SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SEGUIMENT DE LES RECOMANACIONS REALITZADES EN L'INFORME D'AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DE L'AJUNTAMENT DE VALÈNCIA DE L'ANY 2019

Situació a 31 de desembre de 2021

RESUM

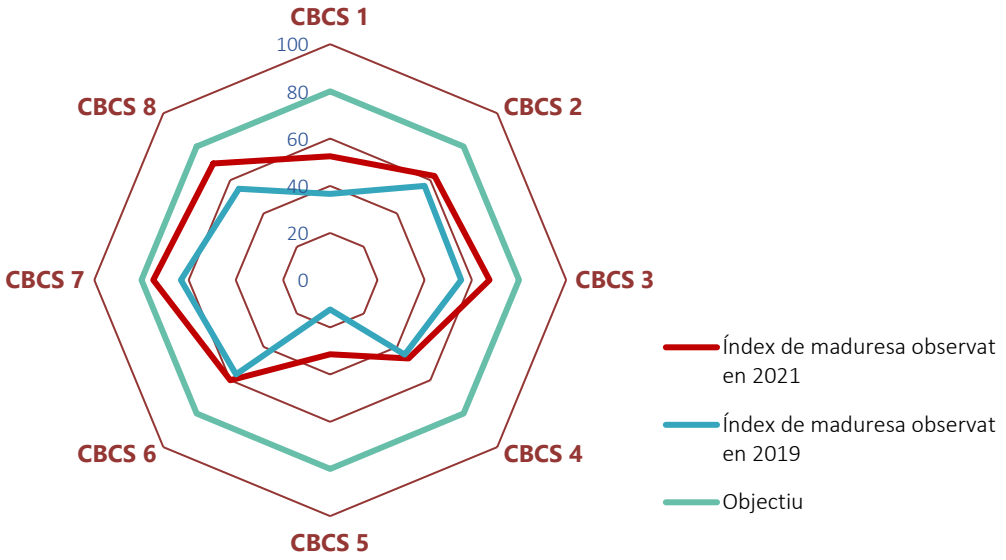
La transformació digital que estan experimentant totes les administracions públiques i la seua interconnexió a través de complexes xarxes informàtiques les exposa de manera cada vegada més intensa a amenaces provinents del ciberespai. Això origina un increment dels riscos associats als sistemes d'informació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

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

Conclusions i recomanacions

Encara que s'han fet progressos des de la nostra auditoria anterior i les nostres recomanacions s'han atés parcialment, l'índex de maduresa general dels controls bàsics de ciberseguretat mostra un valor del 58,2% (47,5% en 2019), i per tant el nivell d'efectivitat en els controls analitzats continua sent insuficient i ha de millorar per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en els controls que presenten deficiències significatives.

L'Ajuntament té en marxa un conjunt de projectes que, si s'executen i es gestionen adequadament, contribuiran a millorar substancialment els nivells de ciberseguretat dels seus sistemes d'informació, un aspecte crític per la seua grandària i complexitat.



L'Ajuntament de València té establida una acceptable governança de la ciberseguretat, però té pendent de constituir el comité de seguretat de la informació.

Els òrgans superiors de l'Ajuntament han de mantindre l'actual nivell de compromís i suport a la seguretat de la informació, a fi de garantir el desenvolupament efectiu dels projectes en curs, millorar els nivells de maduresa dels controls i solucionar les deficiències identificades.

Així mateix, la nostra revisió també ha posat de manifest que el grau de compliment quant a l'adequació a les normes legals relacionades amb la seguretat de la informació ha millorat, però continuen havent-hi incompliments que s'han d'esmenar. L'informe assenyala diversos aspectes sobre els quals s'ha d'actuar per a una ràpida esmena. En relació amb l'Esquema Nacional de Seguretat, l'Ajuntament ha d'actualitzar i aprovar la política de seguretat perquè s'adapte a les noves circumstàncies tècniques i organitzatives, incloent-hi la regulació dels rols de seguretat i el comité de seguretat.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament, entre les quals aconsellem formalitzar un procediment unificat per a gestió d'usuaris amb privilegis d'administració, finalitzar la implantació de les solucions adquirides per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa i finalitzar les actuacions iniciades i planificades per a actualitzar tots els sistemes que es troben fora del període de suport.

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 l'informe complet per a conéixer el veritable abast del treball realitzat.

