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 BENIDORM DE L'ANY 2019

Situació a 31 de desembre de 2021

RESUM

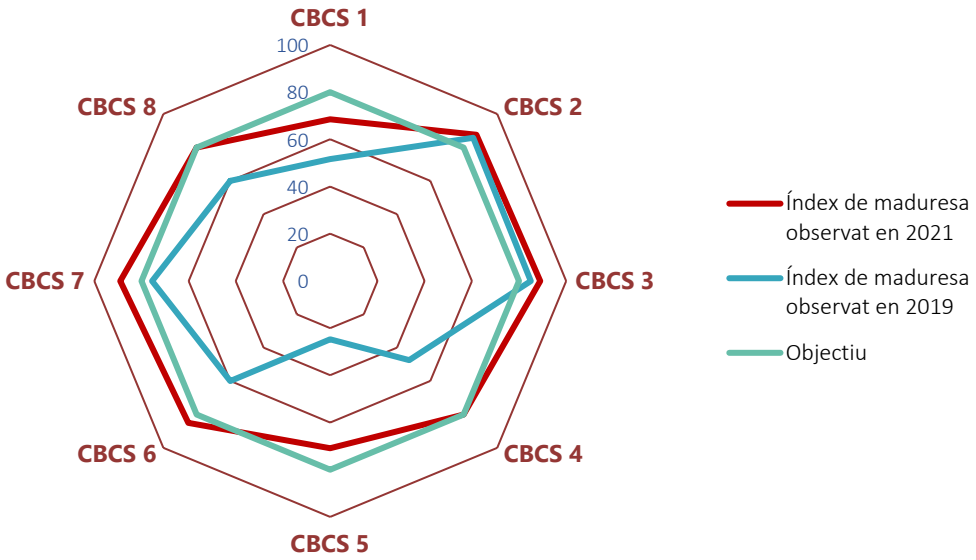
La transformació digital que estan experimentant totes les administracions públiques i la seua interconnexió a través de complexes xarxes informàtiques les exposa de manera cada vegada més intensa a amenaces provinents del ciberespai. Això origina un increment dels riscos associats als sistemes d'informació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

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

Conclusions

L'Ajuntament ha realitzat progressos significatius des de la nostra auditoria anterior i s'han atés la majoria de les nostres recomanacions.

L'índex de maduresa general dels controls bàsics de ciberseguretat aconsegueix l'objectiu establit i mostra un valor del 81,4%, que millora substancialment el 61,3% registrat en la nostra auditoria de 2019.



Hem constatat que l'Ajuntament té establida una acceptable governança de la ciberseguretat. Els òrgans superiors de l'Ajuntament (alcalde i/o la Junta de Govern) són els responsables del sistema de control, 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 ciberresiliencia de l'entitat.

No obstant això, és necessari que el comité de seguretat, com a òrgan col·legiat, es reunisca periòdicament a fi de conéixer l'estat de la seguretat de la informació de l'Ajuntament i prendre les decisions convenients.

Així mateix, la nostra revisió ha posat de manifest un raonable grau de compliment de les normes legals relacionades amb la seguretat de la informació, encara que en l'Informe s'assenyalen diversos aspectes pendents de millora sobre els quals s'ha d'actuar, com la planificació i execució d'auditories de compliment de l'ENS.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament. En particular, aconsellem millorar els controls que impedeixen la connexió de dispositius no autoritzats a la xarxa corporativa i desenvolupar un procés de gestió continuada de la configuració sobre els sistemes crítics 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 llegir-lo per a conéixer el veritable abast del treball realitzat.

Informe de seguiment de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Benidorm 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 12 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 Benidorm, 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 analitzats.

La necessitat d'una ciberhigiene adequada

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

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

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

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

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

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

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

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

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

Per a això, hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica, així 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 del treball.

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

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

4. CONCLUSIONS

L'Ajuntament ha realitzat progressos significatius des de la nostra auditoria anterior i s'han atés la majoria de les nostres recomanacions. L'índex de maduresa general dels controls bàsics de ciberseguretat aconsegueix l'objectiu establit

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 81,4%**, que es correspon amb un nivell de maduresa *N3, procés definit,* és a dir, els processos de control implantats estan estandarditzats i formalment documentats.

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

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

Control	2019			2021		
	Índex de maduresa	Nivell de maduresa	Índex de compli-ment	Índex de maduresa	Nivell de maduresa	Índex de compli-ment
CBCS 1 Inventari i control de dispositius físics	*51,6%*	*N2*	*64,5%*	68,5%	N2	85,6%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	*85,8%*	*N3*	*100%*	87,7%	N3	100%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	*85,0%*	*N3*	*100%*	89,0%	N3	100%
CBCS 4 Ús controlat de privilegis administratius	*47,4%*	*N1*	*59,2%*	81,0%	N3	100%
CBCS 5 Configuracions segures del programari i maquinari	*24,7%*	*N1*	*30,9%*	70,9%	N2	88,6%
CBCS 6 Registre de l'activitat dels usuaris	*60,0%*	*N2*	*75,0%*	85,0%	N3	100%
CBCS 7 Còpies de seguretat de dades i sistemes	*75,5%*	*N2*	*94,3%*	89,0%	N3	100%
CBCS 8 Compliment normatiu i governança de ciberseguretat	*60,0%*	*N2*	*75,0%*	80,0%	N3	100%
General	61,3%	*N2*	74,9%	81,4%	N3	96,8%

