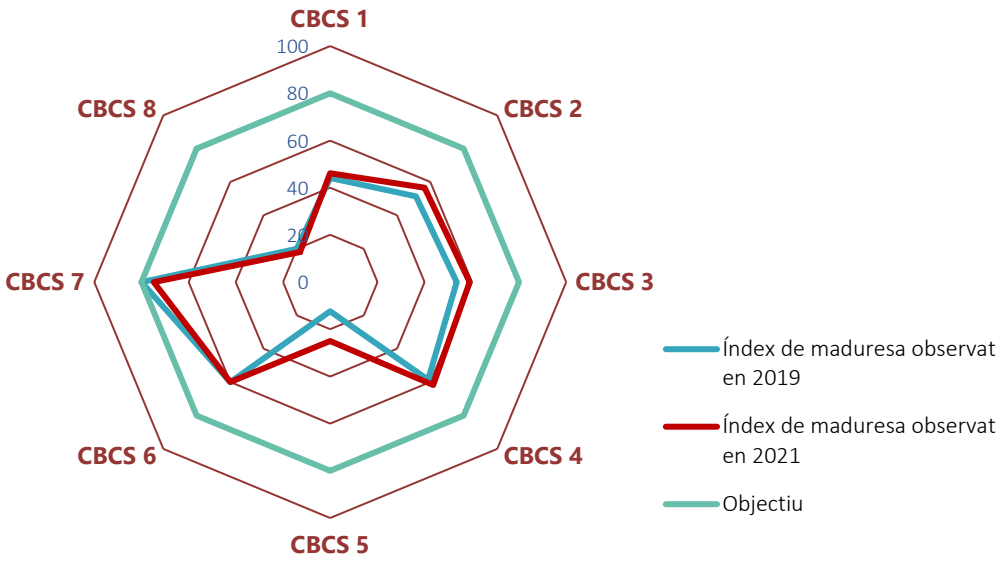
Control	2019			2021		
	Índex de maduresa	Nivell de maduresa	Índex de complí-ment	Índex de maduresa	Nivell de maduresa	Índex de complí-ment
CBCS 1 Inventari i control de dispositius físics	*44,1%*	***N1***	*55,1%*	46,1%	**N1**	57,6%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	*51,3%*	***N2***	*64,1%*	56,5%	**N2**	70,6%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	*53,6%*	***N2***	*67,0%*	59,1%	**N2**	73,9%
CBCS 4 Ús controlat de privilegis administratius	*58,6%*	***N2***	*73,3%*	61,7%	**N2**	77,1%
CBCS 5 Configuracions segures del programari i maquinari	*12,4%*	***N1***	*15,5%*	25,0%	**N1**	31,3%
CBCS 6 Registre de l'activitat dels usuaris	*60,0%*	***N2***	*75,0%*	60,0%	**N2**	75,0%
CBCS 7 Còpies de seguretat de dades i sistemes	*80,0%*	***N3***	*100,0%*	74,8%	**N2**	93,5%
CBCS 8 Compliment normatiu i governança de ciberseguretat	*20,0%*	***N1***	*25,0%*	18,0%	**N1**	22,5%
General	47,5%	***N1***	59,4%	50,2%	**N2**	62,7%

L'índex de compliment dels CBCS és del 62,7%, 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%.

La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una evolució dispar en els diferents controls, però, en conjunt, la millora és clarament insuficient. L'entitat ha d'aplicar mesures per a reconduir la situació i aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació, particularment sobre els controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 1, CBCS 5 i CBCS 8). En l'apartat 5 es fan 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 d'aquesta auditoria com de la realitzada l'any 2019.

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



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

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

Aquesta situació ha de ser esmenada promptament; són els òrgans superiors els qui han d'impulsar l'establiment d'un sistema adequat de gestió de 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.

Considerem que hi ha mancances que impedeixen que la governança es puga considerar efectiva, i les més rellevants són:

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

- L'Ajuntament disposa d'una política de seguretat de la informació i a més té normativa i procediments sobre aquest tema. No obstant això, aquesta normativa és de 2013 i està desactualitzada.

- La falta de lideratge i implicació en matèria de ciberseguretat dels òrgans superiors de l'Ajuntament, identificada en aspectes com la inexistència d'estratègies relacionades amb la seguretat de la informació o els incompliments legals identificats en el nostre treball d'auditoria anterior i que encara no s'han esmenat.

- El comité de seguretat, òrgan imprescindible per a coordinar la seguretat de la informació entre les diferents àrees de l'Ajuntament, no es reuneix i per tant no exerceix les seues funcions de manera efectiva.

És necessari solucionar de manera urgent les mancances identificades, atés que afecten de manera negativa el nivell de seguretat de la informació de l'Ajuntament, i atendre les recomanacions efectuades en aquest informe.

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

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

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

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

També s'assenyalen les mesures per al compliment de la legalitat que cal adoptar.

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

1. Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa i actualitzar el procediment per a la gestió de l'inventari i el control d'actius físics, de manera que reflectisca el procés i les mesures actualment implantades.

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

2. Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat o actualitzar els procediments existents, de manera que incloga:

   - Les mesures actualment implantades, incloent-hi les llistes de programari autoritzat (llistes blanques), les mesures tècniques que impedeixen l'execució del programari 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.

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

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

4. Elaborar i aprovar un procediment per a la identificació i solució de vulnerabilitats de manera que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament i que considere, a més de les mesures implantades, com a mínim, els aspectes següents:

   - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i el seguiment d'anuncis dels fabricants i butlletins en matèria de seguretat.