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

Situació a 31 de desembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

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

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

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 4 de març de 2020 el Consell de la Sindicatura de Comptes va aprovar l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València. Exercici 2019. Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 la realització d'un treball de seguiment de la situació dels controls bàsics de ciberseguretat d'aquest ajuntament i dels altres 14 ajuntaments analitzats.

La necessitat d'una ciberhigiene adequada

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

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

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

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

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

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

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats, proporcionar una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a 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 2019, relacionats amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interés general.

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

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

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

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

Canvi en els sistemes d'informació auditats

El conjunt d'aplicacions que proporciona suport per a la gestió comptable i pressupostària de l'Ajuntament, inclòs el Sistema d'Informació Econòmic Municipal (SIEM), s'ha substituït en 2022 per un nou sistema tecnològicament més complex i avançat denominat SEDA. En l'auditoria actual realitzada en 2022 s'ha omés la revisió del sistema utilitzat fins a l'any 2021, atés que ja no s'estava utilitzant.

La revisió del nou sistema SEDA, que inclou el SIEM anterior i una pluralitat d'altres aplicacions de gestió econòmica, no s'ha inclòs en aquest treball i és objecte d'una auditoria de seguretat específica amb més profunditat.

4. CONCLUSIONS

Encara que s'han realitzat progressos des de la nostra auditoria anterior i les nostres recomanacions s'han atés parcialment, l'índex de maduresa general dels CBCS continua sent insuficient.

L'Ajuntament té en marxa un conjunt de projectes que, si s'executen i gestionen adequadament, contribuiran a millorar substancialment els nivells de ciberseguretat dels seus sistemes d'informació, aspecte crític atesa la seua grandària i complexitat.

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconsegueix un **índex de maduresa general del 58,2%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o no formalitzats documentalment.

L'Ajuntament ha atés de manera parcial les nostres recomanacions i l'índex de maduresa general ha millorat des del 47,5% identificat en la nostra auditoria de 2019, però l'índex de maduresa actual continua sent insuficient per a garantir un adequat grau de seguretat i aconseguir el 80% requerit per l'ENS. Els resultats detallats obtinguts per a cada un dels CBCS i la seua evolució es mostren en el quadre 1.

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

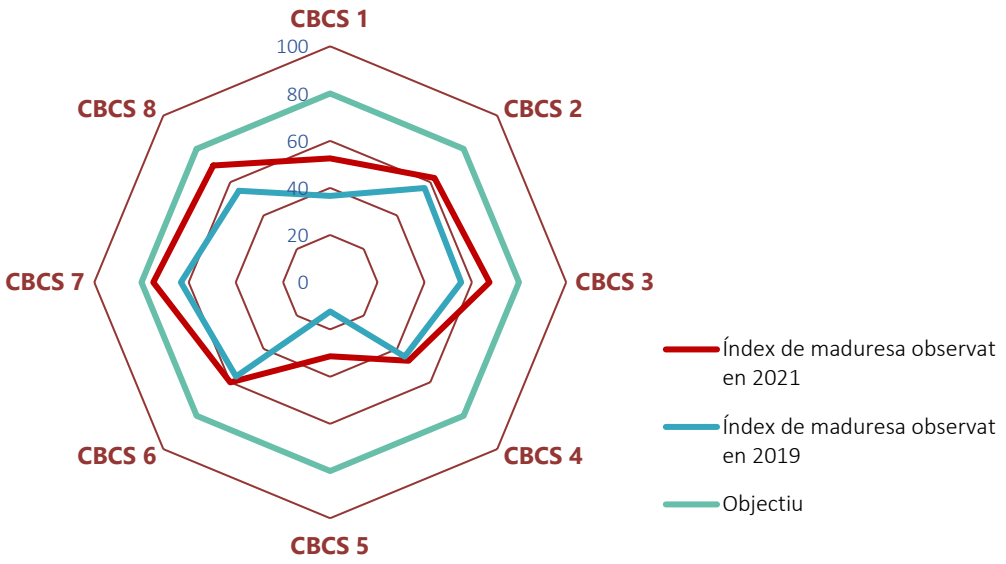
Control	2019			2021		
	Índex de maduresa	Nivell de maduresa	Índex de compli-ment	Índex de maduresa	Nivell de maduresa	Índex de compli-ment
CBCS 1 Inventari i control de dispositius físics	*36,6%*	***N1***	*45,8%*	52,5%	N2	65,6%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	*56,5%*	*N2*	*70,6%*	62,5%	N2	78,1%
CBCS 3 Procés continu d'identificació i remediació de vulnerabilitats	*55,5%*	*N2*	*69,4%*	67,5%	N2	84,4%
CBCS 4 Ús controlat de privilegis administratius	*44,6%*	***N1***	*55,7%*	47,0%	**N1**	58,7%
CBCS 5 Configuracions segures del programari i maquinari	*12,4%*	***N1***	*15,5%*	31,4%	**N1**	39,2%
CBCS 6 Registre de l'activitat dels usuaris	*56,5%*	*N2*	*70,6%*	60,0%	N2	75,0%
CBCS 7 Còpies de seguretat de dades i sistemes	*63,3%*	*N2*	*79,2%*	75,0%	N2	93,8%
CBCS 8 Compliment normatiu i governança de ciberseguretat	*54,8%*	*N2*	*68,4%*	70,0%	N2	87,5%
General	47,5%	***N1***	59,4%	58,2%	N2	72,8%

