

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

**INFORME DE SEGUIMENT DE LES
RECOMANACIONS REALITZADES EN L'INFORME
D'AUDITORIA DELS CONTROLS BÀSICS DE
CIBERSEGURETAT DE L'AJUNTAMENT D'ELDA
DE L'ANY 2020**

Situació a 31 de desembre de 2021



RESUM

La transformació digital que estan experimentant totes les administracions públiques i la seua interconnexió a través de complexes xarxes informàtiques les exposa 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 d'Elda respecte a la situació mostrada en l'auditoria de l'any 2020.

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 insuficient i ha de millorar.

L'índex de maduresa general dels CBCS mostra un valor del 65,5%, per la qual cosa l'Ajuntament ha d'adoptar mesures amb la finalitat d'aconseguir l'objectiu del 80%. A pesar de la millora experimentada des de l'índex de maduresa del 52,5% identificat en la nostra auditoria de 2020, el nivell d'efectivitat en els controls analitzats és insuficient i hi ha clares possibilitats de millora per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació.

L'Ajuntament d'Elda té establida una acceptable governança de la ciberseguretat, però ha de finalitzar les accions en curs per a millorar-la.

Així mateix, la nostra revisió també ha posat de manifest un grau de compliment insuficient quant a l'adequació a les normes legals relacionades amb la seguretat de la informació. L'informe assenyala diversos aspectes sobre els quals s'ha d'actuar per a una ràpida esmena. Respecte de l'Esquema Nacional de Seguretat, l'Ajuntament ha d'efectuar les auditories de compliment previstes en l'article 34. En relació amb la protecció de dades personals, ha de publicar el registre d'activitats de tractament i realitzar una anàlisi de riscos sobre els seus tractaments de dades personals.



També hem efectuat 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 aprovar un procediment unificat de gestió d'usuaris amb privilegis d'administració, aprovar un procediment d'identificació i solució de vulnerabilitats, així com 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 d'Elda de l'any 2020**

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	17
Apèndix 2. Situació dels controls bàsics de ciberseguretat	34
Apèndix 3. Bones pràctiques destacables	43
Acrònims i glossari de termes	46
Tràmit d'al·legacions	48
Aprovació de l'Informe	49



1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

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

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

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 18 de juny de 2020 el Consell de la Sindicatura de Comptes va aprovar l'[Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elda, Exercici 2020](#). Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 fer un treball de seguiment de la situació dels controls bàsics de ciberseguretat d'aquest ajuntament i dels altres 14 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 un ciberatac o per a recuperar-se'n en un temps



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

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

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

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

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats proporcionant una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de 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 2020, relacionats amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interès 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 i recollides en el *Manual de fiscalització de la Sindicatura de Comptes*. Aquests principis exigeixen que complim els requeriments d'ètica, com també que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CBCS revisats.

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 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 insuficient i ha de millorar

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 65,5%**, 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 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 52,5% identificat en la nostra auditoria de 2020, l'índex de maduresa actual continua sent insuficient per a garantir un grau adequat de seguretat i aconseguir el 80% requerit per l'ENS.



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

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

Control	2020			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	62,3%	N2	77,8%	75,0%	N2	93,8%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	65,0%	N2	81,3%	76,0%	N2	95,0%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	59,3%	N2	74,1%	71,3%	N2	89,1%
CBCS 4 Ús controlat de privilegis administratius	57,3%	N2	71,6%	66,6%	N2	83,3%
CBCS 5 Configuracions segures del programari i maquinari	31,4%	N1	39,2%	36,6%	N1	45,8%
CBCS 6 Registre de l'activitat dels usuaris	43,7%	N1	54,6%	60,0%	N2	75,0%
CBCS 7 Còpies de seguretat de dades i sistemes	66,5%	N2	83,1%	73,2%	N2	91,5%
CBCS 8 Compliment normatiu i governança de ciberseguretat	35,0%	N1	43,8%	65,0%	N2	81,3%
General	52,5%	N2	65,7%	65,5%	N2	81,9%

