

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
GANDIA 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 d'una manera cada vegada més intensa a amenaces provinents del ciberespai. Això origina un increment dels riscos associats als sistemes d'informació que sustenten els serveis públics i, per tant, a la informació que manegen. De fet, les entitats locals han sigut un dels objectius més afectats per les recents onades de ciberatacs.

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

Conclusions

Encara que s'han realitzat progressos des de la nostra auditoria anterior i s'han atés de manera parcial les nostres recomanacions, l'índex de maduresa general dels controls bàsics de ciberseguretat és encara insuficient i ha de millorar.

L'índex de maduresa general dels CBCS mostra un valor del 51,7%, per la qual cosa l'Ajuntament ha de prendre mesures per a reconduir la situació amb la finalitat d'aconseguir l'objectiu del 80%. A pesar de la millora experimentada des de l'índex de maduresa del 37,8% identificat en la nostra auditoria de 2019, el nivell d'efectivitat en els controls analitzats és insuficient i l'Ajuntament ha de continuar implantant millores per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en els controls que presenten deficiències significatives.

Hem constatat que l'Ajuntament no té establida una adequada governança de la ciberseguretat. Els òrgans superiors de l'Ajuntament (alcalde i/o la Junta de Govern), com a responsables del sistema de control, han de reforçar el nivell actual de compromís i suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

Així mateix, la nostra revisió ha posat de manifest un grau de compliment deficient de les normes legals relacionades amb la seguretat de la informació. L'informe assenjala diversos aspectes sobre els quals s'ha d'actuar per a una ràpida esmena. Respecte de l'Esquema Nacional de Seguretat, l'Ajuntament ha d'aprovar la política de seguretat de la informació (PSI) per mitjà de l'òrgan superior competent, efectuar la designació de les persones per als rols definits en la PSI i constituir els òrgans de govern de la seguretat allí descrits. En relació amb la protecció de dades personals, l'Ajuntament ha d'aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals i planificar i executar auditories de compliment.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament, entre les quals aconsellem finalitzar i aprovar els procediments de seguretat en elaboració per als controls analitzats, inventariar els actius de l'entitat i impedir la



connexió de dispositius no autoritzats a la xarxa corporativa, establir un procediment de gestió integral del programari que incloga, entre altres, l'actualització de tots els sistemes fora de suport, i aprovar i implantar un procediment de configuració segura o fortificació dels sistemes.

NOTA

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



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

Situació a 31 de desembre de 2021

**Sindicatura de Comptes
de la Comunitat Valenciana**



ÍNDEX (amb hipervincles)

1. Introducció	3
2. Responsabilitats dels òrgans superiors de l'Ajuntament en relació amb els controls de ciberseguretat	4
3. Responsabilitat de la Sindicatura de Comptes	4
4. Conclusions	5
5. Recomanacions i mesures necessàries per al compliment de la legalitat	8
Apèndix 1. Metodologia aplicada	19
Apèndix 2. Situació dels controls bàsics de ciberseguretat	36
Apèndix 3. Bones pràctiques destacables	47
Acrònims i glossari de termes	51
Tràmit d'al·legacions	53
Aprovació de l'Informe	54



1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

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

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

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 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 Gandia, 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

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

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



raonable per a continuar prestant els seus serveis. La ciberhigiene és un principi fonamental¹ relacionat amb la seguretat de la informació i equival a establir mesures rutinàries senzilles per a minimitzar els riscos de les ciberamenaces. De manera anàloga al que ocorre amb la higiene personal, les bones pràctiques de ciberhigiene poden impulsar una major immunitat en les entitats que les apliquen, la qual cosa redueix el risc davant d'un ciberatac.

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

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022 hem realitzat el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Gandia. 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 la millora dels 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 que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CBCS revisats.

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

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

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

4. CONCLUSIONS

Encara que s'han fet progressos des de la nostra auditoria anterior i s'han atés parcialment les nostres recomanacions, l'índex de maduresa general dels controls bàsics de ciberseguretat és encara insuficient i ha de millorar per a aconseguir els nivells exigits per l'ENS.

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconseguix un **índex de maduresa general del 51,7%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o no formalitzats documentalment.

Encara que l'Ajuntament ha atés de manera parcial les nostres recomanacions i l'índex de maduresa general ha millorat des del 37,8% identificat en la nostra auditoria de 2019, l'índex de maduresa actual continua sent insuficient per a garantir un grau de seguretat adequat i aconseguir el 80% requerit per l'ENS.