L'índex de compliment dels CBCS és del 72,8%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80%. Aquest índex ha millorat des del 59,4% del nostre informe anterior.

La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una millora en tots els controls. No obstant això, a pesar de la millora experimentada, el nivell d'efectivitat en els controls analitzats és insuficient, ja que cap aconsegueix l'objectiu i hi ha clares possibilitats de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació, i particularment sobre els controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 4 i 5). En l'apartat 5 es fan les recomanacions pertinents amb aquesta finalitat.

D'una manera més sintètica i gràfica, la situació observada dels controls queda reflectida en el gràfic 1, tant d'aquesta auditoria com de la realitzada l'any 2019.

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



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

L'Ajuntament de València té establida una acceptable governança de la ciberseguretat, però té pendent de constituir el comité de seguretat de la informació. S'ha de mantindre el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació, i 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 de seguretat adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió

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

Hem pogut verificar l'existència d'un 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 processos de gestió adequats, ens permet concloure que la governança de ciberseguretat aconsegueix un nivell acceptable.

No obstant això, hem identificat alguna mancança rellevant, com la inexistència d'un comité de seguretat, que ha de ser esmenada. També cal separar la responsabilitat de la seguretat dels sistemes d'informació de la responsabilitat sobre l'explotació d'aquests sistemes.

Hi ha projectes i iniciatives que es troben en fase d'execució o de planificació que, en cas de finalitzar-se i gestionar-se de manera efectiva, tindran un impacte positiu des del punt de vista operatiu i de la seguretat. A més, hi ha una planificació estratègica de la seguretat de la informació que s'ha materialitzat en el Pla Director de Seguretat dels Sistemes d'Informació, aprovat per la Junta de Govern el 23 de desembre de l'any 2021, que orienta de manera coherent les accions en aquesta matèria.

Els òrgans superiors de l'Ajuntament han de mantindre el nivell actual de compromís i suport a la seguretat de la informació, a fi de garantir el desenvolupament efectiu dels projectes en curs, millorar 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 ha millorat, però continuen existint incompliments que s'han d'esmenar.

La revisió del compliment de legalitat en matèria relacionada amb la seguretat de la informació ha posat de manifest un grau de compliment acceptable, però persisteixen incompliments que s'assenyalen en l'apartat 5, sobre els quals s'ha d'actuar per a una ràpida esmena.

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

Per a esmenar les deficiències de control identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 4 anterior, reformulem les recomanacions que es van efectuar en l'auditoria de 2019, considerant, si és el cas, les

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

millores realitzades des d'aquell moment. L'Ajuntament ha de dedicar els esforços i recursos necessaris per a esmenar les deficiències pendents.

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

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

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

   Finalitzar la implantació de l'eina adquirida per a l'inventari automàtic de dispositius d'usuari.

2. Finalitzar la implantació de les soluciones adquirides per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

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

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

   - L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques del programari instal·lat.
   - La definició d'un pla de manteniment de la totalitat del programari utilitzat a l'Ajuntament.

4. Finalitzar les actuacions iniciades i planificades 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 o incloure en algun dels procediments de seguretat el procés d'identificació i solució de vulnerabilitats, incloent-hi l'anàlisi prèvia a l'entrada en producció dels sistemes, la priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats, identificant dates, prioritat, responsable, solució, etc.