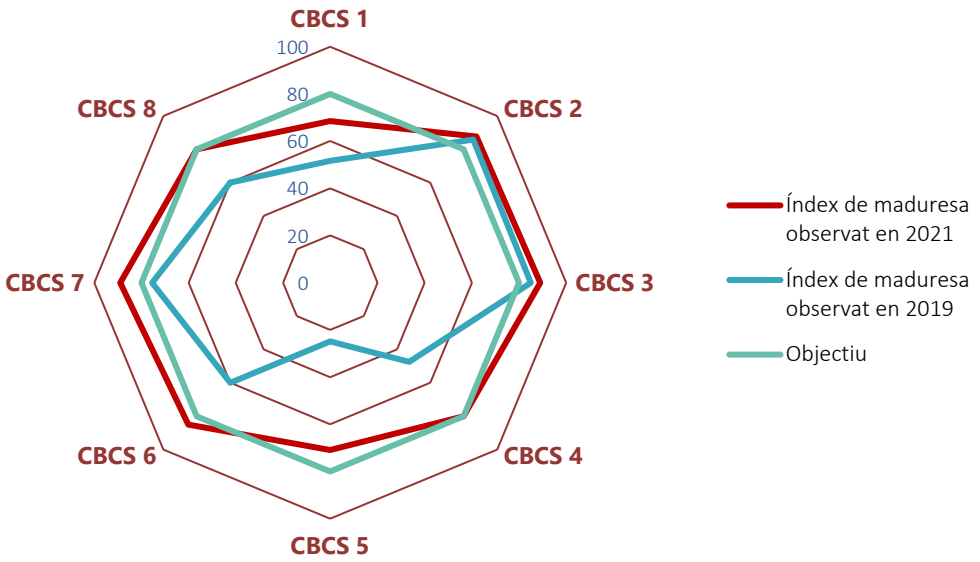
L'índex de compliment dels CBCS resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*.

L'índex de compliment general és la mitjana dels índexs individuals (amb límit individual en el 100%) i aconsegueix el 96,8%, que ha millorat des del 74,9% del nostre informe anterior. La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una millora en tots els controls.

A pesar de la millora experimentada, hi ha controls que no arriben als nivells exigits per l'ENS per a la protecció dels sistemes d'informació (CBCS 1, CBCS 5). En l'apartat 5 es realitzen les recomanacions pertinents amb aquesta finalitat.

D'una manera més sintètica i gràfica, la situació observada dels controls queda reflectida en el gràfic 1, tant en aquesta auditoria com en 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 Benidorm té establida una governança acceptable de la ciberseguretat i ha de mantindre el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació

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

Hem pogut verificar l'existència d'un adequat nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament, juntament amb uns adequats processos de gestió. No obstant això, és necessari que el comité de seguretat, com a òrgan col·legiat, es reunisca periòdicament a fi de conéixer l'estat de la seguretat de la informació de l'Ajuntament i prendre les decisions convenients. Tot això ens permet afirmar que la governança de ciberseguretat aconsegueix un nivell acceptable.

Existeix un grau raonable d'adequació a la normativa relativa a la seguretat de la informació

La revisió del compliment de legalitat en matèria relacionada amb la seguretat de la informació ha posat de manifest un nivell raonable de compliment de la normativa. No obstant això, en l'apartat 5 s'assenyalen diversos aspectes pendents de millora sobre els quals s'ha d'actuar per a esmenar-los ràpidament.

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

Per a esmenar les deficiències de control identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 4 anterior, reformulem les recomanacions que es van efectuar en l'auditoria de 2019, considerant les millores realitzades des de llavors. L'Ajuntament 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 han d'adoptar-se.

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

1. Millorar les solucions actualment implantades per a impedir la connexió de dispositius no autoritzats a la xarxa corporativa i establir aquestes mesures en un procediment aprovat formalment.

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

2. La recomanació de l'informe de 2019 s'ha implementat.

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

3. La recomanació de l'informe de 2019 s'ha implementat.

4. La recomanació de l'informe de 2019 s'ha implementat.

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

5. La recomanació de l'informe de 2019 s'ha implementat.

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

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

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

7. La recomanació de l'informe de 2019 s'ha implementat.

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

8. La recomanació de l'informe de 2019 s'ha implementat.

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:

   - Adoptar les mesures de seguretat descrites en la declaració d'aplicabilitat.
   - Realitzar les auditories de seguretat previstes en el Reial Decret 3/2010.
   - Publicar en la seu electrònica la certificació 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.

10. La recomanació de l'informe de 2019 s'ha implementat.

Seguiment de recomanacions anteriors

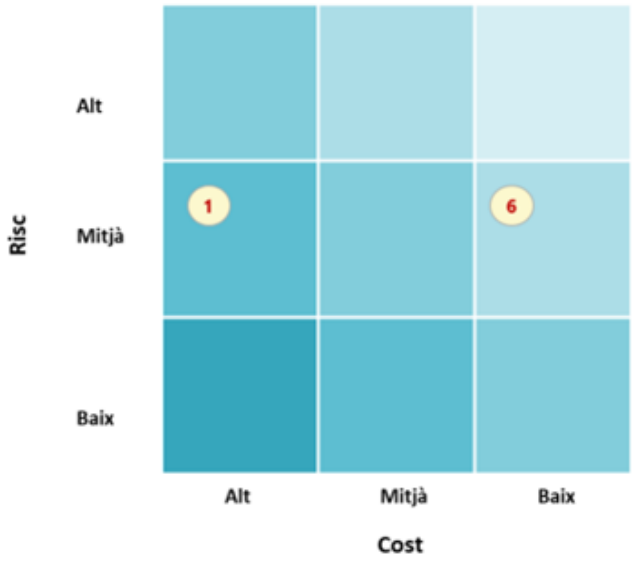
Hem realitzat un seguiment de les recomanacions efectuades en l'informe d'auditoria de l'any 2019.

Tal com es mostra en el quadre 2, de les deu recomanacions realitzades en aquell informe, set han sigut ateses, dues ho han sigut només parcialment i una no ha sigut atesa.