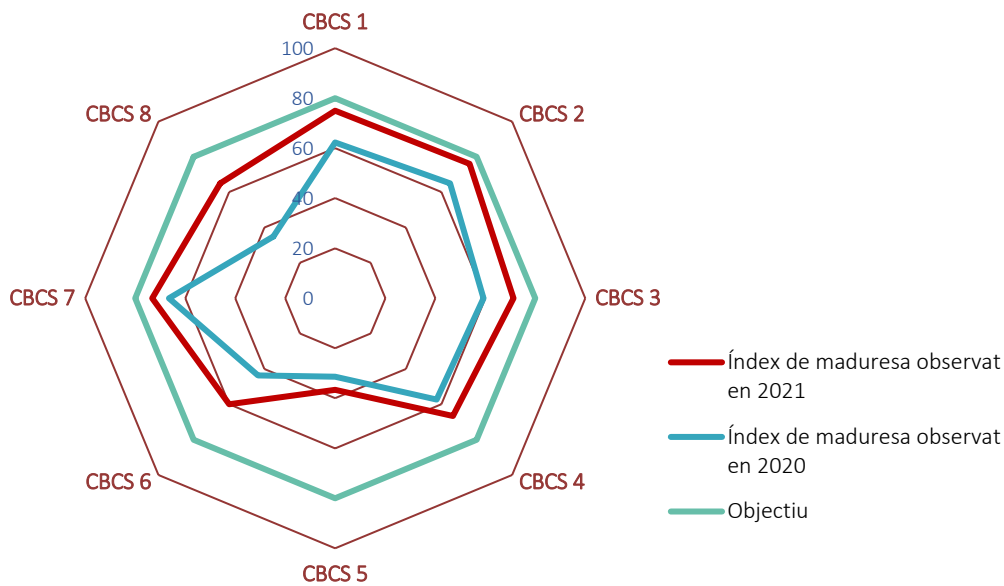
L'índex de compliment dels CBCS és del 81,9%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*. Aquest índex ha millorat des del 65,7% del nostre informe anterior. La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2020 mostra una millora en tots els controls si bé ha sigut insuficient, ja que únicament s'han atés les nostres recomanacions de manera parcial (vegeu l'apartat 5 següent).

A pesar de la millora experimentada, el nivell d'efectivitat en els controls analitzats és insuficient. Hi ha possibilitats clares de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació. 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 2020.



Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



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

L'Ajuntament d'Elda té establida una acceptable governança de la ciberseguretat, però ha de finalitzar les accions iniciades

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 nivell adequat de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament, la qual cosa, juntament amb l'existència d'uns processos de gestió adequats, ens permet afirmar que la governança de ciberseguretat aconsegueix un nivell acceptable.

Hi ha projectes i iniciatives que es troben en fase de planificació o pendents d'implantació que, en cas de ser finalitzats i explotats de manera efectiva, tindran un impacte rellevant des del punt de vista operatiu i de la seguretat. Els òrgans superiors de l'Ajuntament han de mantindre l'actual nivell de compromís i suport amb la seguretat de la informació, a fi de garantir el desenvolupament efectiu dels projectes en curs, consolidar els nivells de maduresa dels controls i solucionar les deficiències identificades.

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 2020, 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 han d'adoptar-se.

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

1. Actualitzar i millorar el procediment de seguretat existent "PR14. Creació i actualització de l'inventari d'actius", de manera que represente amb fidelitat el conjunt de mesures ja implantades per al control dels dispositius físics.
2. Finalitzar el desplegament de les mesures i sistemes planificats que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa, addicionalment a les mesures actualment establides.

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

3. Actualitzar i millorar el procediment de seguretat existent "PR14. Creació i actualització de l'inventari d'actius", de manera que represente amb fidelitat el conjunt de mesures ja implantades per a la gestió integral del programari de l'entitat i que preveja:
 - La formalització de les llistes de programari autoritzat (llistes blanques) actuals, el procés d'autorització per a la instal·lació de programari i les mesures tècniques implantades que impedeixen l'execució del no autoritzat.
 - L'elaboració d'un pla de manteniment de la totalitat del programari utilitzat i que formalitze la gestió actualment realitzada.
4. Finalitzar el procés de renovació en curs per a actualitzar tots els sistemes que es troben fora del període de suport.



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

5. Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:
 - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques i l'anàlisi prèvia a l'entrada en producció dels sistemes.
 - Les accions actualment establides, incloent-hi el seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat, l'ús d'eines de provisió de vacunes i el sistema de revisió de salut d'*endpoint*.
 - La prioritització actualment implantada basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.
6. La sisena recomanació de l'informe de 2020 ha sigut implementada.

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

7. Aprovar un procediment unificat de gestió d'usuaris amb privilegis d'administració que formalitze i amplie el procés actual, que establisca les directrius per a tots els sistemes de l'entitat i que incloga, com a mínim:
 - L'eliminació dels usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió s'han de realitzar 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 utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives).
 - La política d'autenticació que cal aplicar a aquesta mena de comptes, particularment l'autenticació de doble factor en sistemes crítics.

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

8. Aprovar un procediment de configuració segura o fortificació dels sistemes de manera que represente amb fidelitat el conjunt de mesures ja implantades i considere la seguretat per defecte i el criteri de mínima funcionalitat. Es proposa el desenvolupament de guies d'instal·lació específiques per als sistemes que en l'actualitat no en tinguen.



Paral·lelament, s'aconsella incloure en el procediment la gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de preveure la revisió periòdica dels canvis realitzats, 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)

9. Aprovar un procediment per al tractament de *logs* d'auditoria d'activitat d'usuari que represente amb fidelitat el conjunt de mesures ja implantades i especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, les còpies de seguretat, la gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*.