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

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

   - L'eliminació de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió han de realitzar-se amb usuaris nominatius.

- Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.

- La utilització, per cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives).

- La política d'autenticació que cal aplicar a aquest tipus de comptes.

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

7. Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el principi de mínim privilegi. Per a això, es proposa el desenvolupament de guies de seguretat 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.[3]

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

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

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

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

9. Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, la matriu d'assignació de responsabilitats, el control del procés per mitjà de l'eina de gestió de fluxos de treball, les proves de restauració i els requisits de protecció de les còpies.

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

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

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

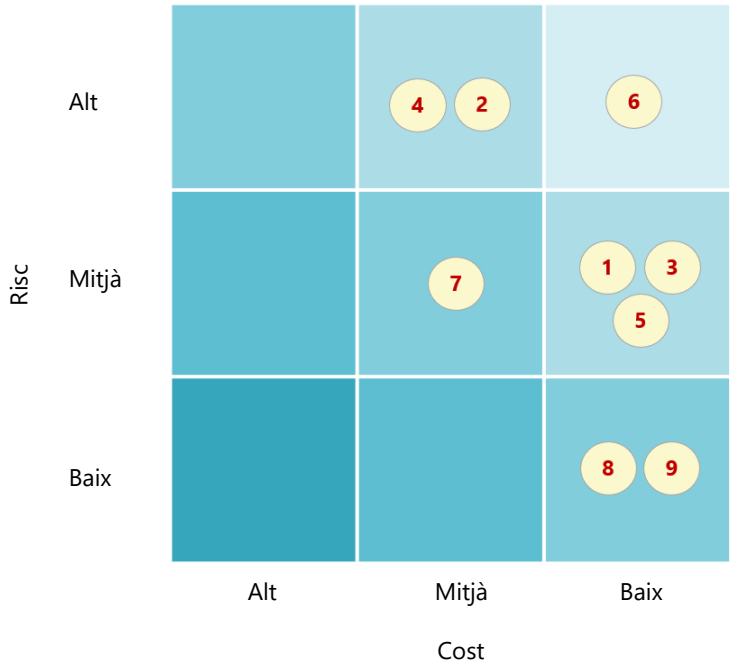
    - Actualitzar i aprovar la política de seguretat perquè s'adapte a les noves circumstàncies tècniques i organitzatives, incloent-hi la regulació dels rols de seguretat i el comité de seguretat.

    - Ha d'actualitzar-se l'auditoria de seguretat i obtindre i publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.

Priorització de les recomanacions

A fi que es puguen establir accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial a mitigar** i **cost estimat de la seua implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2019 adaptant la relació risc/cost de cada recomanació considerant les millores realitzades des de la revisió anterior. No s'hi inclou el punt 10 anterior, ja que és una mesura de compliment obligat.

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



Seguiment de recomanacions anteriors

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

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

Quadre 2. Seguiment de recomanacions

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
1	Aprovar formalment un procediment per a la gestió de l'inventari i el control d'actius físics que reculla el procés complet, incloent-hi les revisions periòdiques de maquinari, actualitzant degudament l'inventari i incloent-hi les dates d'aquestes revisions. A l'hora de garantir un nivell d'actualització adequat de l'inventari, és aconsellable fer prevaldre l'ús d'eines per a la detecció i actualització automàtica dels elements del sistema d'informació davant de procediments manuals.	S'ha adquirit una eina que realitza l'inventari automàtic de tots els equips que disposen d'agent. No obstant això, l'eina no s'ha desenvolupat completament i únicament fa la gestió d'una part dels equips de l'entitat.	Aplicada parcialment	S'actualitza la redacció anterior
2	Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.	S'han adquirit dues eines, una per a la gestió de dispositius per mitjà de connexions sense fils i una altra per mitjà de connexions cablejades. No obstant això, aquesta última es troba en una fase inicial de projecte.	Aplicada parcialment	S'actualitza la redacció anterior
3	Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga: - L'elaboració de llistes de programari autoritzat (llistes blanques) com a complement del procediment existent, la implantació de les mesures tècniques que impedisquen l'execució de programari no autoritzat i la realització de revisions periòdiques de programari. - La definició d'un pla de manteniment de la totalitat del programari utilitzat, incloent-hi tant el gestionat a través de licitacions i clàusules contractuals com la resta de programari utilitzat a l'Ajuntament.	L'eina adquirida per a l'inventariat automàtic d'equips fa l'inventari del programari instal·lat en tots els dispositius amb agent. Aquesta eina permet la realització de revisions periòdiques de programari per a identificar la instal·lació de programari no autoritzat. No obstant això, l'eina no s'ha desplegat completament i únicament realitza la gestió d'una part dels equips de l'entitat.	Aplicada parcialment	Es manté la redacció, ja que continua vigent
4	Revisar i actualitzar tots els sistemes que es troben fora del període de suport.	L'Ajuntament ha actualitzat part dels equips d'usuari que tenien els sistemes operatius sense suport del fabricant.	Aplicada parcialment	S'actualitza la redacció anterior