Priorització de les recomanacions

A fi que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial que cal mitigar** i **cost estimat de la implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2019, adaptant la relació risc/cost de cada recomanació i considerant les millores realitzades des de la revisió anterior. No s'hi inclou el punt 9 anterior, ja que és una mesura de compliment obligat.

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



Actuacions en curs

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

Enumerem a continuació aquelles actuacions que es troben en execució i que per la seua rellevància han de ser destacades en l'Informe:

- Desplegament d'una solució MDM (*mobile device management*). L'Ajuntament es troba en fase d'implantació d'un sistema de control de dispositius mòbils.

- Contractació de serveis especialitzats en ciberseguretat. L'Ajuntament es disposa a incloure entre les seues accions una auditoria de *hacking* des de dins de la seua pròpia xarxa, establint com a objectius els seus propis serveis i sistemes crítics.

- Desplegament de serveis i eines proporcionats pel CCN i el CSIRT-CV, que se sumen als serveis ja implantats en l'organització (LUCÍA, GLORIA):

    - CARMEN, solució desenvolupada amb l'objectiu d'identificar el compromís de la xarxa d'una organització davant amenaces persistents avançades. Eina en fase

d'implantació a data 31 de desembre de 2021 però implantada íntegrament a data d'aquest informe.

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

- MicroCLAUDIA, que proporciona protecció contra codi nociu de tipus *ransomware*.[3] Eina en fase d'implantació a data 31 de desembre de 2021 però implantada íntegrament a data d'aquest informe.

- REYES, que permet realitzar investigació i anàlisi sobre ciberincidents de manera àgil i ràpida. Consisteix en un metacercador d'informació de diverses fonts especialitzades en ciberamenaces, que està integrat amb eines d'anàlisi del CCN-CERT. L'Ajuntament rep informes periòdics del CSIRT-CV amb incidents de seguretat relacionats amb els dominis i correus corporatius (vigilància digital).

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

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

Quadre 2. Seguiment de recomanacions

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
1	Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.	Encara que s'han implantat mesures per a restringir l'accés de dispositius no autoritzats a la xarxa corporativa, el control es pot millorar. Addicionalment, totes les mesures implantades a aquest efecte han de recollir-se en un procediment formalment aprovat.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.
2	Actualitzar el procediment per a la gestió integral del programari de l'entitat, considerant: - L'elaboració de llistes de programari autoritzat (llistes blanques) i la realització de revisions periòdiques del programari instal·lat. - La definició d'un pla de manteniment del programari que considere de manera integral la totalitat del programari utilitzat, incloent-hi tant el gestionat per mitjà de licitacions i clàusules contractuals, com la resta de programari utilitzat a l'Ajuntament.	S'ha elaborat un procediment, que es troba aprovat, en funcionament i s'ha destinat personal a aquest efecte.	**Aplicada**	S'elimina la recomanació feta en 2019.
3	Implantar una eina d'escaneig de vulnerabilitats en la xarxa, com a mesura addicional a les proves de penetració. S'hauran de dur a terme i documentar revisions periòdiques de vulnerabilitats. Aquest procés haurà de ser afegit al procediment de seguretat perimetral.	S'ha implantat una eina SIEM d'anàlisi en temps real que gestiona una empresa experta. S'emeten informes diaris que són revisats i es realitzen accions d'acord amb les vulnerabilitats detectades.	**Aplicada**	S'elimina la recomanació feta en 2019.
4	Completar el document de seguretat perimetral ampliant la documentació referent al procés de solució de vulnerabilitats, considerant: - Anàlisi prèvia a l'entrada en producció de sistemes. - Priorització basada en l'anàlisi de riscos. - La resolució i la documentació de les vulnerabilitats, identificant dates, prioritat, responsable, solució, etc.	Totes les accions relacionades amb la gestió de vulnerabilitats s'han establit en el procediment aprovat a aquest efecte. S'estableixen responsabilitats d'acord amb el tipus de vulnerabilitat detectada.	**Aplicada**	S'elimina la recomanació 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
5	Formalitzar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga: - L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió hauran de realitzar-se amb usuaris nominatius. - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes. - La utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives). - La política d'autenticació que cal aplicar a aquest tipus de comptes.	S'han revisat els usuaris amb privilegis d'administració de tots els sistemes de l'entitat i s'han eliminat els usuaris l'existència dels quals no es trobava justificada. Els administradors tenen diferents perfils d'administració, depenent del tipus de tasques que cal realitzar. Totes les mesures implantades han sigut establides en el procediment aprovat a aquest efecte.	**Aplicada**	S'elimina la recomanació 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 CCN. Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha d'incloure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració.	S'ha elaborat i aprovat un procediment a aquest efecte que descriu la configuració de plantilles, l'ús de guies de seguretat, etc. El departament ha implantat una eina que monitora i detecta canvis en equips, no obstant això, no s'ha definit un grup de sistemes crítics sobre els quals realitzar revisions periòdiques de canvis de configuració.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
7	Aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat d'usuari, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*.	S'ha elaborat i aprovat un procediment que descriu tots els aspectes recomanats. Addicionalment, els registres i la correlació d'aquests es revisen regularment i es realitzen accions amb les incidències detectades.	**Aplicada**	S'elimina la recomanació feta en 2019.
8	Complementar el procés de gestió de còpies de seguretat per mitjà de l'establiment d'un nivell addicional de protecció, de manera que hi haja còpies de seguretat en suport desconnectat o no accessibles de manera directa a nivell de xarxa.	El departament ha implementat el funcionament de còpies immutables. Addicionalment, s'ha auditat aquesta característica per a verificar-ne l'efectivitat i s'han separat les còpies dels usuaris del domini.	**Aplicada**	S'elimina la recomanació feta en 2019.
9	Implantar les mesures necessàries per a donar compliment als requisits de l'RD 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de: - Adoptar les mesures de seguretat de la declaració d'aplicabilitat. - Realitzar les auditories de seguretat previstes en l'article 34. - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.	Sense variació.	**No aplicada**	Es manté la redacció.
10	En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la LO 3/2018, de 5 de desembre. En particular ha de: - Fer públic per mitjans electrònics l'inventari de les seues activitats de tractament per a donar compliment a l'article 31.2 de la Llei Orgànica 3/2018. - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD. - Planificar i executar auditories de compliment en matèria de protecció de dades.	Es realitzen auditories anuals per àrees i es fan treballs regulars en aquest camp. S'emet un informe anual amb les actuacions en aquesta matèria.	**Aplicada**	S'elimina la recomanació feta en 2019.