   - La priorització de les vulnerabilitats identificades basada en l'anàlisi dels riscos, així com la resolució i documentació, identificant dates, prioritat, responsable, solució, etc.

   Addicionalment, implantar alguna eina per a la gestió centralitzada de pedaços de seguretat i actualitzacions que s'aplique a tots els sistemes i aplicacions de l'entitat.

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

5. Elaborar i aprovar un procediment de seguretat per a la gestió d'usuaris amb privilegis d'administració que incloga aspectes com l'alta i baixa d'aquest tipus de comptes, la política d'autenticació, *log* d'accions, etc. i fer extensiu aquest procediment als usuaris amb privilegis d'administració de tots els sistemes i aplicacions de l'entitat.

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

6. Elaborar i aprovar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de

referència, com ara les guies STIC de les sèries 400, 500 i 600 del Centre Criptològic Nacional.[3]

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 seua revisió periòdica, bé manualment o per mitjà d'eines automatitzades de monitoratge de la configuració.

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

7. S'han de formalitzar i aprovar les accions dutes a terme per al tractament de *logs* d'auditoria de l'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, la gestió de drets d'accés al registre i la implantació i documentació del procés de revisió dels *logs*.

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

8. Actualitzar el procediment per a la gestió de còpies de seguretat de dades i sistemes de manera que descriga, a més de les accions dutes a terme (dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració) i els requisits de protecció de les còpies. Addicionalment, realitzar i documentar proves de restauració planificades i implantar les solucions previstes per a la protecció de les còpies.

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

9. 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:

   - Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010.

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

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

[3] 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.

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

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

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

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

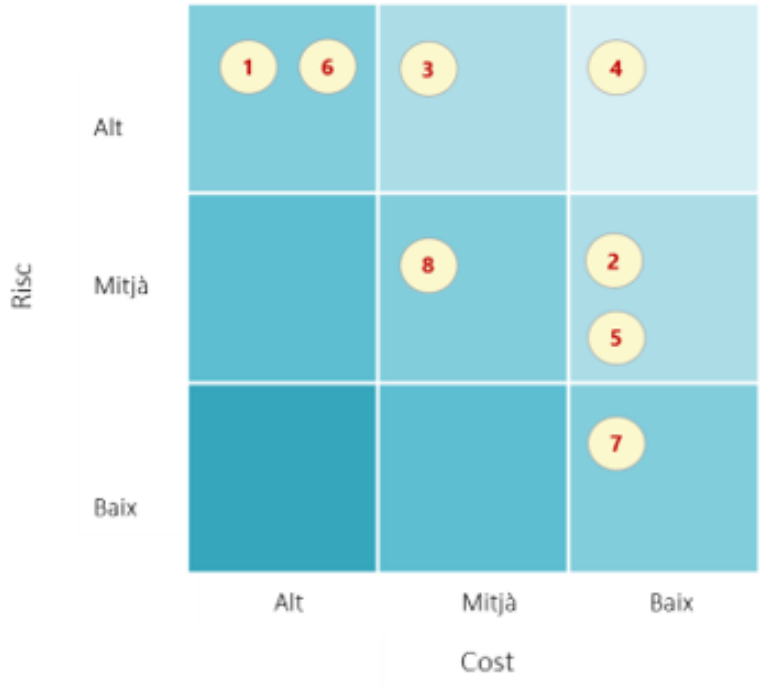
    - Planificar i executar auditories en matèria de protecció de dades.

11. Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.

Priorització de les recomanacions

A fi que es puguen establir accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial a mitigar** i **cost estimat de la seua implantació**. Aquest gràfic no s'ha modificat respecte a l'informe de 2019, considerant que no s'ha realitzat cap millora significativa des de llavors. No s'inclouen els punts 9, 10 i 11 anteriors, ja que són mesures de compliment obligat.

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



Seguiment de recomanacions anteriors

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

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

Quadre 2. Seguiment de recomanacions

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
1	Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.	Sense variació. A més s'ha d'actualitzar el procediment corresponent.	**No aplicada**	S'actualitza la redacció feta en 2019
2	Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat o modificar els procediments existents, de manera que s'hi incloga, addicionalment a les accions actualment implantades: - 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, incloent-hi tant aquell el manteniment del qual realitza directament l'Ajuntament com el programari el manteniment del qual realitzen empreses contractades amb aquesta finalitat.	L'Ajuntament ha realitzat algunes accions que incrementen el nivell de control sobre l'inventari de programari, encara que de manera limitada. El departament TIC ha implantat mesures per a impedir l'execució de programari no autoritzat, però aquestes són parcialment efectives i no s'han establit en un procediment formalment aprovat. No es disposa d'un pla de manteniment integral de programari.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019
3	Revisar i actualitzar tots els sistemes que es troben fora del període de suport.	L'Ajuntament ha renovat part dels equips d'usuari. No obstant això, continua havent-hi sistemes obsolets connectats a la xarxa corporativa.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019
4	Modificar el procediment actual de gestió i manteniment d'actius, incloent-hi el procés de gestió de vulnerabilitats de manera que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament considerant, com a mínim, els aspectes següents: - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i el seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat. - La priorització basada en l'anàlisi dels riscos, la resolució i la documentació de les vulnerabilitats tractades.	L'Ajuntament ha implantat algunes eines destinades a la identificació de vulnerabilitats, com ara microCLAUDIA i CARMEN del CCN i CSIRT-CV. No obstant això, continuen vigents algunes de les mancances identificades durant el treball de 2019. No s'utilitzen eines que permeten la gestió centralitzada de pedaços i actualitzacions (que sí que eren utilitzades durant la nostra revisió anterior), cosa que impacta en l'índex de maduresa del control i amplia la recomanació.	**Aplicada parcialment**	S'actualitza la redacció anterior