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

10. Actualitzar i millorar el procediment de seguretat existent "PR17. Procediment de generació de còpies de seguretat i recuperació de la informació", de manera que represente amb fidelitat el conjunt de mesures ja implantades per a la gestió de còpies de seguretat de dades i sistemes, i que detalle addicionalment les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.

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

11. Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de:
 - Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010.
 - Publicar en la seu electrònica la certificació de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.
12. 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:
 - Publicar el registre d'activitats de tractament, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.
 - Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.
 - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.



- Planificar i executar auditories de protecció de dades.

13. 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 implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2020, 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 a 13 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 2020.

Tal com es mostra en el quadre 2, de les tretze recomanacions i mesures per al compliment de la legalitat realitzades en aquest informe, dues s'han atés i onze ho han sigut només parcialment.

Actuacions en curs

Encara que no s'han tingut en compte en el càlcul dels indicadors que es mostren en l'apartat 4, hem verificat que en el moment de finalització del treball de camp de l'auditoria s'han iniciat o planificat actuacions en matèria relacionada amb la ciberseguretat, la



implantació efectiva de la qual tindrà un impacte positiu en el nivell de ciberseguretat de l'entitat. 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 2020.

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

- Renovació de la solució de teletreball. A fi de donar resposta a les necessitats sobrevingudes per la pandèmia de la COVID-19 i el nou paradigma de teletreball, s'ha articulats un conjunt de projectes i contractes que es troben en licitació o desplegament i que inclouen mesures relatives a la seguretat perimetral, comunicacions i equips d'usuari.
- Renovació de programari de *back office* municipal. Es troba en procés de licitació la renovació de les aplicacions que donen suport a la gestió comptable, administració electrònica, tributs, padró, patrimoni, etc. La licitació inclou la consideració de mesures de seguretat com ara l'autenticació de doble factor, entre altres.
- Desplegament de la solució EMMA del CCN, que proporciona diferents serveis de seguretat que inclouen visibilitat, control/resposta, segmentació, compliment, BYOD, gestió de convidats i vigilància en accés remot. La solució, proporcionada pel CCN però desplegada i suportada únicament per empreses certificades, es finançarà per mitjà de fons europeus Next Generation EU.