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

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

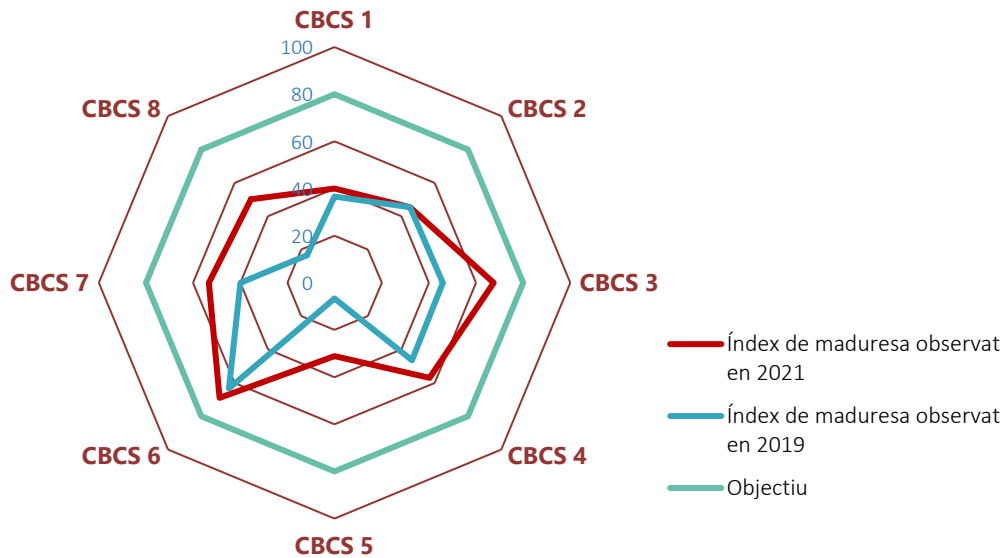
Control	2019			2021		
	Índex de maduresa	Nivell de maduresa	Índex de compliment	Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1 Inventari i control de dispositius físics	36,6%	N1	45,8%	40,0%	N1	50,0%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	45,3%	N1	56,6%	45,3%	N1	56,6%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	45,9%	N1	57,4%	67,5%	N2	84,4%
CBCS 4 Ús controlat de privilegis administratius	46,4%	N1	58,1%	57,0%	N2	71,3%
CBCS 5 Configuracions segures del programari i maquinari	6,6%	N0	8,3%	31,1%	N1	38,9%
CBCS 6 Registre de l'activitat dels usuaris	65,5%	N2	81,7%	69,0%	N2	86,3%
CBCS 7 Còpies de seguretat de dades i sistemes	40,0%	N1	50,0%	53,3%	N2	66,7%
CBCS 8 Compliment normatiu i governança de ciberseguretat	16,5%	N1	20,6%	50,1%	N2	62,7%
General	37,8%	N1	47,3%	51,7%	N2	64,6%

L'índex de compliment dels CBCS és del 64,6%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*. Aquest índex ha millorat des del 47,3% del nostre informe anterior. La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una millora en quasi tots els controls, especialment en els que estaven en una situació més deficient, si bé la millora ha sigut insuficient i cap control aconsegueix l'objectiu, atés el baix grau d'atenció a algunes de les nostres recomanacions (vegeu apartat 5 següent).

A pesar de la millora experimentada, el nivell de maduresa en els controls analitzats és insuficient i hi ha clares possibilitats de millora per a aconseguir els nivells exigits per l'ENS. Han d'implantar-se millores amb major intensitat en aquells controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 1, CBCS 2 i CBCS 5). En l'apartat 5 es fan 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 Gandia no té establida una adequada governança de la ciberseguretat, situació que cal esmenar. A més, s'ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

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

Hem pogut verificar l'existència d'un insuficient nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament. Les mancances més rellevants identificades són les següents:

- La falta d'un marc normatiu i procedimental formalment aprovat, inclosa la inexistència d'una política de seguretat de la informació.²
- La inexistència d'un comitè de seguretat de la informació, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat, que ha d'incloure representació de les àrees de l'organització afectades.

² Segons el CCN, en [Aproximación al marco de gobernanza de la ciberseguridad](#), "la importància cabdal de la política de seguretat de la informació, com a base essencial per a la construcció de la seguretat de la informació, fa que constitueixca sempre el primer element que s'ha d'escometre, i ha de ser públicament aprovada pel seu òrgan directiu, com a evidència del **compromís** de l'organització amb la seguretat de la informació i el seu manteniment".



- La inexistència de determinats rols clau en l'organització, com el responsable de seguretat de la informació.

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

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

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

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

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

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

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

1. Aprovar formalment i completar el procediment existent per a la gestió de l'inventari i el control d'actius físics, incloent-hi les revisions periòdiques de maquinari i les dates d'aquestes revisions, actualitzant degudament l'inventari i incloent-hi el detall necessari de cada actiu.

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

2. Millorar les solucions implantades per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa i establir aquestes mesures en un procediment aprovat.

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

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



- L'inventari del programari, amb un abast que en garantisca la completesa (la totalitat de sistemes d'informació de l'entitat) i un nivell d'actualització adequat.
 - Llistat de programari autoritzat en l'entitat i els procediments necessaris per a actualitzar-lo, incloent-hi les accions implantades actualment relacionades amb l'autorització i control de les instal·lacions.
 - Els controls a implantar per a limitar la instal·lació i execució solament al programari autoritzat.
 - La definició d'un pla de manteniment del programari que considere la totalitat de l'utilitzat, incloent-hi tant el gestionat per mitjà de licitacions i clàusules contractuals com la resta de programari utilitzat a l'Ajuntament.
4. Revisar i actualitzar tots els sistemes que es troben fora del període de suport.

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

5. Aprovar el procediment existent d'identificació i solució de vulnerabilitats que inclou les accions actualment implantades i establir tasques per a la gestió periòdica de pedaços de seguretat i actualitzacions.

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

6. Formalitzar un 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 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, l'ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.
 - La política d'autenticació que cal aplicar a aquest tipus de comptes.

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

7. Aprovar els procediments existents de fortificació de sistemes i aplicar-los a tots els sistemes crítics de l'entitat. Els procediments existents han de considerar 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. 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 d'eines automatitzades de monitoratge de la configuració.

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

8. Aprovar formalment el procediment existent per al tractament de *logs* d'auditoria d'activitat d'usuari, i especificar, 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*.
9. La recomanació de l'informe de 2020 ha sigut parcialment aplicada i es refon amb l'anterior.

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

10. Aprovar formalment el procediment existent per a la gestió de còpies de seguretat de dades i sistemes. Aquest procediment ha de definir, a més de les dades, sistemes afectats, periodicitat de les còpies, ubicacions i responsables, les proves periòdiques de restauració planificades i els requisits de protecció de les còpies.
11. Millorar les mesures addicionals de protecció sobre les còpies de seguretat.

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

12. 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:
 - Aprovar la política de seguretat per part de l'òrgan superior competent (alcalde i/o la Junta de Govern), amb el contingut previst en l'ENS.
 - Designar les persones que assumiran els rols definits en la política de seguretat i constituir els òrgans que s'hi descriuen.
 - Adoptar les mesures de seguretat descrites en la declaració d'aplicabilitat.
 - Realitzar les auditories de compliment previstes en l'article 34 del Reial Decret 3/2010.
 - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS de 13 d'octubre de 2016.