APÈNDIX 1
Metodologia aplicada

Introducció

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

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

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

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

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

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

[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 Benidorm. Exercici 2019, així com obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això n'hem avaluat tant el disseny[5] com l'eficàcia operativa[6] per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport. També hem revisat el compliment de la normativa bàsica relativa a la seguretat de la informació.

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

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada dels huit CBCS revisats en l'auditoria de l'any 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 a revisar –la gran amplitud, complexitat i diversitat dels sistemes d'informació d'un ens local de grans dimensions– ha sigut necessari delimitar i concretar quins sistemes s'havien d'analitzar. En aquest sentit, hem analitzat les aplicacions que suporten els processos de gestió comptable i pressupostària i la gestió tributària i recaptadora, així com els controls que tenen implantats.

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

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

Metodologia

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

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

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

Hem avaluat la situació dels CBCS utilitzant el model de nivell de maduresa dels processos, definit en l'apèndix 1 de la guia esmentada, ja que, a més de ser un sistema àmpliament

acceptat, permet establir objectius, realitzar comparacions entre entitats diferents i veure'n l'evolució al llarg del temps.

La guia pràctica de fiscalització dels OCEX 5313

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

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

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

[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 fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.[10]

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

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

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

[10] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices*, 2017.<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 què s'especifica amb el màxim detall els aspectes comprovats en cada control.

Quadre 5. Els CBCS i els seus subcontrols

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

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

Avaluació dels resultats del treball

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

Subcontrols

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

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

Quadre 6. Avaluació dels subcontrols

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

Quadre 7. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El control no s'està aplicant en aquest moment.
N1 Inicial / ad hoc	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. *L'eficàcia del procés depén de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.*
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. *Es disposa d'un catàleg de processos que es manté actualitzat. Aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant dels incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor d'allò desconegut (o no planificat).* *L'èxit és més que bona sort: es mereix.* *Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2 i que sí que es gestiona en el nivell 3.*
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. *Es disposa d'un sistema de mesures i mètriques per a conéixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.* *En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.*
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. *El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.* *S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, utilitzant-se com a indicadors en la gestió de la millora dels processos.* *En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes a base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.*

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

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

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indicadors globals

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

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

- L'**índex de compliment** analitza igualment el nivell de maduresa aconseguit, però en relació amb l'exigència aplicable en cada cas, tenint en compte la categoria del sistema.

Governança de ciberseguretat

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

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

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

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

  La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,[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 Benidorm. Exercici 2019.

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

Quadre 8. Situació de les recomanacions

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

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

Comunicació i confidencialitat

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

Atés que la informació utilitzada en l'auditoria té un caràcter sensible i pot afectar la seguretat dels sistemes d'informació, els resultats amb el màxim detall de cada un dels controls revisats només es comuniquen amb caràcter confidencial als responsables de l'Ajuntament perquè puguen adoptar les mesures correctores que consideren necessàries. En aquest informe els resultats es mostren de manera sintètica.

APÈNDIX 2

Situació dels controls bàsics de ciberseguretat

CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

L'Ajuntament complementa l'eina d'inventari analitzada en l'auditoria anterior, OCS Inventory, amb una nova eina, Microsoft Endpoint Configuration Manager 2019, amb què s'ha millorat la gestió de l'inventari d'actius de maquinari.

La nova eina inclou els elements sense agent de xarxa, permet veure canvis significatius en els diferents dispositius, permet la gestió centralitzada del programari, la gestió de pedaços i actualitzacions, el control d'accés a recursos en xarxa, l'aplicació de polítiques, la generació d'informes, etc.

Respecte al control de dispositius físics no autoritzats, el departament gestiona les preses de xarxa deshabilitant els ports en els *switches*, que a més es controlen per *mac*. A més, el departament ha deshabilitat el servei DHCP i restringit l'accés als recursos compartits únicament a elements del domini de l'Ajuntament.

Com que hi ha usuaris que es connecten al sistema d'informació a través d'escriptoris virtualitzats, el departament ha implantat mesures addicionals de protecció per a aquests sistemes, com l'accés amb doble factor d'autenticació o la prohibició de compartir discos durs locals o dispositius USB amb els sistemes remots.

Encara que s'ha millorat el control sobre els dispositius físics no autoritzats, les mesures descrites no estan implantades en tots els dispositius de l'entitat, no es recullen en els procediments aprovats i hi ha millores que garantirien major efectivitat al control.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 68,5%**, 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 1 del 85,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 51,6%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 16,9 punts en l'índex de maduresa del control.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

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

Situació del control

L'Ajuntament ha millorat el control establit sobre el programari amb la implantació de l'eina descrita en el control anterior, Microsoft Endpoint Configuration Manager 2019, que inventaria tot el programari i inclou millores respecte a l'aplicació OCS Inventory revisada durant l'auditoria anterior, com la visualització del programari fora o prop del període de finalització de suport o aspectes com la gestió centralitzada d'aplicacions i pedaços.