Quadre 2. Seguiment de recomanacions

Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
<p>1 Aprovar el procediment per a la gestió de l'inventari i el control d'actius físics, amb ampliació prèvia perquè incloga les revisions periòdiques de maquinari, incloent-hi les dates d'aquestes revisions.</p>	<p>S'ha elaborat i aprovat un procediment. No obstant això, a aquest procediment li falten el detall i la maduresa necessaris.</p> <p>S'han consolidat en una única eina els diferents inventaris existents.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>2 Complementar amb mesures tècniques o de gestió les solucions actuals que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.</p>	<p>S'ha millorat la implantació de les mesures tècniques existents per a restringir l'accés de dispositius físics no autoritzats.</p> <p>S'han planificat mesures i sistemes de protecció addicionals que es troben pendents de desplegament.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>3 Complementar i aprovar formalment la normativa de seguretat existent, considerant la gestió integral del programari de l'entitat, incloent-hi:</p> <ul style="list-style-type: none"> - L'elaboració de llistes de programari autoritzat (llistes blanques), l'optimització de les mesures tècniques que impedeixen l'execució del no autoritzat i la realització de revisions periòdiques de programari. - La definició d'un pla de manteniment de la totalitat del programari utilitzat a l'Ajuntament. 	<p>S'ha elaborat i aprovat un procediment. No obstant això, a aquest procediment li falten el detall i la maduresa necessaris.</p> <p>S'han implantat determinades mesures tècniques addicionals per a impedir l'ús de programari no autoritzat basades en la protecció d'<i>endpoint</i>.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>4 Identificar i actualitzar tots els sistemes que es troben fora del període de suport.</p>	<p>S'ha actualitzat una part dels sistemes que es trobaven fora del període de suport.</p> <p>Per als sistemes pendents d'actualització, s'han iniciat accions per a reemplaçar-los, que es troben en curs.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</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>Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:</p> <p>5</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 les accions actualment establides de seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat. - La prioritització actualment implantada basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades. 	<p>S'ha desplegat el sistema microCLAUDIA per a la provisió de vacunes davant de codi nociu en equips d'usuari.</p> <p>S'ha desplegat un sistema de protecció d'<i>endpoint</i> que inclou revisió de salut dels sistemes.</p> <p>S'han realitzat amb determinada periodicitat exercicis de <i>hacking</i> ètic.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>6</p> <p>Optimitzar l'ús actual d'eines que permeten la gestió unificada i automatitzada de pedaços de seguretat i altres actualitzacions.</p>	<p>S'han revisat els processos per a explotar les eines disponibles per a la gestió automatitzada de pedaços de seguretat i altres actualitzacions.</p>	<p>Aplicada</p>	<p>S'elimina la recomanació feta en 2020.</p>
<p>Aprovar 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> <p>7</p> <ul style="list-style-type: none"> - L'eliminació, sempre que siga possible des del punt de vista tècnic, dels usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió s'han de realitzar 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 utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques que cal realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives) - La política d'autenticació que cal aplicar a aquest tipus de comptes. 	<p>S'han aplicat millores en el control, incloent-hi l'eliminació d'usuaris no nominatius compartits de determinats sistemes o l'autenticació de doble factor en sistemes crítics.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</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>8 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 dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN.</p> <p>Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha d'incloure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració.</p>	<p>S'han aplicat millores en el control, incloent-hi millores en les plantilles de seguretat dels equips d'usuari i servidors i la inclusió de requisits específics de seguretat en els plecs de prescripcions tècniques per a l'adquisició i desplegament de determinats sistemes crítics de l'entitat.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>9 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, les còpies de seguretat, la gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels <i>logs</i>. Per a la revisió de <i>logs</i> és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.</p>	<p>S'han desplegat mecanismes i sistemes addicionals per a la recollida i emmagatzematge centralitzats de <i>logs</i> de determinats sistemes crítics de l'entitat.</p> <p>S'ha contractat un servei de gestió de resposta a amenaces de sistema de protecció d'<i>endpoint</i> que inclou atenció 24/7 i que proporciona parcialment serveis equivalents a un centre d'operacions de seguretat (SOC).</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>10 Aprovar formalment el procediment existent per a la gestió de còpies de seguretat de dades i sistemes, i complementar-lo perquè 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>S'ha elaborat i aprovat un procediment. No obstant això, a aquest procediment li falta el detall i maduresa necessaris.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</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 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:</p> <ul style="list-style-type: none"> - Aprovar per part de l'òrgan superior competent la política de seguretat (PS) desenvolupada. - Realitzar la designació de les persones per als rols definits en la PS i constitució dels òrgans que s'hi descriuen. - Aprovar la declaració d'aplicabilitat elaborada i adoptar les mesures de seguretat que s'hi descriuen. - Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010. - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents. 	<p>S'han aprovat la política, normativa i procediments de seguretat de la informació.</p> <p>S'han designat els responsables previstos en la política i s'ha creat el comitè de seguretat.</p> <p>S'han elaborat i aprovat la declaració d'aplicabilitat i el pla d'adequació</p> <p>S'ha emplenat i remès l'informe INES.</p> <p>S'ha realitzat, l'any 2021, una auditoria de compliment.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>12 En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i en la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de:</p> <ul style="list-style-type: none"> - Nomenar un DPD d'acord amb el que es preveu en l'article 37.1.a de l'RGPD. - Elaborar el registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018. - Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD. - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD. - Planificar i executar auditories de protecció de dades. 	<p>S'ha realitzat el nomenament de delegat de protecció de dades (DPD).</p> <p>S'ha elaborat un registre d'activitats del tractament.</p>	<p>Aplicada parcialment</p>	<p>S'actualitza la redacció feta en 2020.</p>
<p>13 Dura a terme l'auditoria del registre de factures exigida per la Llei 25/2013, de 27 de desembre.</p>	<p>S'ha realitzat l'auditoria del registre de factures de l'exercici 2020.</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 realitza amb el suport de complexos sistemes informatitzats, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de tot tipus provinents del ciberespai, majors riscos de ciberseguretat i s'han multiplicat els incidents de seguretat de què són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials –i en molts casos, reals– tant econòmiques com en la prestació dels serveis públics.

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

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

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

Tot i que l'adopció de mesures de seguretat adequades fa més resilients les organitzacions davant dels ciberatacs, l'anàlisi dels incidents produïts que es realitza en els informes INES² del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs es mantinguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan implementades correctament.

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

² Informe Nacional de l'Estat de Seguretat dels Sistemes de les TIC del CCN.



Objectiu de l'auditoria

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022, el nostre objectiu ha sigut realitzar el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elda. Exercici 2020, 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 disseny³ com la seua eficàcia operativa⁴ per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport. També hem revisat el compliment de la normativa bàsica relativa a la seguretat de la informació.

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

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

Abast

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

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

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

³ 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.

⁴ 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.

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

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

Àmbit temporal

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

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

Metodologia

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

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

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



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

La guia pràctica de fiscalització dels OCEX 5313

La guia pràctica de fiscalització dels OCEX GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat", va ser aprovada per la Conferència de Presidents dels Òrgans de Control Extern el 12 de novembre de 2018, i forma part del *Manual de fiscalització* de la Sindicatura de Comptes, que pot consultar-se 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),⁵ que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. L'avantatge principal d'aquests controls és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant ciberatacs al voltant del 85%. Si s'implementen els vint controls el risc es pot reduir un 94%.