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

- 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.

14. L'incompliment assenyalat en l'informe de 2020 ha sigut esmenat.

Priorització de les recomanacions

A fi que puguem 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 seua implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2019 adaptant la relació risc/cost de cada recomanació i considerant les millores realitzades des de la revisió anterior. No s'hi inclouen els punts 11 i 12 anteriors, ja que són mesures de compliment obligat.

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



Seguiment de recomanacions anteriors

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



Tal com es mostra en el quadre 2, de les catorze recomanacions realitzades en aquell informe, una s'ha atés completament, dues no s'han atés i en onze s'han realitzat accions parcials de millora.

Actuacions en curs

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

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

- Contractació de serveis especialitzats en ciberseguretat: en l'actualitat, l'Ajuntament es troba en fase d'adequació al que s'estableix en l'ENS i l'RGPD i per a fer-ho s'ha contractat un servei de consultoria amb una empresa externa. El servei inclou un pla d'adequació a la normativa vigent en aquestes matèries i un pla de treball a aquest efecte.
- Canvi integral en els centres de processament de dades (CPD): l'Ajuntament té prevista una renovació integral dels seus CPD. Aquest projecte està en fase d'execució i, en la data d'aquest informe, ja s'ha adjudicat la contractació. La nova infraestructura inclourà dos CPD semblants i una unitat d'emmagatzematge, que permetran millores com l'alta disponibilitat dels serveis municipals crítics o canvis en el repositori de fitxers.
- Millora en les còpies de seguretat: l'Ajuntament també té previst millorar el control sobre les còpies de seguretat de dades i sistemes. Per a això, es disposa a comprar un dispositiu amb les característiques d'encryptació, no modificació i compressió de dades. A més, està previst afegir un nivell addicional de còpies de seguretat en el núvol.
- L'Ajuntament prepara la licitació d'un contracte que preveu l'actualització de determinats sistemes operatius fora de suport.
- Col·laboració amb CSIRT-CV: l'Ajuntament ha desplegat serveis i eines proporcionats pel CSIRT-CV, com a part del Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana. Algunes de les solucions ja s'han desplegat i s'han avaluat en aquest treball, com:
 - CARMEN, solució desenvolupada amb l'objectiu d'identificar el compromís de la xarxa d'una organització per part d'amenaques persistents avançades (APT).



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

El pla es completarà amb el desplegament i posada en marxa de les eines següents:

- GLORIA, plataforma per a la gestió d'incidents i amenaces de ciberseguretat a través de tècniques de correlació d'incidències (SIEM).
- SAT-INET (Sistema d'Alerta Primerenca d'Internet): servei desenvolupat i implantat per l'Equip de Resposta davant Incidents de Seguretat de la Informació del Centre Criptològic Nacional (CCN-CERT) per a la detecció en temps real de les amenaces i incidents.
- LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces), eina per a la gestió de ciberincidents en les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat.

³ Un segrestador o *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	<p>Aprovar formalment un procediment per a la gestió de l'inventari i el control d'actius físics que reculla el procés complet, incloent-hi les revisions periòdiques de maquinari, actualitzant degudament l'inventari i incloent-hi les dates d'aquestes revisions.</p> <p>A l'hora de garantir un nivell d'actualització adequat de l'inventari, és aconsellable fer prevaldre l'ús d'eines per a la detecció i actualització automàtica dels elements del sistema d'informació davant de procediments manuals.</p>	<p>S'ha elaborat un procediment que recull el procés implantat, però no s'ha aprovat formalment.</p> <p>Encara que s'ha implantat una nova eina d'inventari, aquesta eina és manual i no inclou el detall necessari de cada actiu. Hi ha eines addicionals de detecció automatitzada com a control compensatori.</p>	<p>Aplicada parcialment</p>	<p>Es manté la redacció feta en 2019.</p>
2	<p>Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.</p>	<p>S'ha implantat la limitació per <i>mac</i> en els <i>switches</i> de l'Ajuntament, però aquesta mesura no s'aplica a la totalitat de <i>switches</i> ni s'ha establert en un procediment aprovat. No hi ha mesures de protecció addicionals.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
3	<p>Aprovar formalment i implantar un procediment de gestió integral del programari de l'entitat, que incloga:</p> <ul style="list-style-type: none"> L'inventari del programari, amb un abast que en garantisca la completesa (la totalitat de sistemes d'informació de l'entitat) i un nivell adequat d'actualització. Llistat de programari autoritzat en l'entitat i els procediments necessaris per a actualitzar-lo, incloent-hi les accions implantades actualment relacionades amb l'autorització i control de les instal·lacions. Controls que cal implantar per a limitar la instal·lació i execució solament al programari autoritzat. La definició d'un pla de manteniment del programari que considere la totalitat de l'utilitzat, incloent-hi tant el gestionat per mitjà de licitacions i clàusules contractuals com la resta de programari utilitzat a l'Ajuntament. 	<p>Sense variació.</p>	<p>No aplicada</p>	<p>Es manté la redacció feta en 2019.</p>