L'Ajuntament ha aprovat en 2021 un pla de manteniment de programari que defineix les accions que es realitzen en aquest aspecte i ha destinat personal a aquest efecte.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 87,7%**, que es correspon amb un **nivell de maduresa *N3, procés definit***; és a dir, els processos de control implantats estan estandarditzats i formalment documentats. Això representa un **índex de compliment del CBCS 2 del 100%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 85,8%, que es correspon amb un nivell de maduresa *N3, procés definit*. Per tant, s'ha produït una millora d'1,9 punts en l'índex de maduresa del control.

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

Objectiu del control

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

Situació del control

L'Ajuntament ha fet un pas important en el procés d'identificació i solució de vulnerabilitats, perquè ha implantat una eina de SIEM (*security information and event management*) per a l'anàlisi i correlació d'esdeveniments en temps real, que a més es nodreix de bases de dades de dues plataformes, una pública col·laborativa i una altra privada. Aquesta eina s'ha externalitzat i la gestiona una empresa especialista en la matèria.

Totes les accions encaminades a la gestió de vulnerabilitats –la identificació, priorització i resolució– s'han detallat en un procediment aprovat que estableix la priorització atesa la

criticitat de les vulnerabilitats, i inclou l'actualització de sistemes i dispositius prèviament a l'entrada en producció.

El departament també ha millorat el sistema utilitzat per a aplicar pedaços i actualitzacions, atés que la nova eina implantada, Microsoft Endpoint Configuration Manager 2019, permet la gestió centralitzada de pedaços i actualitzacions.

Finalment, s'ha millorat la situació del control per mitjà d'accions com:

- Dividir resultats dels tests de *hacking* ètic per àrees i establir responsables en cada àrea.
- Implantació d'eines del CCN com CARMEN i MicroCLAUDIA, en fase d'implantació amb data 31 de desembre de 2021, però totalment implantades durant la redacció d'aquest informe.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 89,0%**, que es correspon amb un **nivell de maduresa *N3, procés definit***; és a dir, els processos de control implantats estan estandarditzats i documentats formalment. Això representa un **índex de compliment del CBCS 3 del 100%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 85,0%, que es correspon amb un nivell de maduresa *N3, procés definit*. Per tant, s'ha produït una millora de 4 punts en l'índex de maduresa del control.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

Per a esmenar les deficiències detectades durant el treball d'auditoria anterior, l'Ajuntament ha realitzat les correccions i millores que es proposaven.

S'han eliminat, quan ha sigut possible des del punt de vista tècnic, tots els usuaris no nominatius de tots els sistemes. Únicament s'utilitzen usuaris no nominatius per a processos del sistema que requereixen privilegis, casos en què el nom d'usuari identifica inequívocament el procés que realitza.

S'han eliminat els usuaris per defecte de tots els sistemes i s'ha establit en el procediment aprovat que s'han d'evitar noms d'usuari que suggerisquen que els usuaris tenen privilegis d'administració.

Per a cada administrador de sistemes de l'entitat, el departament utilitza diferents comptes amb diferents nivells de seguretat depenent de les tasques que cal realitzar. A més, hi ha

en un nivell addicional, consistent en la creació d'usuaris administradors per serveis o grups de servidors que s'administren. Aquest nivell addicional aconsegueix segmentar les màquines sobre les quals un administrador té privilegis i disminuir la zona d'exposició en cas d'infeccions per *ransomware*.

S'han establit en els procediments bones pràctiques en la creació i gestió d'usuaris i contrasenyes, com ara, entre altres:

- Canviar els noms d'usuari i les contrasenyes que per defecte venen en els dispositius i sistemes.
- Evitar noms d'usuari que suggerisquen que un usuari té privilegis d'administració.
- Establir, sempre que siga possible i proporcione avantatges de seguretat, una política d'usuari únic, de manera que s'utilitzen els usuaris del domini en els serveis i aplicacions que ho permeten.
- No utilitzar l'usuari administrador del domini, les credencials del qual són conegudes únicament pels responsables i custodiades per la direcció, cosa que s'ha establit en el procediment.

Totes les accions dutes a terme pel departament per a la gestió d'usuaris amb privilegis administratius i canvis de contrasenyes s'han afegit al procediment aprovat.

Encara que s'ha verificat que hi ha controls efectius en cada un dels punts detallats, l'Ajuntament pot continuar millorant en alguns aspectes:

- L'ús de polítiques de contrasenyes en els sistemes que no permeten la integració dels usuaris amb les polítiques del domini.
- Auditoria d'accions d'usuaris administradors extensiva a tots els sistemes.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 81,0%**, que es correspon amb un **nivell de maduresa *N3, procés definit***; és a dir, els processos de control implantats estan estandarditzats i documentats formalment. Això representa un **índex de compliment del CBCS 4 del 100%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 47,4%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora notable de 33,6 punts en l'índex de maduresa del control.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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

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

Situació del control

El departament ha completat el procediment existent amb totes les tasques que duen a terme: protocol d'instal·lació d'estacions de treball, actualització de microprogramari d'equips, revisions periòdiques, configuracions basades en plantilles, etc.

La configuració de dispositius i sistemes es realitza a partir de plantilles preconfigurades que a més es revisen i actualitzen periòdicament. Per a l'elaboració d'aquestes plantilles, hi ha responsables i s'estableix en el procediment que han de seguir les recomanacions de seguretat de les principals entitats en matèria de seguretat (CCN, CIS, etc.).

El procediment aprovat a aquest efecte inclou un apartat de "Mesuraments i mètriques" que descriu la recollida d'indicadors a fi de garantir la millora contínua sobre el control. No obstant això, no es recullen identificadors amb la finalitat d'establir objectius quantitatius, la qual cosa impedeix aconseguir nivells de maduresa superiors.