	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	Modificar l'actual normativa de control d'accés o 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 ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes. - La política d'autenticació que cal aplicar a aquest tipus de comptes.	L'Ajuntament ha esmenat part de les deficiències detectades durant la nostra auditoria anterior, però continua havent-hi possibilitats de millora per a garantir l'efectivitat del control. Les accions implantades s'han d'establir en un procediment formalment aprovat.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019
6	Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del Centre Criptològic Nacional. 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 a través de procediment manual o per mitjà d'eines automatitzades de monitoratge de la configuració.	Encara que hi ha algunes accions que milloren lleugerament l'índex de maduresa del control, com la seguretat millorada en els equips nous o la còpia de seguretat dels fitxers de configuració de determinats sistemes, es mantenen les nostres recomanacions anteriors.	**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
7	Aprovar formalment un procediment per al tractament de *logs* d'auditoria de l'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.	El departament TIC ha habilitat el registre d'accions en diferents sistemes, que són analitzats i centralitzats en un SIEM gestionat conjuntament pels tècnics i per una empresa externa. No obstant això, la posada en marxa és posterior al 31 de desembre de 2021, per la qual cosa no ha sigut considerat per al càlcul de l'índex de maduresa del control, però sí per a reformular la recomanació. No existeix un procediment aprovat i actualitzat que reculla les accions implantades.	**No aplicada**	S'actualitza la redacció feta en 2019
8	Ampliar l'abast del procediment existent de còpia de seguretat de manera que incloga la realització de proves periòdiques de recuperació, establint, com a mínim, periodicitat de les proves, abast i personal necessari.	Si bé el procés implantat a l'Ajuntament per a la còpia de seguretat d'aplicacions i sistemes era efectiu durant la nostra revisió anterior, la inexistència de determinades mesures de control fa disminuir lleugerament aquest índex. L'Ajuntament té prevista la implantació d'un centre *offline* d'emmagatzematge per a esmenar les mancances existents.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019
9	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: - Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010. - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.	L'Ajuntament no ha emplenat la Instrucció Tècnica de Seguretat de l'Informe de l'Estat de la Seguretat (Informe INES). La situació dels altres aspectes revisats és la mateixa que en la nostra auditoria anterior, encara que hi ha accions en curs destinades a esmenar els incompliments detectats. L'Ajuntament ha licitat i adjudicat un projecte per a l'adequació a l'ENS, que es troba en execució i no s'ha considerat en el càlcul dels índexs de maduresa per haver-se iniciat amb posterioritat al 31 de desembre de 2021.	**No aplicada**	S'actualitza la redacció feta en 2019

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
10	En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que estableixen l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de: - Nomenar un DPD d'acord amb el que es preveu en l'article 37.1.*a* de l'RGPD. - Elaborar el registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018. - Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD. - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD. - Planificar i executar auditories en matèria de protecció de dades.	L'Ajuntament ha licitat i adjudicat un projecte per a complir els requisits establits per la normativa. Les accions dutes a terme no han sigut considerades en el càlcul dels índexs de maduresa per haver-se iniciat amb posterioritat al 31 de desembre de 2021, encara que sí que s'han tingut en compte per a reformular les nostres recomanacions. En 2022 s'ha nomenat el DPD.	**No aplicada**	S'actualitza la redacció feta en 2019
11	Dur a terme l'auditoria del registre de factures exigida per la Llei 25/2013, de 27 de desembre.	Sense variació en 2021.	**No aplicada**	Es manté la redacció

Actuacions en curs

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

Enumerem a continuació les actuacions que es troben en execució quan s'ha emés aquest informe i que cal destacar per la seua rellevància:

- En 2021 es van adjudicar quatre lots del "contracte de servei per a la gestió de la infraestructura i seguretat de les TIC de l'Ajuntament de Paterna", que inclouen el manteniment, actualització, llicenciament, assessorament i assistència tècnica de la infraestructura, seguretat, programari i comunicacions de les TIC de l'Ajuntament, que inclou, entre altres:
  - Auditories de ciberseguretat de determinats sistemes crítics.
  - Actualització de versions de determinats sistemes.
  - Campanyes de formació i conscienciació als treballadors.
  - Implantació de doble factor d'autenticació en determinats sistemes.
  - Hores de suport/formació al personal del departament.
  - *Hacking* ètic.
  - Implantació de nous serveis i millores dels existents.
- Finalització de la implantació de l'eina SIEM i explotació de la seua informació, projecte que es troba en fase d'execució durant el segon semestre de 2022; l'Ajuntament rep informes periòdics i manté reunions per a esmenar incidents.
- Adjudicació en 2022 del "contracte de servei d'auditoria de revisió i adequació de compliment de l'ENS i normativa en matèria de protecció de dades personals i prestació de les funcions associades a la figura del delegat de protecció de dades", del qual s'han realitzat algunes accions durant el segon semestre de 2022, com les reunions inicials de l'ENS o el nomenament del DPD.
- L'Ajuntament ha iniciat en 2022 un projecte amb les subvencions rebudes per mitjà dels fons europeus del pla de recuperació, transformació i resiliència Next Generation EU. El projecte inclou:

- La posada en marxa d'un centre d'operacions de ciberseguretat (SOC). El projecte compta amb la instal·lació d'un agent de monitoratge de llocs i servidors, la integració d'un sistema d'alerta primerenca sobre el del CSIRT-CV, la implantació d'un EDR i aspectes de formació.