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>4 Revisar i actualitzar tots els sistemes que es troben fora del període de suport.</p>	<p>Actualment, es mantenen en producció dispositius amb sistemes operatius fora del període de suport.</p>	<p>No aplicada</p>	<p>Es manté la redacció feta en 2019.</p>
<p>Aprovar un procediment d'identificació i solució de vulnerabilitats que incloga les accions actualment implantades, n'amplie l'abast de manera que s'aplique a la totalitat de sistemes de l'Ajuntament i l'apliquen tots els membres del departament de sistemes. Aquest procediment ha d'incloure:</p> <ul style="list-style-type: none"> • La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i el seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat. • La prioritització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades. • L'ús d'eines que permeten la gestió unificada i automatitzada de pedaços de seguretat i altres actualitzacions. 	<p>L'Ajuntament ha elaborat un procediment de gestió de vulnerabilitats que inclou totes les recomanacions proposades en la nostra auditoria, però no s'ha aprovat formalment.</p> <p>S'han introduït millores en el procés d'identificació i solució de vulnerabilitats, com ara establir la periodicitat amb què s'utilitzen les eines de detecció proactiva de vulnerabilitats i gestió de pedaços i actualitzacions.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>Formalitzar un procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga:</p> <ul style="list-style-type: none"> • L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió hauran de realitzar-se amb usuaris nominatius. • Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes. • La política d'autenticació que cal aplicar a aquest tipus de comptes. 	<p>S'ha eliminat la majoria dels comptes d'usuari no nominatius amb permisos d'administració. Hi ha comptes no nominatius, però el seu ús està controlat.</p> <p>S'ha creat un inventari de comptes d'administració.</p> <p>No obstant això, no s'ha aprovat un procediment que definisca la gestió d'usuaris amb privilegis administratius ni es revisen periòdicament els usuaris amb aquests privilegis.</p> <p>No s'ha aprovat un procediment que definisca la política de contrasenyes aplicable a tots els sistemes i no s'aplica una política homogènia en tots els sistemes.</p>	<p>Aplicada parcialment</p>	<p>Es manté la redacció feta en 2019.</p>



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>7 Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN.</p> <p>Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà d'un procediment manual o d'eines automatitzades de monitoratge de la configuració.</p>	<p>S'ha definit un procediment que descriu les accions dutes a terme amb la finalitat de mantindre la configuració segura de <i>switches</i> i equips Windows.</p> <p>S'ha incorporat un tallafoc a la xarxa corporativa i es guarden les configuracions dels <i>switches</i> i el tallafoc.</p> <p>El procediment de fortificació no està formalment aprovat, no s'aplica a tots els elements de l'entitat (servidors, dispositius mòbils, tauletes, etc.), ni existeix un procediment de gestió de canvis en les configuracions de sistemes crítics de l'entitat.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>8 Aprovar formalment un procediment per al tractament de <i>logs</i> 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 <i>logs</i>.</p>	<p>S'ha desenvolupat una política de gestió de <i>logs</i>, però no es troba formalment aprovada.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>9 Formalitzar les accions implantades per a la gestió d'incidències de seguretat i assignar aquesta tasca a diversos membres del departament, de manera que si la persona que habitualment la realitza no es troba, l'execució estiga garantida.</p>	<p>La política de <i>logs</i> d'auditoria defineix com a responsables tots els membres del departament, no obstant això, no està formalment aprovada.</p>	<p>Aplicada parcialment</p>	<p>La recomanació resultant es refon amb l'anterior, ja que són coincidents.</p>
<p>10 Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes, que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.</p>	<p>L'Ajuntament ha desenvolupat una política que estableix les accions dutes a terme i la periodicitat de còpia dels fitxers i servidors, però no ha sigut formalment aprovada per la corporació.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>11 Aplicar mesures addicionals de protecció sobre la còpia de seguretat, per exemple, emmagatzemant-la en un suport desconnectat, o en sistemes no accessibles directament a través de la xarxa, etc.</p>	<p>S'han establert mesures addicionals de protecció sobre les còpies, com ara còpies periòdiques desconnectades de la xarxa corporativa.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>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:</p> <ul style="list-style-type: none"> • Aprovar una política de seguretat per part de l'òrgan superior competent que precise, com a mínim, objectius i missió de l'organització, marc legal i normatiu, definició de rols i funcions, estructura organitzativa i el procés d'aprovació i revisió d'aquesta. • Designar les persones que assumiran els rols definits en la política de seguretat. <p>12 • Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriuen.</p> <ul style="list-style-type: none"> • Realitzar les auditories de compliment previstes en l'article 34 de l'RD 3/2010. • Emplenar la Instrucció Tècnica de Seguretat de l'Informe de l'Estat de la Seguretat, de la Secretaria d'Estat d'Administracions Públiques (Informe INES). • 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. 	<p>Projecte en fase d'execució.</p> <p>S'ha desenvolupat una política de seguretat que estableix els rols dels responsables en matèria de seguretat. No obstant això, la política no s'ha aprovat formalment.</p> <p>No s'han realitzat les auditories de compliment ni s'han obtingut els distintius corresponents.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>



Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>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:</p> <ul style="list-style-type: none"> Finalitzar l'elaboració del registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la LO 3/2018. <p>13 • Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb als articles 32.2 i 35 de l'RGPD.</p> <ul style="list-style-type: none"> Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD. Planificar i executar auditories de compliment en matèria de protecció de dades. 	<p>En fase d'execució.</p> <p>S'ha elaborat i publicat el registre d'activitats i s'ha elaborat l'anàlisi de riscos.</p> <p>No s'han aplicat mesures per a protegir dades personals ni s'han dut a terme les auditories pertinents.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2019.</p>
<p>14 Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.</p>	<p>S'ha dut a terme l'auditoria del registre de factures.</p>	<p>Aplicada</p>	<p>S'elimina.</p>



APÈNDIX 1

Metodologia aplicada



Introducció

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

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

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

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

Tot i que l'adopció de mesures de seguretat adequades fa més resilients les organitzacions davant dels ciberatacs, l'anàlisi dels incidents produïts que es realitza en els informes INES⁴ del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs es mantinguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan correctament implementades.

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

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



Objectiu de l'auditoria

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022, el nostre objectiu ha sigut realitzar el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Gandia. Exercici 2019, així com obtenir una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això hem avaluat tant el seu disseny⁵ com la seua eficàcia operativa⁶ 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

⁵ L'avaluació del disseny d'un control implica la consideració per l'auditor si el control, de manera individual o en combinació amb altres controls, és capaç de previndre de manera eficaç, o de detectar i corregir, la materialització dels riscos previstos. És a dir, és capaç de complir l'objectiu de control.