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

⁵ 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) assenyala⁶ que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen" i reduir els ciberriscos.⁷

Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.⁸

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

⁶ [Review of Cyber Hygiene Practices](#), ENISA, desembre de 2016. Vegeu la pàgina 14.

⁷ 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.

⁸ 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 què s'especifica amb el màxim detall els aspectes comprovats en cada control.



Quadre 5. Els CBCS i els seus subcontrols

Control	Objectiu del control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots els dispositius de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats	L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
		CBCS 1-2: Control d'actius físics no autoritzats	L'entitat disposa de mesures de seguretat per a controlar (detectar i restringir) l'accés de dispositius físics no autoritzats.
CBCS 2 Inventari i control de programari autoritzat	Gestionar activament tot el programari en els sistemes, de manera que només es puga instal·lar i executar programari autoritzat.	CBCS 2-1: Inventari de programari autoritzat	L'entitat disposa d'un inventari de programari complet, actualitzat i detallat.
		CBCS 2-2: Programari suportat pel fabricant	El programari utilitzat per l'entitat té suport del fabricant. En cas contrari, es marca en l'inventari com fora de suport.
		CBCS 2-3: Control de programari no autoritzat	L'entitat disposa de mecanismes que impedeixen la instal·lació i execució de programari no autoritzat.
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per a 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 permeta la recuperació de la informació en temps oportú.	CBCS 7-1: Realització de còpies de seguretat	L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema.
		CBCS 7-2: Realització de proves de recuperació	Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica, i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmises 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	<p>Cobreix al 100% l'objectiu de control i:</p> <ul style="list-style-type: none">- El procediment està formalitzat (documentat i aprovat) i actualitzat.- El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	<p>En línies generals, compleix l'objectiu de control, si bé pot haver-hi certs aspectes no coberts al 100% i:</p> <ul style="list-style-type: none">- Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.).- Les proves realitzades per a verificar la implementació són satisfactòries.- S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	<p>Cobreix de forma molt limitada l'objectiu de control i:</p> <ul style="list-style-type: none">- Se segueix un procediment, encara que pot no estar formalitzat.- El resultat de les proves d'implementació i d'eficàcia no és satisfactori. <p>Cobreix en línies generals l'objectiu de control, però:</p> <ul style="list-style-type: none">- No se segueix un procediment clar.- Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	<p>No cobreix l'objectiu de control.</p> <p>El disseny cobreix l'objectiu de control, però el resultat de la revisió realitzada posa de manifest que la implementació o l'eficàcia operativa del control no són satisfactòries (s'han detectat incompliments significatius i generalitzats).</p>

Controls

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



OCEX 5313, que al seu torn 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 qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.</i> <i>En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.</i>
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. <i>El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.</i> <i>S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, utilitzant-se com a indicadors en la gestió de la millora dels processos.</i> <i>En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes a base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.</i>



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

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

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

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

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

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

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

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



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

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

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

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

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

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

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:⁹

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%.

⁹ *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 gestiona adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una forma responsable.¹⁰

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.**¹¹

La responsabilitat sobre aquest procés és de l'alta direcció, que, en el cas dels ajuntaments, correspon al seu alcalde 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.

¹⁰ Vegeu el [glossari de la Information Systems Audit and Control Association \(ISACA\)](#).

¹¹ 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.¹² L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació,¹³ que ha de materialitzar-se en aspectes com ara:

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

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

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

La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,¹⁴ que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat, i és la màxima autoritat en l'organització respecte a les decisions de seguretat que afecten els sistemes que manegen informació o presten algun servei. La seua composició ha de constar en la PSI.

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

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

- Decidir els criteris de valoració 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.

¹² [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.

¹³ [UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información](#), apartat 3.4.

¹⁴ [Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC](#), CCN, gener de 2021.



Seguiment de les recomanacions

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

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

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

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

Comunicació i confidencialitat

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



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



APÈNDIX 2

Situació dels controls bàsics de ciberseguretat



CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

L'Ajuntament ha elaborat i aprovat un procediment que recull la responsabilitat respecte a l'inventariat d'actius. No obstant això, al procediment li falten el detall i la maduresa necessaris.

La gestió de l'inventari ha sigut millorada després de la consolidació en una única eina dels diferents inventaris existents en l'auditoria anterior.

S'han implantat correctament mesures tècniques per a restringir l'accés de dispositius físics no autoritzats que en l'auditoria anterior vam observar que únicament s'havien desplegat parcialment. A més, s'han planificat mesures i sistemes de protecció addicionals que es troben pendents de desplegament.