- L'aplicació de les mesures de protecció per a compliment de l'ENS, com ara l'adequació d'infraestructures, la protecció de la informació (centre d'emmagatzematge *offline*) i les comunicacions i aspectes de formació.

APÈNDIX 1
Metodologia aplicada

Introducció

Cada vegada un major nombre d'aspectes de la gestió pública es realitzen amb el suport de complexos sistemes informatitzats, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de tota classe provinents del ciberespai, majors riscos de ciberseguretat i s'han multiplicat els incidents de seguretat 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, i per això 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 a incidents i recuperar-se'n.

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

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

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

Objectiu de l'auditoria

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

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

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

Abast

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

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

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

[5] 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.

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

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

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

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls a 31 de desembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe, ja que fins a aquell moment s'ha admés qualsevol evidència disponible. Per tant, amb caràcter general l'Informe reflecteix la situació en aquell moment, ja que és freqüent que, des que s'inicia el treball de camp, determinades deficiències observades i assenyalades als gestors s'esmenen 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, així com 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 531, "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 més detall sobre la metodologia utilitzada ens remetem a aquesta guia.

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS. No obstant això, atesa l'amplitud de l'ENS, que està format per 75 mesures de seguretat, per a la seua inclusió en els CBCS es va seleccionar una sèrie limitada de controls. Per a triar els més rellevants es va atendre el marc conceptual establit per la prestigiosa organització Center for Internet Security (CIS),[7] que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. El seu avantatge principal és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant ciberatacs al voltant del 85%. Si s'implementen els vint controls, el risc es pot reduir un 94%.

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

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

Quadre 3. Els CBCS i l'ENS

Control		Mesura de seguretat de l'ENS*
CBCS 1	Inventari i control de dispositius físics	op.exp.1
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	op.exp.1 op.exp.2
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	mp.sw.2 op.exp.4
CBCS 4	Ús controlat de privilegis administratius	op.acc.4 op.acc.5
CBCS 5	Configuracions segures del programari i maquinari	op.exp.2 op.exp.3
CBCS 6	Registre de l'activitat dels usuaris	op.exp.8 op.exp.10
CBCS 7	Còpies de seguretat de dades i sistemes	mp.info.9
CBCS 8	Compliment normatiu i governança de la ciberseguretat	

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

Els CBCS com a mesures de ciberhigiene

L'European Union Agency for Cybersecurity (ENISA) assenyala[8] que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen" i reduir els ciberriscos.[9]

Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a afrontar els riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.[10]

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

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

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

[10] 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.

Quadre 4. Punts d'acció d'ENISA

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

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

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

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

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

Quadre 5. Els CBCS i els seus subcontrols

Control	Objectiu del control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots el dispositius de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats	L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
		CBCS 1-2: Control d'actius físics no autoritzats	L'entitat disposa de mesures de seguretat per a controlar (detectar i restringir) l'accés de dispositius físics no autoritzats.
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	Hi ha un procés per a identificar les vulnerabilitats dels components del sistema que assegura que aquestes són identificades en temps oportú.
		CBCS 3-2: Priorització	Les vulnerabilitats identificades són analitzades i prioritzades per a la seua resolució atés el risc que suposen per a la seguretat del sistema.
		CBCS 3-3: Resolució de vulnerabilitats	Es fa un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que aquestes es resolen en el temps previst en el procediment.
		CBCS 3-4: Pedaços	L'entitat disposa de procediments i eines que permeten aplicar els pedaços de seguretat publicats pels fabricants en un temps raonable.
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 en facilita el correcte control.
		CBCS 4-2: Canvi de contrasenyes per defecte	Les contrasenyes per defecte dels comptes que no s'utilitzen o bé són estàndard es canvien abans de l'entrada en producció del sistema.
		CBCS 4-3: Ús dedicat de comptes d'administració	Els comptes d'administració només es realitzen per a les tasques que són estrictament necessàries.
		CBCS 4-4: Mecanismes d'autenticació	Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes.
		CBCS 4-5: Auditoria i control	L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades.

Control	Objectiu del control	Subcontrol	
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 per mitjà de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
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 fa un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades, o bé són transmeses a través de la xarxa.
CBCS 8 Compliment normatiu i governança de ciberseguretat	L'entitat compleix els requisits legals i reglamentaris que li són aplicables i té establida una adequada governança de ciberseguretat.	CBCS 8-1: Compliment de l'ENS	L'entitat compleix els requeriments establits en l'ENS.
		CBCS 8-2: Compliment de la LOPD/RGPD	L'entitat compleix els requeriments establits en la LOPD/RGPD.
		CBCS 8-3: Compliment de la Llei 25/2013	L'entitat compleix els requeriments establits en la Llei 25/2013, de 27 de desembre.