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



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

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

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

Àmbit temporal

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

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

Metodologia

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

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

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



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

La guia pràctica de fiscalització dels OCEX 5313

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

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

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

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



Quadre 3. Els CBCS i l'ENS

Control	Mesura de seguretat de l'ENS*
CBCS 1 Inventari i control de dispositius físics	op.exp.1
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	op.exp.1 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) assenyala⁸ que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen", reduint els ciberriscos.⁹

Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats als quals 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 prioritars recomanats per ENISA com a bones pràctiques de ciberhigiene.

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

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

¹⁰ Carnegie Mellon University Software Engineering Institute, [Cyber Hygiene: A Baseline Set of Practices](#), 2017.



Quadre 4. Punts d'acció d'ENISA

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

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

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

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

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



Quadre 5. Els CBCS i els seus subcontrols

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



Control	Objectiu del control	Subcontrol	
CBCS 5 Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors	Establir, implantar i gestionar la configuració de seguretat, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de previndre atacs a través de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6 Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels logs d'auditoria)	Recollir, gestionar i analitzar logs d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de logs d'auditoria	El log d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
		CBCS 6-2: Emmagatzematge de logs: retenció i protecció	Els logs es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de logs	Els logs de tots els sistemes són revisats periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels logs d'auditoria, de manera que se'n facilite la revisió.
		CBCS 6-4: Monitoratge i correlació	L'entitat disposa d'un SIEM (<i>security information and event management</i>) o una eina d'anàlisi de logs per a realitzar correlació i anàlisi de logs.
CBCS 7 Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeti 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 permeti 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: <ul style="list-style-type: none">- El procediment està formalitzat (documentat i aprovat) i actualitzat.- El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	En línies generals, compleix l'objectiu de control, si bé pot haver-hi certs aspectes no coberts al 100% i: <ul style="list-style-type: none">- Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.).- Les proves realitzades per a verificar la implementació són satisfactòries.- S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	Cobreix de forma molt limitada l'objectiu de control i: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- No se segueix un procediment clar.- Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	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 basen en la *Guía de seguridad CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 7. Nivells de maduresa

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



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

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

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

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

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

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

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

Confidencialitat És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.

Integritat És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, assegurant que no se n'ha produït l'alteració, pèrdua o destrucció, ja siga de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.

Disponibilitat Es tracta de la capacitat d'un servei, un sistema o una informació, de ser accessible i utilitzable pels usuaris o processos autoritzats quan aquests ho requerisquen.



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

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

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

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

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

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

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

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

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

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

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

Governança de ciberseguretat

A l'efecte d'aquest treball, s'entendrà per governança de la seguretat de la informació i les comunicacions o de ciberseguretat (termes que utilitzem de manera indistinta en aquest informe) el conjunt de responsabilitats i activitats realitzades per l'alta direcció amb l'objectiu de proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconsegueixen 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'[Anàlisis núm. 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE](#) del Tribunal de Comptes Europeu.



La implicació dels òrgans superiors és, potser, el factor més important per a la implantació amb èxit d'un sistema de gestió de la seguretat de la informació o de ciberseguretat.¹⁴ L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació¹⁵ que ha de materialitzar-se en aspectes com ara:

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

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

- 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 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información](#), 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 Gandia. Exercici 2019.

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

Quadre 8. Situació de les recomanacions

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

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

Comunicació i confidencialitat

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



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



APÈNDIX 2

Situació dels controls bàsics de ciberseguretat



CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

L'Ajuntament ha elaborat un procediment que recull totes les accions dutes a terme per a mantindre controlat i actualitzat l'inventari de dispositiu maquinari; no obstant això, el procediment no s'ha aprovat formalment.

A fi de mantindre un històric d'ubicacions dels equips d'usuari de l'entitat, el departament d'informàtica ha substituït l'eina d'inventariat GLPI per una base de dades Access de desenvolupament propi. Les dades van ser exportades de l'eina GLPI, que continua sent utilitzada per a l'inventari d'impressores i *switches*, i és actualitzada per personal administratiu. No obstant això, la nova base de dades s'actualitza de manera manual, no disposa dels camps necessaris de cada actiu ni inclou tots els equips de l'entitat. Tampoc s'ha evidenciat l'existència de revisions periòdiques.

Adicionalment, l'Ajuntament manté, per mitjà de l'eina utilitzada per a la gestió centralitzada de l'antivirus, un inventari addicional dels actius amb agent de xarxa instal·lat, encara que únicament es consulta per a realitzar determinades revisions i no per a revisar periòdicament el maquinari.

Per a impedir l'accés a la xarxa corporativa de dispositius no autoritzats s'ha afegit a la normativa una prohibició expressa, si bé aquesta prohibició no és suficient per a garantir l'efectivitat del control, ni la normativa està formalment aprovada.

Una de les millores implantades per a controlar l'accés a la xarxa de dispositius no autoritzats és la limitació per *mac* en els *switches*. No obstant això, aquesta mesura no s'inclou en cap procediment ni està implantada en la totalitat de dispositius. No hi ha mesures addicionals de protecció com un servidor de validació per a l'accés de dispositius a la xarxa o controls per a un altre tipus de dispositius.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 40,0%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 1 del 50,0%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 36,6%, que es correspon amb un nivell de maduresa N1, inicial/ad hoc. Per tant, s'ha produït una millora de 3,4 punts en l'índex de maduresa del control.



CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

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

Situació del control

Hi ha diferents inventaris que formen l'inventari de programari de l'entitat. Es distingeix entre el programari de gestió, el llicenciat i el programari lliure. Els inventaris anteriors es completen amb l'inventari de programari que inclou l'eina utilitzada per a la gestió centralitzada de l'antivirus sobre tots els elements que disposen d'agent de xarxa.