Hi ha un cert nivell de control sobre l'inventari i el control d'actius físics, i la seua valoració global aconsegueix un **índex de maduresa del 75,0%**, pròxim a l'objectiu, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 1 del 93,8%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 62,3%, que es correspon amb un nivell de maduresa N2, *repetible però intuïtiu*. Per tant, s'ha produït una millora de 12,7 punts en l'índex de maduresa del control.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

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

Situació del control

L'Ajuntament ha elaborat i aprovat un procediment que recull la responsabilitat respecte a l'inventariat de programari. No obstant això, al procediment li falta el detall i la maduresa necessaris.



Hem verificat que s'ha actualitzat la major part dels sistemes que es trobaven fora del període de suport. No obstant això, encara hi ha un limitat nombre de sistemes pendents d'actualització, per als quals s'han iniciat accions per a reemplaçar-los que es troben en curs.

Adicionalment, l'entitat ha implantat determinades mesures per a impedir l'ús de programari no autoritzat. Aquestes mesures inclouen la protecció d'*endpoint*¹⁵ per a impedir l'ús d'aplicacions que no es troben en les llistes d'aplicacions reconegudes per defecte i el control d'aplicacions a nivell perimetral.

Hi ha un cert nivell de control sobre l'inventari i control de programari autoritzat, que aconseguix un **índex de maduresa del 76,0%**, pròxim a l'objectiu, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 2 del 95,0%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 65,0%, que es correspon amb un nivell de maduresa N2, *repetible però intuïtiu*. Per tant, s'ha produït una millora d'11 punts en l'índex de maduresa del control.

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

Objectiu del control

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

Situació del control

Hem analitzat la gestió de les vulnerabilitats dels sistemes i hem observat que s'han implantat mesures addicionals per a la identificació i resolució de vulnerabilitats, però no s'ha desenvolupat, i formalment aprovat, un procediment a aquest efecte.

L'Ajuntament ha implantat l'eina microCLAUDIA del Centre Criptològic Nacional. Hem verificat que s'ha instal·lat adequadament en els sistemes Windows de la corporació i es realitzen els corresponents desplegaments de vacunes davant de codi nociu.

S'ha desplegat un sistema de protecció d'*endpoint* que inclou paràmetres de revisió de salut dels sistemes. Si bé aquest sistema es trobava disponible en l'auditoria anterior, no s'havia desplegat completament per a totes les seues funcionalitats.

¹⁵ Un punt final o *endpoint* és un dispositiu informàtic remot que es comunica a través d'una xarxa a la qual està connectat. Es refereix típicament a dispositius utilitzats com ara ordinadors d'escriptori, portàtils, telèfons intel·ligents, tauletes o dispositius d'Internet de les coses.



A més, es realitzen amb determinada periodicitat exercicis de *hacking* ètic, tant externs, per mitjà de la contractació dels serveis, com interns, a través de l'ús de noves eines específiques instal·lades.

Sobre la gestió de pedaços i actualitzacions, s'han revisat els processos per a explotar adequadament les eines disponibles per a la gestió automatitzada de pedaços de seguretat i actualitzacions, incloent-hi revisions periòdiques del desplegament d'actualitzacions.

Hi ha un cert nivell de control sobre la gestió de vulnerabilitats, i la valoració global del control és d'un **índex de maduresa del 71,3%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 3 del 89,1%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 59,3%, que es correspon amb un nivell de maduresa N2, *repetible però intuïtiu*. Per tant, s'ha produït una millora de 12 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

Hem analitzat la gestió realitzada dels comptes d'administració en els diferents sistemes i hem verificat que, encara que no s'ha desenvolupat i aprovat un procediment a aquest efecte, s'han aplicat determinades millores en el control d'aquests comptes.

Hem verificat que s'han eliminat els usuaris no nominatius compartits de determinats sistemes.

Per als sistemes que disposen d'usuaris per defecte, hem verificat que es troba en llicitació la seua renovació, incloent-hi requisits de seguretat en aquest projecte.

A més, s'ha aprovat una política de contrasenyes aplicada de manera homogènia en tots els sistemes. Hem constatat que s'han aplicat mesures de seguretat addicionals a determinats sistemes crítics, com ara l'autenticació de doble factor.

Hi ha un cert nivell de control sobre els comptes amb privilegis administratius, per la qual cosa la valoració global del control existent aconsegueix un **índex de maduresa del 66,6%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment d'aquest CBCS 4 del 83,3%**.



La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 57,3%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 9,3 punts en l'índex de maduresa del control.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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

Situació del control

L'Ajuntament ha aplicat determinades millores tècniques i organitzatives en el control. No obstant això, no s'ha elaborat i aprovat un procediment sobre la gestió de canvis i la configuració segura dels sistemes

Hem verificat que s'han realitzat millores en les plantilles de seguretat dels equips d'usuari i servidors. A més, s'han inclòs requisits específics de seguretat en els plecs de prescripcions tècniques per a l'adquisició i desplegaments de determinats sistemes crítics de l'entitat.