Avaluació dels resultats del treball

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

Subcontrols

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

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

Quadre 6. Avaluació dels subcontrols

Avaluació	Descripció
Control efectiu	Cobreix al 100% l'objectiu de control i: - 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 *Guía de seguridad CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 7. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El control no s'està aplicant en aquest moment.
N1 Inicial / ad hoc	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *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 és de categoria ALTA si alguna de les seues dimensions de seguretat aconsegueix el nivell ALT.

b) Un sistema d'informació és 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 és 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:[11]

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

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

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

[11] *Guia de seguretat de les TIC. CCN-STIC 824. Informe Nacional de l'Estat de Seguretat dels Sistemes TIC.*

Indicadors globals

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

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

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

Governança de ciberseguretat

A l'efecte d'aquest treball, s'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 manera responsable.[12]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Seguiment de les recomanacions

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

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

Quadre 8. Situació de les recomanacions

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

En el quadre 2 es mostren les recomanacions 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 a la situació en què es trobava el control en la nostra auditoria anterior. S'ha contractat un servei d'auditoria que inclourà la revisió i actualització de tots els procediments.

L'Ajuntament va adjudicar, a principi de 2021, un contracte de renovació d'equips d'usuari. El departament TIC ha realitzat una revisió completa dels seus actius i l'actualització de l'inventari; a més, ha desenvolupat guies d'instal·lació per al nou equipament i utilitza fulls de lliurament que detallen qui són els responsables de cada equip.

Es disposa d'un nou sistema MDM per a la gestió i administració de dispositius mòbils, però ens han indicat que en el moment de la revisió aquest sistema no està completament operatiu ni integra la totalitat de dispositius existent en l'entitat.

Sobre el control de dispositius físics no autoritzats, s'han aplicat determinades mesures de seguretat per a impedir les connexions no autoritzades, però aquestes tenen una efectivitat molt limitada, per la qual cosa mantenim la nostra recomanació sobre aquest tema.

El nivell de control sobre l'inventari i el control d'actius físics és insuficient, i la seua valoració global aconsegueix un **índex de maduresa del 46,1%,** 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 57,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 44,1%; per tant, s'ha produït una lleu millora de 2 punts en aquest índex.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

Gestionar activament (inventariar, revisar i corregir) tot el programari, de manera que només es puga instal·lar i executar programari autoritzat i que el no autoritzat siga detectat i s'evite instal·lar-lo i executar-lo.

Situació del control

L'Ajuntament ha realitzat algunes accions que milloren el control sobre l'inventari i el programari autoritzat. No obstant això, han de continuar treballant per a aconseguir els nivells exigits per l'ENS. A més, las accions realitzades per al control de programari no es troben establides en un procediment actualitzat i formalment aprovat.

El departament TIC ha substituït la majoria d'equips d'usuari els sistemes operatius dels quals estaven obsolets i sense suport del fabricant per mitjà del projecte d'actualització descrit en el CBCS 1. No obstant això, continua havent-hi sistemes obsolets connectats a la xarxa corporativa que, encara que no és un nombre significatiu, representen un risc i haurien d'actualitzar-se.

Encara que no es disposa de cap aplicació que impedisca totalment l'execució de programari no autoritzat en els sistemes de l'entitat, hi ha mesures compensatòries que proporcionen una certa efectivitat del control:

- Aplicació de polítiques de seguretat als equips d'usuari per a impedir instal·lacions a usuaris sense privilegis d'administració.

- Llista d'aplicacions que cal instal·lar en tots els equips inclosa en els procediments interns del departament TIC. Encara que no és una llista blanca formalment aprovada, els procediments interns del departament TIC inclouen la llista d'aplicacions per als equips nous, que defineixen els tècnics d'acord amb les necessitats de l'organització.

- El programari d'inventari, l'antivirus i el tallafoc tenen opcions per a impedir l'execució d'aplicacions no autoritzades, però el bloqueig de programari no autoritzat en aquestes aplicacions no és completament efectiu.

Hi ha accions previstes, com la migració de les bases de dades d'aplicacions crítiques obsoletes o la implantació d'un sistema EDR, que milloraran el control una vegada implantades.

L'Ajuntament no disposa d'un pla de manteniment que descriga la gestió integral de programari, que incloga tant el contractat com la resta utilitzada a l'Ajuntament.

Hi ha un insuficient nivell de control sobre l'inventari i control de programari autoritzat, i l'**índex de maduresa és 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 2 del 70,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 51,3%, per tant, s'ha produït una lleu millora de 5,2 punts en aquest índex.

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

Objectiu del control

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

Situació del control

L'Ajuntament ha realitzat determinats canvis en el control de vulnerabilitats; no obstant això, l'índex de maduresa del control no reflecteix aquestes millores. Això és pel fet que en un dels subcontrols avaluats no es realitzen les accions que garantisquen l'efectivitat del control.

L'Ajuntament ha realitzat el desplegament de l'eina microCLAUDIA del CCN en els sistemes i equips d'usuari de l'entitat, eina que proporciona protecció contra codi nociu de tipus *ransomware*, que a més s'inclou en la maqueta d'equips d'usuari. També han desplegat la solució CARMEN, oferida pel CCN-CERT i gestionada pel CSIRT-CV, que alerta per mitjà d'informes periòdics d'anomalies en la xarxa. Els tècnics del departament d'informàtica apliquen mesures concordes amb els resultats d'aquests informes, encara que no documenten les actuacions en l'eina de *ticketing*. Les alertes de CARMEN s'envien al correu del responsable, si bé haurien d'arribar a tots els integrants del departament.

Una de les bones pràctiques dutes a terme pel departament TIC és la contractació d'una empresa que realitza la vigilància del sistema SIEM de l'Ajuntament i que informa periòdicament de les deficiències detectades i manté reunions per a esmenar-les, encara que s'ha implantat durant l'exercici 2022 i no s'ha valorat per a aquest informe per no trobar-se dins del període auditat.