Encara que hi ha cert control sobre les aplicacions instal·lades en els dispositius de l'entitat, es mantenen les recomanacions anteriors, atés que:

- La política de gestió de programari no està formalment aprovada.
- No hi ha revisions periòdiques del programari instal·lat.
- No hi ha mesures que permeten bloquejar aplicacions no autoritzades.
- No existeix un pla de manteniment de programari.
- Hi ha sistemes fora del període de suport.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 45,3%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 2 del 56,6%**.

No s'han realitzat millores per a esmenar les deficiències detectades de control identificades en l'informe realitzat l'any 2019, per la qual cosa no s'ha millorat l'índex de maduresa.

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

Objectiu del control

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



Situació del control

L'Ajuntament ha realitzat diverses millores que permeten un bon nivell de control sobre les vulnerabilitats de dispositius i sistemes. Encara que no s'ha aprovat formalment, s'ha elaborat una política de gestió de vulnerabilitats que estableix les accions que s'han de dur a terme per a la seua identificació, anàlisi, seguiment i resolució.

L'efectivitat del control s'aconsegueix gràcies a les diferents eines implantades per a identificar vulnerabilitats:

- Execució periòdica de l'eina d'escaneig de vulnerabilitats, eina ja revisada en l'anterior auditoria. El seu ús ha sigut millorat per mitjà de l'execució periòdica d'aquesta sobre la xarxa corporativa, identificant vulnerabilitats crítiques que són esmenades atenent la seua criticitat.
- La nova eina centralitzada d'antivirus s'utilitza per a la gestió de pedaços i actualitzacions en aplicacions i sistemes.
- Instal·lació del programari MicroCLAUDIA del CCN-CERT.
- Implantació de l'eina CARMEN, oferida pel CCN-CERT i gestionada pel CSIRT-CV, que alerta per mitjà d'informes d'anomalies en la xarxa i els tècnics prenen mesures amb els resultats d'aquests informes.
- Contractació d'una auditoria externa de vulnerabilitats.

A més de l'ús de les eines anteriors, els tècnics de l'Ajuntament generen *tickets* per cada vulnerabilitat crítica detectada per a la seua resolució. Hem revisat, per mitjà d'una traça completa, el procés d'identificació, prioritització i accions addicionals realitzades per a la resolució d'una de les vulnerabilitats detectades.

Encara que hi ha cert nivell de control sobre les vulnerabilitats, per a aconseguir els nivells exigits per l'ENS, també s'ha de:

- Establir la periodicitat de les revisions de pedaços i actualitzacions. Aplicar aquestes actualitzacions d'acord amb la periodicitat definida.
- Establir en el procediment la periodicitat amb què s'executa l'eina d'escaneig de vulnerabilitats i executar aquests escanejos atesa la periodicitat fixada.
- Incloure en el procediment escrit les mesures que ja estan implantades actualment: CARMEN del CCN-CERT, contractació d'auditories externes, etc.

Finalment, el procediment ha d'aprovar-se formalment.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 67,5%**, 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 3 del 84,4%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 45,9%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 21,6 punts en l'índex de maduresa del control.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

Encara que s'han realitzat determinades accions per a esmenar deficiències detectades en l'auditoria anterior, com la revisió i eliminació de comptes administratius no nominatius de la majoria de sistemes o la creació d'un inventari de comptes d'administració, l'Ajuntament ha de continuar millorant la gestió dels privilegis administratius:

- Aprovació d'un procediment que definisca la gestió d'usuaris amb privilegis administratius, que incloga l'alta, baixa i revisió periòdica d'usuaris, de manera que totes les aplicacions i sistemes tinguen actualitzats els usuaris actius de l'entitat.
- Revisió i eliminació d'usuaris no nominatius amb permisos d'administració de tots els sistemes, com els existents en alguns dels sistemes revisats.
- Revisió periòdica d'usuaris i perfils sobre totes les aplicacions de l'entitat, incloent-hi comptabilitat i recaptació.
- Aprovació de la política de contrasenyes aplicable a tots els sistemes i aplicació d'aquesta política.

La valoració global del control aconsegueix un **índex de maduresa del 57,0%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 4 del 71,3%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 46,4, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 10,6 punts en l'índex de maduresa del control.



CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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

Situació del control

Hem analitzat les accions dutes a terme per l'Ajuntament per al control de configuracions de dispositius i sistemes i hem verificat que no existeix un procés formalment establert a aquest efecte.

El departament d'informàtica ha treballat per a implantar determinades mesures per a aplicar configuracions segures als dispositius i aplicacions, com incorporar un tallafoc a la xarxa corporativa, definir procediments de fortificació per a equips d'usuari i *switches* o guardar les configuracions de *switches* i tallafoc.

No obstant això, continua havent-hi deficiències en els aspectes que s'enumeren a continuació:

- Els procediments que defineixen les accions dutes a terme amb la finalitat de mantindre la configuració segura de dispositius i sistemes no s'han aprovat formalment.
- El tallafoc és gestionat íntegrament per una empresa externa i configurat amb els seus propis criteris i recomanacions. L'Ajuntament únicament li fa peticions puntuals.
- Els procediments de fortificació han de seguir pautes i recomanacions en ciberseguretat, com les recomanacions dels fabricants o de les institucions de referència en la matèria, com el Centre Criptològic Nacional.
- No es manté un registre històric de les configuracions dels dispositius, únicament s'aplica a *switches* i només es guarda l'última configuració.
- No es disposa d'un procediment de gestió de canvis per a sistemes crítics de l'entitat que descriga les accions que cal realitzar per a canvis en aquests sistemes i que monitore i alerte de canvis no autoritzats.

Hi ha un nivell de control insuficient sobre les configuracions segures en dispositius i sistemes; la valoració global del control presenta un **índex de maduresa del 31,1%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 38,9%**.