No obstant això, no es disposa de plantilles de configuració amb caràcter de fortificació per a tots els sistemes de l'entitat, particularment per als sistemes crítics. Ni es disposa de sistemes que permeten monitorar en temps real la integritat de les configuracions.

La valoració global del control existent sobre les configuracions segures és que l'organització aconsegueix un **índex de maduresa del 36,6%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 45,8%**.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 31,4%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una insuficient millora de 5,2 punts en l'índex de maduresa del control.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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



Situació del control

Hem analitzat les accions de l'Ajuntament per al registre de l'activitat dels usuaris en els diferents sistemes i hem verificat que, encara que s'han aplicat certes mesures addicionals, no s'ha elaborat i aprovat un procediment.

Hem verificat que s'han desplegat mecanismes i sistemes addicionals per a la recollida i emmagatzematge centralitzats de *logs* de determinats sistemes crítics de l'entitat, incloent-hi el servidor de directori, el tallafoc i el sistema de protecció d'*endpoint*, si bé l'explotació d'aquests *logs* únicament es realitza de manera reactiva davant determinats esdeveniments.

A més, s'ha contractat un servei de gestió de resposta a amenaces del sistema de protecció d'*endpoint* que inclou atenció 24/7. Aquest servei, que proporciona parcialment serveis equivalents a un centre d'operacions de seguretat (SOC), inclou la cerca d'amenaces, detecció d'atacs i el servei de solució.

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

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 43,7%, que es correspon amb un nivell de maduresa N1, *inicial/ad hoc*. Per tant, s'ha produït una millora de 16,3 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 permeti la recuperació de la informació en temps oportú.

Situació del control

L'Ajuntament ha elaborat i aprovat un procediment sobre la gestió de còpies de seguretat de dades i sistemes. No obstant això, al procediment li falta el detall i la maduresa necessaris.

A més, hem verificat que s'han aplicat determinades mesures addicionals de protecció a les còpies realitzades.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 73,2%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però hi ha controls parcialment establerts o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 91,5%**.



La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 66,5%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*. Per tant, s'ha produït una millora de 6,7 punts en l'índex de maduresa del control.

CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT

Objectiu del control

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

Situació del control

Compliment de l'ENS

Des de la revisió realitzada l'any 2020, l'Ajuntament ha realitzat les següents accions que han millorat el nivell de compliment exigint pel Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica:

- El dia 30 d'abril de 2021, el Ple municipal va acordar l'aprovació de la política, normativa i procediments de seguretat de la informació, d'acord amb l'Esquema Nacional de Seguretat.
- A conseqüència de l'aprovació de la política de seguretat de la informació, es van designar els responsables previstos en la política i es va crear el comitè de seguretat.
- S'han elaborat i aprovat la declaració d'aplicabilitat i el pla d'adequació.
- S'ha emplenat i remés anualment l'Informe de l'Estat de la Seguretat (Informe INES).
- S'ha realitzat l'any 2021 una revisió de compliment.

A pesar de les iniciatives anteriors, hi ha mancances que s'han d'esmenar:

- No s'ha implantat la totalitat de les mesures de seguretat i accions previstes en la declaració d'aplicabilitat i el pla d'adequació.
- No s'ha certificat el compliment de l'ENS.

Compliment de l'RGPD

Quant al compliment en matèria de protecció de dades personals, des de la revisió de l'any 2020 l'Ajuntament ha realitzat accions que han millorat el nivell de compliment de les exigències de l'RGPD.

S'ha nomenat un delegat de protecció de dades (DPD), tal com exigeix l'RGPD en el seu article 37.



S'ha elaborat un registre d'activitats del tractament, segons s'especifica en l'article 30 de l'RGPD.

A més, s'ha contractat un servei de consultoria i suport tècnic en matèria de seguretat de la informació i de protecció de dades que ha iniciat diverses tasques a fi de donar compliment a les obligacions de l'RGPD.

No obstant això, hi ha mancances que s'han d'esmenar:

- No s'ha publicat el registre d'activitats del tractament ni és accessible per mitjans electrònics, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.
- No s'han realitzat les anàlisis de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.
- No s'han aplicat les mesures organitzatives i tècniques necessàries per a protegir les dades personals, requerides per l'article 24.1 de l'RGPD.
- No s'han executat auditories de compliment en matèria de protecció de dades.

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

Compliment de la legalitat del registre de factures

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

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió ha millorat respecte a l'informe emés l'any 2020 i l'Ajuntament ha aconseguit un **índex de maduresa del 65,0%**, que es correspon amb un **nivell de maduresa N2**, que indica que encara existeixen incompliments significatius de la normativa, i hi ha aspectes que s'han de millorar.