Una de les mancances detectades durant la revisió és la no utilització d'un gestor centralitzat per a l'aplicació de pedaços i actualitzacions. Encara que hi ha controls compensatoris (aplicació de directives per a forçar els equips a buscar i descarregar actualitzacions o la instal·lació manual d'aquestes), la inexistència d'un gestor centralitzat impedeix tindre una visió global del conjunt de sistemes, i hi ha un desconeixement d'aquells que no s'estan actualitzant.

Encara que algunes de les accions relacionades amb el control de vulnerabilitats estaven establides en un procediment aprovat, l'Ajuntament ha d'actualitzar els procediments amb les accions dutes a terme.

La valoració global sobre aquest control aconsegueix un **índex de maduresa del 59,1%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 3 del 73,9%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 53,6%, per tant, s'ha produït una lleu millora de 5,5 punts en aquest índex.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

L'Ajuntament ha realitzat determinats canvis en l'ús controlat dels privilegis administratius respecte de la situació observada en la revisió anterior, però totes les accions s'han de recollir en procediments formalment aprovats.

El departament TIC ha revisat els usuaris administradors en els sistemes crítics i ha eliminat els usuaris genèrics no nominatius i els comptes no utilitzats, de manera que ha esmenat la deficiència detectada en 2019.

A més de la revisió d'usuaris en els diferents sistemes, el departament TIC ha establit, per a cada un dels administradors, l'ús de comptes amb diferents nivells de privilegis, que utilitzen en funció del treball que cal realitzar.

El control existent sobre els usuaris administradors s'ha d'establir en un procediment formalment aprovat i les accions implantades (identificació, control d'accessos, mecanismes d'autenticació, registre d'accions, etc.) han d'aplicar-se de manera homogènia en tots els sistemes i aplicacions de l'entitat.

Hi ha un cert nivell de control sobre els comptes amb privilegis administratius i la valoració global del control representa un **índex de maduresa del 61,7%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment d'aquest CBCS 4 del 77,1%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 58,6%, per tant, s'ha produït una lleu millora de 3,1 punts en l'índex de maduresa del control.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

Establir una configuració base segura del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors, i gestionar-la activament, utilitzant un procés de gestió

de canvis i configuracions rigorós, per a previndre que els atacants exploten serveis i configuracions vulnerables.

Situació del control

El departament TIC ha desenvolupat un procediment que descriu les accions realitzades per a la instal·lació d'equips nous, que inclou aspectes relacionats amb les configuracions segures de programari i maquinari, encara que és un document intern del departament i no està formalment aprovat.

El procediment anterior descriu els treballs sobre les màquines prèviament a la seua entrada en producció, i inclou aspectes de seguretat com ara revisar que les polítiques de seguretat s'apliquen correctament o la implantació de la seguretat millorada amb una aplicació pròpia de la marca dels equips. No obstant això, aquesta funcionalitat únicament està habilitada en els equips de nova adquisició.

El departament TIC disposa de repositoris on s'emmagatzemen configuracions d'alguns sistemes, com els tallafocs o *switches*, i a més el procediment de còpies de seguretat estableix la ubicació, responsables i periodicitat d'aquestes còpies.

No es disposa de sistemes per al monitoratge de canvis no autoritzats en les configuracions ni les accions dutes a terme per a impedir canvis no autoritzats estan documentades i aprovades en un procediment de gestió de canvis.

Hi ha, per tant, un deficient nivell de control en l'aplicació de configuracions segures en dispositius i programari, de manera que s'han de dedicar esforços i recursos per a millorar el control. La valoració global del control aconsegueix un **índex de maduresa del 25,0%**, que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 31,3%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 12,4%; per tant, s'ha produït una millora de 12,6 punts en l'índex de maduresa del control.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

L'Ajuntament tenia habilitats, durant el nostre treball anterior d'auditoria, els registres d'activitat en els sistemes revisats i existia un cert nivell de control en funcionament, però

els controls s'aplicaven de manera informal i no estan establits en un procediment formalment aprovat.

Encara que l'Ajuntament ha fet canvis que milloren significativament la situació observada durant la nostra auditoria anterior, aquests canvis s'han implantat en 2022, per la qual cosa no han sigut considerats quan s'ha calculat l'índex de maduresa del control.

S'ha contractat la implantació d'un sistema SIEM que inclou part dels sistemes de l'entitat, i la formació i report d'anomalies per part de l'empresa adjudicatària. El servei contractat és 24/7[17] i l'empresa genera informes mensuals que s'analitzen en reunions amb el personal del departament TIC, que corregeixen les vulnerabilitats detectades. Aquestes vulnerabilitats s'introdueixen automàticament en el gestor de *tickets* com a incidències. A més, el departament TIC documenta les reunions, contractes i actes en un gestor d'expedients.

El departament TIC ha habilitat el registre de les accions en el programari utilitzat per a la gestió d'usuaris administradors que comparteixen els membres del departament TIC.

L'Ajuntament segueix sense un procediment aprovat que definisca una política per als registres d'auditoria (sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés als *logs*, etc.).

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 60,0%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 6 del 75,0%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 60,0%; per tant, a data 31 de desembre de 2021, no s'ha produït cap millora respecte de la situació anterior.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

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

Situació del control

L'Ajuntament ha fet alguns canvis respecte a la situació observada en la revisió anterior. Encara que s'han aplicat algunes accions de millora, hi ha circumstàncies que fan que el control no aconseguisca el mateix nivell de maduresa que aconseguia en 2019.

[17] 24 hores, 7 dies a la setmana.