La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 6,6%, que es correspon amb un nivell de maduresa *NO, inexistent*. Per tant, s'ha produït una millora de 24,5 punts en l'índex de maduresa del control.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

L'Ajuntament ha realitzat determinats canvis per a millorar el control sobre el registre de l'activitat dels usuaris en els diferents sistemes, però continuen existint millores que s'han d'aplicar.

S'ha desenvolupat un procediment de registre d'activitat, que estableix el seu abast i el període de retenció. No obstant això, aquesta política no s'ha aprovat formalment.

Durant l'auditoria anterior vam comprovar que l'Ajuntament disposava d'una eina implantada per a auditar la xarxa corporativa, però únicament incloïa alguns sistemes. Actualment s'ha completat la llista de sistemes integrats en l'eina amb diferents sistemes crítics de l'entitat. L'accés a aquesta eina es realitza per mitjà d'usuaris nominatius i únicament és accessible per als membres del departament d'informàtica. L'eina allotja dues setmanes de trànsit de xarxa, atés el volum generat, a més del registre d'activitat de cada un dels sistemes inclosos, del qual és capaç d'allotjar 25 anys de registres segons els responsables.

Encara que s'ha produït una millora en el control dels registres d'usuari, l'Ajuntament ha de seguir amb les accions de millora:

- Afegir al procediment actual els sistemes sobre els quals es realitza el registre d'activitat, tipus d'accions que es registren, periodicitat de les revisions i responsables d'aquestes, així com mecanismes existents per a impedir modificacions en els registres.
- Incloure en el sistema centralitzat de *logs* la resta de serveis crítics de l'entitat, com les aplicacions o sistemes que sustenten els processos de comptabilitat o la recaptació.

Hi ha cert nivell de control sobre el registre d'activitat dels usuaris, per la qual cosa la valoració global del control aconseguix un **índex de maduresa del 69,0%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 6 del 86,3%**.



La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 65,5%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 3,5 punts en l'índex de maduresa del control.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

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

Situació del control

Per a esmenar les deficiències detectades en l'auditoria de 2019, l'Ajuntament ha desenvolupat una política que estableix les accions dutes a terme i la periodicitat de les còpies de seguretat i s'han establert mesures addicionals de protecció sobre les còpies, com incloure una còpia desconnectada de la xarxa corporativa.

No obstant això, l'Ajuntament ha de continuar millorant els seus procediments per a garantir l'efectivitat del control i aconseguir el nivell requerit per la normativa:

- El procediment de còpies no està formalment aprovat per la corporació.
- No hi ha eines que permeten la gestió centralitzada i automatitzada de la còpia de seguretat.
- No realitza proves planificades de recuperació de dades o sistemes complets, ni es preveuen en el procediment.
- La còpia desconnectada és únicament setmanal.

La valoració global del control és que l'Ajuntament aconseguix un **índex de maduresa del 53,3%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establerts o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 66,7%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 40,0%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 13,3 punts en l'índex de maduresa del control.



CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT

Objectiu del control

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

Situació del control

Compliment de l'ENS

L'Ajuntament, des de l'auditoria realitzada l'any 2019, ha realitzat determinades accions encaminades a complir el que es preveu en l'RD 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica. Per a això s'ha contractat un servei per a la implantació de les mesures pertinents, projecte que està actualment en fase d'execució i les activitats del qual no han finalitzat, per la qual cosa encara incompleix les obligacions imposades per la normativa.

Durant l'execució del projecte s'ha desenvolupat una política de seguretat en la qual s'estableixen els rols i responsabilitats en matèria de seguretat, però aquesta política de seguretat no està aprovada per l'alcalde o la Junta de Govern, ni els rols s'han assignat formalment i tampoc s'ha constituït el comitè de seguretat TIC.

S'ha realitzat la declaració d'aplicabilitat i emés l'informe INES, però l'Ajuntament no ha finalitzat les tasques d'adaptació que estableix l'ENS ni ha realitzat les auditories de compliment.

Compliment RGPD

En relació amb la protecció de dades de caràcter personal, l'Ajuntament ha elaborat i publicat el registre d'activitats de tractament i en el moment de realització d'aquesta auditoria es trobava realitzant l'anàlisi de riscos requerida per l'RGPD.

Encara que l'Ajuntament ha nomenat responsables i creat un comitè sobre aquest tema, no ha finalitzat els treballs amb l'empresa adjudicatària, per la qual cosa no ha aplicat les mesures organitzatives i tècniques necessàries per a protegir les dades personals, ni ha realitzat auditories de compliment.

Compliment de la legalitat del registre de factures

L'Ajuntament ha aportat, durant aquest treball de seguiment, l'auditoria del registre de factures exigida per la normativa.

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió ha millorat respecte a l'índex de maduresa del 16,5% obtingut en l'informe emés l'any 2019 i ha aconseguit un **índex de maduresa del 50,1%**, que es correspon amb un



nivell de maduresa N2, que indica que hi ha incompliments significatius de la normativa, i hi ha aspectes que s'han de millorar.

Governança de ciberseguretat

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

Els òrgans superiors de l'Ajuntament (alcalde i 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.

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

- **La falta d'un marc normatiu i procedimental formalment aprovat**, inclosa la inexistència de polítiques de seguretat de la informació formalment assumides per l'organització.
- **La inexistència del comitè de seguretat de la informació**, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat i que ha d'incloure representació de les àrees de l'organització afectades.
- **La inexistència de determinats rols clau formalment establits en l'organització, com el responsable de seguretat**. Aquesta deficiència constitueix una de les més greus en termes de governança, ja que la seua responsabilitat, la gestió de la seguretat de la informació i dels serveis prestats no pot considerar-se adequadament assumida per la resta dels responsables de l'organització.
- **La responsabilitat de determinats aspectes sobre la ciberseguretat de l'Ajuntament recau en la pràctica íntegrament en els tècnics o en tercers**. La inexistència d'una governança adequada implica que són els tècnics del departament TIC o empreses adjudicatàries els que adopten decisions sobre determinats aspectes en matèria de ciberseguretat, com els criteris per a la realització de còpies de seguretat, decidides pels tècnics, o la implantació del tallafoc corporatiu ateses les recomanacions de l'empresa adjudicatària, però sense la participació activa del comitè de seguretat en aquesta presa de decisions.