Per mitjà de l'eina comentada en punts anteriors, Microsoft Endpoint Configuration Manager 2019, el departament monitora i detecta canvis en equips, no obstant això, no s'ha definit un grup de sistemes crítics sobre els quals realitzar revisions periòdiques de canvis de configuració.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 70,9%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 5 del 88,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 24,7%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora notable de 46,2 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, conscient de l'oportunitat de millora en aquest punt, ha elaborat i aprovat un procediment de gestió de registres d'auditoria que defineix l'abast dels sistemes a auditar, les accions, responsabilitats, permisos d'accés als registres, períodes de retenció,

utilització del SIEM, directives que s'apliquen, política de còpia de seguretat dels registres, etc.

El departament utilitza l'eina AlienVault per a la recopilació dels registres dels diversos sistemes, cosa que permet homogeneïtzar el tractament dels diferents registres. L'eina anterior, a més, actua com a correlador d'esdeveniments.

Tal com indica el responsable del departament, AlienVault integra diversos sistemes i genera un volum gran de registres. Per aquest motiu, el departament ha redefinit el procés de revisió i ha externalitzat el procés en una empresa especialitzada, a fi de garantir la revisió d'anomalies 24/7.

Addicionalment, el responsable del departament rep diàriament un informe d'anomalies detectades i genera *tickets* amb els incidents detectats per a resoldre'ls.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 85,0%**, que es correspon amb un **nivell de maduresa *N3, procés definit***; és a dir, els processos de control implantats estan estandarditzats i documentats formalment. Això representa un **índex de compliment del CBCS 6 del 100%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 60,0%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 25 punts en l'índex de maduresa del control.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

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

Situació del control

L'Ajuntament, conscient de la necessitat d'establir un control robust que garantisca la recuperació de les dades i sistemes en cas de desastre, ha elaborat un pla de recuperació de desastres i ha treballat per a millorar les còpies de seguretat.

Per a això, ha substituït l'eina revisada en l'auditoria anterior, Symantec Backup Exec, per Veeam Backup. En la nova eina s'inclouen tots els sistemes crítics de l'entitat i informa els responsables de l'estat diari de les còpies.

L'Ajuntament ha decidit focalitzar esforços a millorar les proves de restauració, conscient que aquest tipus de proves són claus per a garantir la recuperació dels sistemes en cas d'incidents. Per a això, s'ha annexat al procediment un *log* de sistemes restaurats, que inclou el sistema a restaurar, les dades, la data, la duració de la restauració, els motius i els responsables de cada prova planificada de restauració.

Addicionalment, s'ha elaborat un pla de recuperació de desastres que descriu la restauració total en el cas d'incidents greus.

L'únic punt que es va recomanar millorar durant el treball de revisió anterior va ser mantindre una còpia de les dades crítiques desconnectada o aïllada de la xarxa corporativa. L'Ajuntament ha donat solució a aquesta recomanació implantant dues mesures: d'una banda, el programari de còpies permet la immutabilitat d'aquestes, és a dir, garanteix la integritat de les dades impedint que cap usuari o procés modifique les dades originals; d'una altra, s'han separat els usuaris del domini de tot el sistema de còpies. Addicionalment, la immutabilitat de les còpies de seguretat ha sigut auditada per un tercer per a corroborar-ne el funcionament.

A més d'això, s'ha completat el sistema de còpies de seguretat amb un sistema desduplicador de còpies, que millora les còpies gestionant de manera eficient aspectes com l'espai d'emmagatzematge (evita dades duplicades, comprimeix les dades) o la reducció de la càrrega de la xarxa.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 89,0%**, que es correspon amb un **nivell de maduresa *N3, procés definit***; és a dir, els processos de control implantats estan estandarditzats i documentats formalment. Això representa un **índex de compliment del CBCS 7 del 100%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 75,5%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 13,5 punts en l'índex de maduresa del control.

CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT

Objectiu del control

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

Situació del control

Compliment de l'ENS

Durant la revisió de la normativa realitzada en el treball d'auditoria anterior, l'Ajuntament es trobava realitzant diverses accions encaminades al compliment de l'ENS i al que s'estableix per la normativa en matèria de protecció de dades de caràcter personal.

En l'informe anterior es va recomanar a l'Ajuntament realitzar les auditories que el mateix ENS preveu i publicar en seu la documentació i distintius corresponents. No obstant això, prèviament a la realització d'una auditoria de l'ENS, l'Ajuntament ha prioritzat la implantació de les mesures de seguretat necessàries.

Encara que la millora en els diferents controls de ciberseguretat és de consideració notable, els treballs han de continuar fins a realitzar les auditories de compliment previstes en l'ENS per a obtindre el certificat de conformitat.

Compliment de l'RGPD

Respecte a la protecció de dades de caràcter personal, l'Ajuntament ha donat continuïtat als treballs que cursava durant el període de revisió.

S'han realitzat revisions d'adequació en diferents àrees i es realitza un seguiment de suggeriments i incidències per part del DPD.

Addicionalment, s'ha evidenciat una responsabilitat proactiva en aquesta matèria, atés que es realitzen auditories anuals per àrees prioritzant aquelles en què les dades són més sensibles. En finalitzar cada exercici, s'emet un informe amb totes les actuacions realitzades.

Compliment legalitat del registre de factures

S'han realitzat les auditories corresponents.

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió aconsegueix un **índex de maduresa del 80,0%**, que es correspon amb un **nivell de maduresa N3**, que indica que existeix un grau raonable d'adequació a la normativa. La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 60,0%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 20,0 punts en aquest índex, encara que hi ha diversos aspectes assenyalats abans relatius al compliment de legalitat que han de ser esmenats.

Governança de ciberseguretat

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

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

Si bé en l'auditoria hem observat l'existència d'un acceptable nivell de compromís i conscienciació amb la ciberseguretat per part dels gestors i responsables de les àrees implicades, és important que hi haja un bon nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament.