Durant el nostre treball d'auditoria anterior vam observar l'existència d'un bon nivell de control sobre les còpies de seguretat de dades i sistemes, atés que es realitzaven quasi totes les accions avaluades: realització de còpies, realització de determinades proves de restauració planificades, protecció de còpies de seguretat i el procés estava correctament documentat. No obstant això, durant aquest treball, hem observat que alguna de les pràctiques que en aquell moment es va valorar com a efectiva ha deixat de dur-se a terme. Per exemple, han deixat d'utilitzar-se còpies de seguretat desconnectades. Encara que hi ha controls compensatoris (els servidors de còpia únicament són accessibles des de certes màquines), hi ha un cert nivell de risc que no existia amb les còpies de seguretat desconnectades.

Encara que l'objectiu de l'Ajuntament és implantar un centre *offline* d'emmagatzematge, que s'ha inclòs en l'"expedient per a la contractació del subministrament, instal·lació i posada en marxa d'un centre d'operacions de ciberseguretat i aplicació de les mesures de protecció per a compliment de l'ENS, finançat pel pla de recuperació, transformació i resiliència - Unió Europea Next Generation", en data 31 de desembre de 2021 aquesta millora no es trobava implantada i no s'ha considerat en el càlcul de l'índex de maduresa en aquesta data.

Addicionalment, una de les mancances detectades és la revisió de l'estat de les còpies únicament per part d'un dels tècnics responsables. Aquesta pràctica comporta el risc de no realitzar correctament les còpies i no advertir-ho en cas d'absència de la persona que habitualment fa el treball.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 74,8%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 93,5%**, la qual cosa implica un empitjorament respecte de la nostra auditoria anterior.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 80,0%; per tant, ha disminuït en 5,2 punts l'índex de maduresa del control.

CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT

Objectiu del control

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

Situació del control

Compliment de l'ENS

No s'han realitzat les auditories previstes en l'article 34 del Reial Decret 3/2010 ni, en conseqüència, s'han publicat 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.

El nostre informe d'auditoria dels CBCS de l'any 2019 es va donar a conéixer al Ple de l'Ajuntament en sessió ordinària celebrada el 28 d'octubre de 2020, en el qual es va acordar l'inici d'un expedient de contractació per a esmenar els incompliments legals detectats. Aquesta contractació, adjudicada al juliol de 2022, inclou un projecte destinat al compliment de l'ENS.

A més dels incompliments advertits en el nostre treball anterior, l'Ajuntament no ha emplenat i remés l'Informe de l'Estat de la Seguretat (Informe INES) corresponent a l'exercici fiscalitzat.

Compliment de l'RGPD

Quant al compliment en matèria de protecció de dades personals, durant la revisió realitzada l'any 2019 detectem deficiències significatives, com la inexistència del rol del DPD a l'Ajuntament, absència del registre d'activitats del tractament o d'una anàlisi de riscos en aquest camp, entre altres.

Malgrat les nostres recomanacions de 2019, l'Ajuntament ha continuat incomplint la normativa en aquesta matèria, per la qual cosa ha rebut un avís de l'AEPD per a esmenar la seua situació.

En la licitació per al compliment de l'ENS adjudicada en 2022, l'Ajuntament ha inclòs la contractació de serveis relacionats amb la protecció de dades de caràcter personal, com el nomenament del DPD, realitzat en 2022, encara que pendent de notificar a l'AEPD.

Continuen existint, per tant, incompliments significatius que s'han d'esmenar:

- No s'ha finalitzat i publicat el registre d'activitats de tractament, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.

- No s'han realitzat les anàlisis de riscos sobre els tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.

- No s'han aplicat les mesures organitzatives i tècniques necessàries per a protegir les dades personals, requerides per l'article 24.1 de l'RGPD.

- No s'han executat auditories de compliment en matèria de protecció de dades.

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

Compliment de la legalitat del registre de factures

No s'han realitzat les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.

Indicadors

En resum, i encara que es treballa per a esmenar la situació, la valoració global sobre el compliment dels aspectes de legalitat a data 31 de desembre de 2021 ha empitjorat respecte a l'informe emés l'any 2019 (20,0%), de manera que l'Ajuntament aconsegueix un **índex de maduresa del 18,0%**, 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 22,5%**.

La disminució en l'índex de maduresa respecte de la situació observada durant la nostra auditoria anterior és deguda al fet que, a més de continuar vigents els incompliments observats en el nostre treball anterior, l'Ajuntament no ha emés l'informe INES corresponent a l'exercici fiscalitzat.

Com ja s'ha assenyalat, per a esmenar la situació, l'Ajuntament ha adjudicat al juliol de 2022 un contracte per a fer les tasques d'adequació a l'ENS i a la normativa de protecció de dades de caràcter personal. Les millores introduïdes per mitjà d'aquest contracte no han sigut considerades per al càlcul dels índexs de maduresa per haver-se realitzat amb posterioritat al 31 de desembre de 2021.

Governança de la ciberseguretat

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

Hi ha un cert nivell de compromís i conscienciació amb la ciberseguretat per part dels membres del departament TIC i dels òrgans superiors de l'Ajuntament, que s'observa en aspectes com:

- L'Ajuntament disposa d'una política de seguretat aprovada, que es completa amb un marc normatiu i procedimental, però aquesta documentació no està actualitzada.

- L'existència de suport al departament TIC, tant polític com en forma de recursos econòmics i humans.

No obstant això, determinades circumstàncies indiquen que la governança no pot considerar-se efectiva. Basem aquesta afirmació en les mancances rellevants següents:

- La falta de lideratge en matèria de ciberseguretat dels òrgans superiors de l'Ajuntament.