Resulta, per tant, necessària la solució urgent de les mancances identificades, atés que tenen un impacte negatiu en el nivell de seguretat de la corporació. En aquest sentit, els



òrgans de govern tenen la responsabilitat de liderar i ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat.

Encara que el nivell de governança de l'Ajuntament és clarament insuficient i ha de millorar-se, s'ha evidenciat la implicació dels tècnics en matèria de ciberseguretat, que es posa de manifest en aspectes com l'aplicació de mesures de seguretat basada en els seus coneixements o els de tercers, l'ús de subvencions per a millorar la seguretat dels sistemes o l'impuls de la governança en matèria de ciberseguretat per a coordinar els responsables de les diferents àrees.



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.

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

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

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

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

Els aspectes destacats a continuació, en general, s'han considerat en l'avaluació dels CBCS. No obstant això, alguns no formen part dels CBCS tal com estan definits en la GPF-OCEX 5313, però els comentem per les raons indicades abans. Cal aclarir que l'existència d'aspectes concrets particularment rellevants no implica necessàriament que el control global 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.

Repositori de documentació i fidelitat d'aquesta amb la realitat dels processos de control implantats

L'entitat té implantat un programari per a la gestió de la seua documentació i els seus protocols interns, que permet mantindre un històric de versions i canvis. És destacable que els procediments existents representen amb fidelitat la realitat dels controls implantats, cosa que evita la utilització de models estandarditzats no adaptats a l'entitat.



L'elaboració, per part dels mateixos responsables i tècnics del departament d'informàtica, de documents que descriuen els procediments de control establits sense incloure informació genèrica d'utilitat limitada 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*.

No obstant això, tots els procediments escrits han d'estar formalment aprovats.

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

L'entitat ha establert un control en les interfícies d'alguns dels dispositius de xarxa. Si bé la solució no proporciona protecció davant d'amenaques avançades, ni s'ha implantat en la totalitat de sistemes, sí que permet impedir la connexió de dispositius no autoritzats per error o per atacs bàsics, de manera que proporciona un cert nivell de seguretat a un cost reduït d'implementació i gestió.

Sistema de control de vulnerabilitats

És particularment destacable la gestió de les vulnerabilitats realitzada pel departament TIC. El conjunt d'accions dutes a terme fa que el control estiga molt prop d'aconseguir els nivells exigits per l'ENS: antivirus d'*endpoint*, gestió de pedaços centralitzada, escaneig periòdic de vulnerabilitats en la xarxa, implantació de solucions del CSIRT-CV i CCN i contractació d'auditories externes de *hacking ètic* i *pentesting*.

Hi ha determinades accions que el departament realitza periòdicament i de manera correcta; no obstant això, aquestes tasques no estan establides per mitjà d'avisos a tot el departament en un calendari, per la qual cosa existeix el risc de no realitzar determinades accions.

És particularment destacable la contractació, per part de l'Ajuntament, d'auditories de *hacking ètic* amb una empresa especialitzada en ciberseguretat. Aquestes auditories han inclòs tests d'intrusió de les zones públiques de la xarxa corporativa, l'escaneig de la xarxa local i algunes proves relacionades amb *phishing* o *malware* l'objectiu de les quals ha sigut els treballadors de l'Ajuntament.



Registre d'activitat

Respecte al registre d'activitat, el departament ha implantat una solució de SIEM que inclou el registre d'activitat dels sistemes crítics de l'entitat. Aquesta eina és únicament accessible per als tècnics del departament i el seu ús està establert en un procediment escrit, però no aprovat per la corporació.

La implantació d'aquest tipus d'eines optimitza considerablement el control sobre el registre d'activitat dels usuaris en sistemes i aplicacions. No obstant això, és la corporació qui ha de decidir quins sistemes són crítics, quines accions registrar, durant quant de temps, etc. Addicionalment, s'ha d'establir en el procediment aprovat quines revisions s'han de realitzar sobre aquests registres, qui ha de realitzar-les i amb quina periodicitat.



ACRÒNIMS I GLOSSARI DE TERMES

- CBCS: Controls bàsics de ciberseguretat
- CCN: Centre Criptològic Nacional
- CGTI: Controls generals de tecnologies de la informació
- ENS: Esquema Nacional de Seguretat
- INES: Informe Nacional de l'Estat de la Seguretat
- LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal
- PSI: Política de seguretat de la informació
- RGPD: Reglament General de Protecció de Dades
- SGSI: Sistema de gestió de seguretat de la informació
- SIC: Sistemes d'informació i comunicacions

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

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

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

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

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



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

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

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

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

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

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



TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que es preveu en la secció 1220 del *Manual de fiscalització* de la Sindicatura, l'esborrany previ de l'Informe d'auditoria es va discutir amb el regidor delegat responsable de Seguretat Ciutadana, Trànsit, Mobilitat, Govern Interior i Coordinació Administrativa i Falles i amb els responsables corresponents de l'àrea de tecnologies de la informació, perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.c del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'Informe d'auditoria corresponent a l'exercici 2021, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

Una vegada transcorregut aquest termini no s'han rebut al·legacions.



APROVACIÓ DE L'INFORME

En compliment de l'article 19.j de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.h del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 4 de maig de 2022, va aprovar aquest informe d'auditoria.



Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Informe seguiment recomanacions controls bàsics CBSC Ajuntament Gandia 2019_VAL - SEFYCU 3236022

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 U972 LKUU Q4VX UQAN

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 - 10/05/22 09:50
VICENT CUCARELLA TORMO