Hem observat l'adequada governança en l'Ajuntament en aspectes que permeten l'establiment d'un sistema de gestió de la seguretat de la informació (SGSI) efectiu, com són els següents:

- **Existència d'un marc normatiu i procedimental formalment aprovat**, inclosa l'existència de polítiques de seguretat de la informació formalment assumides per l'organització.

- **L'existència de determinats rols clau en l'organització, com el responsable de seguretat**.

No obstant això, encara que existeix un **comité de seguretat**, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat i que inclou representació de les àrees de l'organització afectades, aquest no es reuneix periòdicament. És necessari que es reprenguen les reunions del comité de seguretat, atés que són els òrgans de govern els que tenen la responsabilitat de liderar i ser exemplars en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat.

Com a control compensatori, hem constatat la implicació proactiva del responsable del departament TIC, que manté setmanalment reunions amb el responsable de seguretat, a fi de mantindre's mútuament al corrent de l'estat de les tasques pendents, incidents, pròximes actuacions, etc.

APÈNDIX 3
Bones pràctiques destacables

Introducció

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

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

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

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

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

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

Protecció d'interfícies per a restringir l'accés de dispositius físics no autoritzats

L'entitat ha establit un control basat en l'aplicació de determinades configuracions bàsiques de seguretat en les interfícies dels dispositius de xarxa, en la gestió escrita de preses i serveis de xarxa i en la realització de revisions periòdiques.

Si bé la solució no proporciona protecció davant d'amenaces avançades, sí que permet impedir la connexió de dispositius no autoritzats per error o per atacs bàsics, i proporciona un cert nivell de seguretat a un cost reduït d'implementació i gestió.

A més de la protecció d'interfícies de xarxa, el departament restringeix l'accés als discos locals i als dispositius USB en totes les connexions d'escriptoris virtualitzats. També es restringeix l'accés a dispositius USB des d'alguns dispositius de la policia.

Els procediments representen amb fidelitat la realitat dels processos de control implantats

L'entitat compta amb un conjunt de procediments de seguretat que disposen del nivell de detall i completesa requerit i a més representen amb fidelitat la realitat dels controls implantats.

L'elaboració, per part dels mateixos responsables i tècnics del departament d'informàtica, de documents que descriuen els processos de control establits facilita en gran manera la repetitivitat de les accions, amb independència dels tècnics que les executen, i garanteix la consistència de les actuacions, tal com es defineix per als controls que disposen d'un nivell *N3, procés definit*.

Aquests procediments no inclouen informació genèrica d'utilitat limitada, i s'ha evitat utilitzar models estandarditzats no adaptats a l'entitat.

Auditories externes

El departament d'informàtica realitza auditories a determinats sistemes o característiques per a garantir-ne el funcionament.

Exemple d'això ha sigut una auditoria aportada sobre la immutabilitat de les còpies de seguretat, característica que s'ha implantat i de la qual s'ha auditat el funcionament correcte.

Addicionalment, l'Ajuntament contracta auditories tècniques com les realitzades en *hacking* ètic.

Seguretat perimetral millorada

Un *sandbox* (o caixa d'arena) és un entorn de proves aïllat que permet executar aplicacions perilloses o dubtoses sense risc de posar en perill altres sistemes de l'organització.

El departament ha implantat dues eines de fabricants diferents a fi d'analitzar el correu electrònic i la navegació, de manera que es garanteix una doble anàlisi de qualsevol fitxer sospitós.

A més, el perímetre de la xarxa de l'Ajuntament compta amb dos *firewalls* de diferents fabricants. Això proporciona una alta disponibilitat i garanteix un nivell addicional de seguretat en l'entrada i eixida de connexions.

SIEM millorat

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.

El SIEM ha sigut millorat integrant els esdeveniments publicats en Open Threat Exchange (OTX), base de dades d'amenaces pública alimentada per diverses fonts. Aquesta integració permet la detecció precoç i prevenció d'incidents de ciberseguretat.

Addicionalment, el SIEM és revisat 24/7 per l'empresa adjudicatària a aquest efecte, es completa amb la llista d'amenaces de la mateixa empresa, emet informes que es revisen diàriament i es realitza còpia de seguretat dels seus esdeveniments.

Vigilància digital

La vigilància digital és un servei de rastreig d'informació i detecció d'amenaces basada en intel·ligència artificial i proporciona alertes als qui analitzen aquesta informació. Atesa la seua importància, l'Ajuntament ha decidit implantar Trillion, que juntament amb els reports del CSIRT-CV alerten l'Ajuntament d'incidències com la vulneració de credencials dels seus comptes o el registre de dominis semblants.

Prevenció de ransomware

A més de l'eina MicroCLAUDIA del CCN, l'Ajuntament completa la prevenció contra el *ransomware* amb una altra eina, InterceptX de Sophos, instal·lada en els equips i que és capaç de detectar encriptació de fitxers per *ransomware* i parar els serveis del sistema infectat, a fi d'evitar que la infecció es propague.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

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

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

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

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

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

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

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

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

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

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

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

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

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, l'esborrany previ de l'Informe de fiscalització es va discutir amb la regidora delegada d'Innovació i amb el responsable del departament d'informàtica perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*c* del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'Informe de fiscalització corresponent a l'exercici 2021, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

Dins del termini concedit, l'Ajuntament ha formulat les al·legacions que ha considerat pertinents.

Pel que fa al contingut de les al·legacions i al seu tractament, cal assenyalar el següent:

1. Totes les al·legacions s'han analitzat detingudament.

2. Les al·legacions admeses s'han incorporat al contingut de l'Informe.

En els annexos I i II s'incorporen el text de les al·legacions formulades i l'informe motivat que se n'ha emés i que ha servit perquè la Sindicatura les estimara o desestimara.