La situació del control en l'informe realitzat l'any 2020 mostrava un índex de maduresa del 35,0%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora substancial de 30,0 punts en l'índex de maduresa del control.

Governança de ciberseguretat

L'Ajuntament d'Elda té establida una acceptable governança de la ciberseguretat, però ha de finalitzar les accions iniciades.

Hem pogut verificar l'existència d'un adequat nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament, la qual cosa, juntament amb l'existència d'uns adequats processos de gestió, ens permet afirmar que la governança de



ciberseguretat aconseguix un nivell acceptable. Els aspectes fonamentals identificats que sustenten aquesta afirmació són:

- La participació activa de l'alta direcció en la gestió de la seguretat de la informació i en els processos establits per a gestió de riscos.
- L'existència d'una política de seguretat de la informació aprovada, que constitueix el conjunt de directrius i principis que representen el compromís de l'entitat respecte a la protecció dels actius d'informació de l'Ajuntament.
- La definició i nomenament de rols, i la creació d'òrgans de govern de la seguretat de la informació, particularment el responsable de seguretat, el DPD, i el comitè de seguretat TIC. Hem verificat que existeixen i exerceixen de manera efectiva i continuada les funcions establides.
- El compromís amb la gestió i el compliment de requisits legals fonamentals relacionats amb la seguretat de la informació.
- La realització d'inversions que permeten donar compliment als objectius estratègics en matèria de seguretat, incloent-hi el desenvolupament de projectes i la implantació de sistemes que han contribuït decisivament a l'establiment de controls tècnics, sense perjudici de les millores encara necessàries.
- L'articulació de projectes, en el context d'utilització dels fons Next Generation EU, que tenen com a objecte promoure la seguretat de la informació, eliminar les mancances més rellevants identificades i aconseguir el compliment normatiu.

Hi ha projectes i iniciatives que es troben en fase de planificació o pendents d'implantació que, en cas de ser finalitzats i explotats de manera efectiva, tindran un impacte rellevant des del punt de vista operatiu i de la seguretat.



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.

Protecció d'endpoint i control d'accés a xarxa

L'Ajuntament ha adquirit i implantat una eina de protecció d'endpoint que disposa d'un conjunt de solucions que proporcionen un adequat nivell de protecció en els equips dels usuaris. Aquest conjunt de solucions inclou la classificació dels actius en diferents nivells de salut depenent del seu estat respecte a diferents variables de seguretat.



La solució d'*endpoint* ha sigut integrada amb el sistema de protecció perimetral d'una manera particularment efectiva, que permet l'accés a les xarxes internes de l'Ajuntament únicament a aquells actius que disposen de l'agent de protecció d'*endpoint* i aconseguisquen un nivell de salut mínim determinat.

Explotació de l'eina de ticketing en determinats processos de l'entitat

L'entitat ha desplegat una eina de *ticketing* i gestió de fluxos de treball que ha sigut integrada amb determinats sistemes i processos interns d'una manera particularment efectiva.

Les implementacions i funcionalitats més rellevants de l'eina són:

- La gestió de llicències i contractes de manteniment.
- La gestió de la resolució de vulnerabilitats identificades.
- La gestió de projectes.

Servei de suport de gestió de resposta a amenaces 24/7

L'entitat disposa d'un servei extern de gestió de resposta a amenaces d'*endpoint* amb suport 24/7, servei que inclou la cerca d'amenaces, la detecció d'atacs i el servei de solució. Aquest servei, facilitat pel fabricant d'un dels sistemes de seguretat de l'entitat, proporciona de manera parcial serveis equivalents a un centre d'operacions de seguretat (SOC).



ACRÒNIMS I GLOSSARI DE TERMES

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

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

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

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

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

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



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

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

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

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

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

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



TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que es preveu en la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir amb el regidor de Recursos Humans i Modernització 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 1 de juny de 2022, va aprovar aquest informe d'auditoria.



Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Informe seguiment recomanacions ciberseguretad Ajuntament Elda. 2020 - SEFYCU 3307541

Puede acceder a este documento en formato PDF - PAdES y comprobar su autenticidad en la Sede Electrónica usando el código CSV siguiente:



URL (dirección en Internet) de la Sede Electrónica: <https://sindicom.sedipualba.es/>

Código Seguro de Verificación (CSV): KUAA V33E HCWN CYYP DA4F

En dicha dirección puede obtener más información técnica sobre el proceso de firma, así como descargar las firmas y sellos en formato XAdES correspondientes.

Resumen de firmas y/o sellos electrónicos de este documento

Huella del documento
para el firmante

Texto de la firma

Datos adicionales de la firma



Vicent Cucarella Tormo
Síndic Major

Firma electrónica - ACCV - 09/06/2022 7:19
VICENT CUCARELLA TORMO