  L'organització no disposa de plans ni d'estratègies elaborades i aprovades pels òrgans superiors en relació amb la seguretat de la informació, ni impulsa les mesures de

seguretat necessàries, incloent-hi la formació i conscienciació dels seus treballadors. Són els membres del departament TIC, per pròpia iniciativa i sense el suport del comité de seguretat de la informació, els qui implanten les mesures necessàries relacionades amb la ciberseguretat i impulsen el compliment de la normativa en aquesta matèria.

- La falta d'atenció als incompliments legals identificats durant el nostre informe d'auditoria anterior. A data 31 de desembre de 2021, l'Ajuntament seguia sense nomenar el DPD ni atendre cap dels incompliments que assenyalàvem. Al juliol de 2022 l'Ajuntament ha contractat un "servei d'auditoria de revisió i adequació a l'ENS i normativa de protecció de dades personals".

- La necessitat que el comité de seguretat de la informació funcione de manera efectiva, òrgan imprescindible per a coordinar la seguretat de la informació entre les diferents àrees de l'Ajuntament.

  És en el comité de seguretat on s'han de prendre les decisions concretes en matèria de seguretat de la informació, aprovant les mesures pertinents i impulsant les accions que cal dur a terme. Encara que aquest òrgan està definit en la política de seguretat aprovada per l'Ajuntament, no exerceix les seues funcions de manera efectiva. El comité ha de reunir-se periòdicament i, en una entitat de les dimensions de l'Ajuntament de Paterna i atesa la complexitat dels seus sistemes, recomanem que es faça almenys mensualment.

- La política de seguretat de la informació i les normes i procediments de seguretat no estan actualitzades.

  L'Ajuntament disposa de política de seguretat de la informació aprovada en 2013, que a més es completava amb un marc normatiu (ús correcte d'equips, serveis, instal·lacions, aplicacions autoritzades, control físic d'accessos, etc.) i procedimental (procediments que detallen com es fan les tasques habituals, responsables, etc.). No obstant això, aquesta documentació ha de ser actualitzada amb els processos actualment implantats.

- Alguns dels rols en matèria de seguretat no estan correctament definits.

  El rol de responsable de seguretat es correspon amb la responsable del departament TIC i això és incompatible. D'acord amb l'ENS i la guia CCN-STIC 801, el responsable de la seguretat "ha de ser una persona física, jeràrquicament independent del responsable del sistema". Si el responsable de seguretat està legitimat per a determinar, supervisar i pronunciar-se sobre la idoneïtat de les mesures de seguretat adoptades, aquest rol no pot recaure sobre la persona encarregada de la seua implantació i explotació diària.

- Falta d'agilitat administrativa, particularment en la gestió de les contractacions, que disminueix la capacitat de reacció davant situacions de risc i limita les oportunitats de millora.

APÈNDIX 3
Bones pràctiques destacables

Introducció

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

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

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

Implantació d'una eina SIEM

El registre d'accions dels diferents sistemes i dispositius és recollit per l'eina d'analítica de *logs* implantada a aquest efecte, que a més de l'anàlisi de *logs* detecta comportaments anòmals per mitjà de la correlació d'esdeveniments.

L'eina SIEM és revisada 24/7 per una empresa contractada a aquest efecte, que revisa diàriament i emet informes sobre l'estat dels sistemes de l'Ajuntament. A més, es mantenen

reunions periòdiques entre els tècnics del departament TIC i l'empresa, en les quals es revisen les incidències detectades i es proposen correccions, a més de registrar-se en actes totes les decisions.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

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

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

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

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

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

Cibervigilància / Vigilància digital: Vigilància digital és un servei de detecció d'amenaces i rastreig d'informació sensible a través d'internet basat en intel·ligència artificial que facilita a les empreses adequar la seua estratègia de negoci i millorar el procés de presa de decisions.

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

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

EDR:[18] Un sistema EDR, sigla en anglés d'*endpoint detection and response*, és un sistema de protecció dels equips i infraestructures de l'empresa. Combina l'antivirus tradicional juntament amb eines de monitoratge i intel·ligència artificial per a oferir una resposta ràpida i eficient davant els riscos i les amenaces més complexes.

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

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i han de descriure: *a*) l'ús correcte d'equips, serveis i instal·lacions; *b*) el que es considerarà ús indegut, i *c*) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat ha d'estar a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, ha d'estar disponible en la intranet corporativa de l'entitat a través d'una adreça URL. La normativa de seguretat de cada entitat deriva i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desenvolupament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

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

Política de seguretat de la informació: És un document d'alt nivell que defineix el que significa *seguretat de la informació* en una organització d'acord amb l'article 11 del Reial Decret 3/2010 i articula la gestió continuada de la seguretat. Ha de ser aprovada pel president o presidenta o la junta de govern d'una entitat local o el consell d'administració d'una societat. Ha d'estar accessible per a tots els membres de l'organització i redactada de manera senzilla, precisa i comprensible. Convé que siga breu, i que deixe els detalls tècnics per a altres documents més precisos que ajuden a dur a terme el que s'hi proposa: normes de seguretat i procediments de seguretat.

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

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

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

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir amb el responsable del sistema, la responsable de seguretat i una representant designada per la secretària general, 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 11 de gener de 2023, 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 Paterna 2019_val - SEFYCU 3783217

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 3RFN LJY3 FP43 QTJE

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 - 17/01/23 07:45 VICENT CUCARELLA TORMO