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 15 de juny de 2022, va aprovar aquest informe d'auditoria.

ANNEX I

Al·legacions presentades

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

C/ Sant Vicent, 4 - 46002
Tel. +34 96 386 93 00
Fax +34 96 386 96 53
sindicom@gva.es
www.sindicom.gva.es

JUSTIFICANTE DE PRESENTACIÓN EN REGISTRO ELECTRÓNICO

NÚMERO DE REGISTRO 202203189	FECHA DE ENTRADA 07/06/2022 12:46
ÁREA Fiscalización - Alegaciones	PROCEDIMIENTO PAA2020/35 Seguimiento de las 11 auditorías de los controles básicos de ciberseguridad cuyo trabajo de campo se ha realizado en 2019 (una vez transcurrido un año desde su finalización)
DATOS DEL PRESENTADOR Nombre: NIF / CIF: E-mail: Entidad: BENIDORM	
FIRMA DIGITAL B3228E5D45A055F7AA435091AD73B2F972495718	
DOCUMENTOS ENVIADOS Fichero1: 25119496T_202267_Informe para alegaciones.pdf Fichero2: 25119496T_202267_Informe auditoria facturas Ayuntamiento de Benidorm 2019_compressed.pdf Fichero3: 25119496T_202267_Informe auditoria facturas Ayuntamiento de Benidorm 2020_compressed.pdf	

INFORME DE ALEGACIONES AL BORRADOR DEL INFORME DE SEGUIMIENTO DE LAS RECOMENDACIONES REALIZADAS EN EL INFORME DE AUDITORÍA DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE BENIDORM DEL AÑO 2019. SITUACIÓN A 31 DE DICIEMBRE DE 2021

Sr. Interventor

En relación con el borrador del informe de seguimiento de la auditoría de Ciberseguridad que llevó a cabo la Sindicatura de Comptes en el Ayuntamiento de Benidorm (PAA2020/35), he de manifestarle que en él quedan reflejadas fielmente las circunstancias de la seguridad de nuestra instalación informática.

No obstante, observo que en el apartado del CBCS. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD, respecto al cumplimiento de la legalidad del registro de facturas, se apunta que no se han aportado las auditorías correspondientes.

Durante el desarrollo de los trabajos de auditoría no fuimos conscientes de la necesidad de entregarlas, dado que -tratándose de una revisión- ya en la primera ya se había aportado la del año correspondiente.

Por esta razón, debemos remitirles los informes anuales de 2019 y 2020 de la “Evaluación del Cumplimiento de la Normativa de Morosidad y del Registro Contable de Facturas”. Con ello, espero quede subsanada esta carencia y se pueda reflejar en el informe definitivo, modificándose las referencias que aparecen en las páginas 9, 15 y 41, así como, en su caso, en las puntuaciones calculadas.

Benidorm,

Jefe del Departamento de Informática

ANNEX II

Informe sobre les al·legacions presentades

ANÀLISI DE LES AL·LEGACIONS EFECTUADES PER L'AJUNTAMENT DE BENIDORM A L'ESBORRANY DE L'INFORME DE SEGUIMENT DE LES RECOMANACIONS REALITZADES EN L'INFORME D'AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DE L'AJUNTAMENT DE BENIDORM DE L'ANY 2019

Per mitjà d'un escrit de la Sindicatura de 25 de maig de 2022 es va remetre a l'Ajuntament de Benidorm l'esborrany de l'Informe de seguiment de recomanacions perquè efectuara les al·legacions que considerara oportunes. Amb data 9 de juny es van rebre pel registre electrònic les al·legacions formulades i respecte a aquestes s'assenyala el següent:

Al·legació única

Apartat "Compliment normatiu i governança de ciberseguretat", de l'esborrany de l'Informe, en què s'assenyala que no s'han aportat les auditories del registre de factures

Comentaris

En l'al·legació realitzada per l'Ajuntament s'inclouen els informes d'auditoria del registre de factures dels exercicis 2019 i 2020, per la qual cosa es modifica el contingut de l'Informe.

Conseqüències en l'Informe

Es modifiquen els índexs de maduresa i compliment del CBCS 8, quadre 1, que passen a ser 80,0% i 100,0% respectivament.

Es modifiquen els índexs de maduresa i compliment generals, en el segon paràgraf de l'apartat 4 (passa a ser 81,4%), i quadre 1, que passen a ser 81,4% i 96,8% respectivament.

L'índex de compliment general del segon paràgraf després del quadre 1 passa a ser 96,8%.

Es modifica el gràfic 1 i s'adapta a la nova puntuació del CBCS 8.

S'elimina la recomanació 11 (era nova d'aquest informe), de l'apartat 5.

Es modifica el text "No s'inclouen els punts 9 i 11 anteriors, ja que són mesures de compliment obligat" del paràgraf anterior al gràfic 2, que queda així:

> "No s'inclou el punt 9 anterior, ja que és una mesura de compliment obligat."

En l'apèndix 2, els següents apartats del CBCS 8, "Compliment normatiu i governança de ciberseguretat", queden redactats així:

> **"Compliment legalitat del registre de factures**
>
> S'han realitzat les auditories corresponents.
>
> **Indicadors**
>
> En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió aconsegueix un **índex de maduresa del 80,0%**, que es correspon amb un **nivell de maduresa N3**, que indica que existeix un grau raonable d'adequació a la normativa. La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 60,0%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 20,0 punts en aquest índex, encara que hi ha diversos aspectes assenyalats abans relatius al compliment de legalitat que han de ser esmenats."

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 ciberseguretat Ajuntament Benidorm en 2019 - SEFYCU 3346808

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 WMRZ 2ML7 RP7R TLA9

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 - 28/06/22 07:46 VICENT CUCARELLA TORMO