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
5	Aprovar o incloure en algun dels procediments de seguretat el procés d'identificació i solució de vulnerabilitats, incloent-hi l'anàlisi prèvia a l'entrada en producció dels sistemes, la priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats, identificant dates, prioritat, responsable, solució, etc. Per a la millora dels processos existents d'identificació de vulnerabilitats es proposa l'ús d'eines d'escaneig i la realització de tests de penetració.	L'Ajuntament ha realitzat el desplegament de l'eina microCLAUDIA del CCN en els sistemes i equips d'usuari de l'entitat. A més, ha adquirit una eina que realitza la gestió centralitzada de pedaços i actualitzacions de tot el programari instal·lat en els equips, incloent-hi sistemes operatius i aplicacions. No obstant això, l'eina no s'ha desplegat completament i únicament realitza la gestió d'una part dels equips de l'entitat. S'han realitzat diversos exercicis de *hacking* ètic a fi d'avaluar l'estat de seguretat dels sistemes d'informació.	**Aplicada parcialment**	S'actualitza la redacció anterior
6	Ajustar la instal·lació de la sonda del CCN de manera que permeta la identificació inequívoca de l'origen dels esdeveniments de seguretat.	L'Ajuntament ha desplegat les solucions CARMEN i SAT-INET, que permeten identificar intents d'intrusió i realitzen la detecció en temps real d'amenaces i incidents.	**Totalment o substancialment aplicada**	S'elimina la recomanació
7	Formalitzar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga: - L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió s'han de realitzar amb usuaris nominatius. - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes. - La 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.	L'Ajuntament ha establit l'ús de doble factor d'autenticació en l'eina de virtualització d'aplicacions. A més, hi ha un projecte per a l'ús de doble factor d'autenticació en la plataforma d'accés remot, que es troba en fase de proves en el moment de la revisió.	**No aplicada**	Es manté la redacció

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'informe
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 en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN. Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, per mitjà de procediment manual o a través d'eines automatitzades de monitoratge de la configuració.	L'Ajuntament ha realitzat millores en l'arquitectura de la xarxa de dades, implementant canvis en la seua configuració que proporcionen millores significatives tant en el rendiment i com en la seguretat en les comunicacions. S'han desenvolupat noves guies d'instal·lació d'equips d'usuari que inclouen l'aplicació de determinades configuracions de seguretat. L'Ajuntament ha iniciat un projecte per a la licitació d'un sistema EDR per a protecció de dispositius *endpoint,* però aquest projecte es troba temporalment suspés. S'ha adquirit una eina per a supervisar i garantir de manera permanent la conformitat de les configuracions d'elements crítics de l'electrònica de xarxa.	**Aplicada parcialment**	Es manté la redacció
9	Aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat d'usuari que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.	L'Ajuntament ha iniciat un projecte, que es troba en fase de prova, per a la implantació d'un SIEM i un centre d'operacions de seguretat.	**No aplicada**	Es manté la redacció
10	Millorar el sistema d'auditoria dels *logs* del programari de comptabilitat.	El sistema comptable s'ha substituït l'any 2022 pel nou sistema SEDA, de manera que la recomanació de l'informe anterior no és aplicable en aquest informe. La Sindicatura està realitzant una auditoria de seguretat específica del nou sistema.	Sense validesa en el marc actual	S'elimina la recomanació

	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
11	Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, proves de restauració i els requisits de protecció de les còpies.	L'Ajuntament ha implementat millores respecte a la gestió i control de les còpies realitzades per mitjà de l'elaboració d'una matriu d'assignació de responsabilitats, i la incorporació a l'eina corporativa per a la gestió de fluxos de treball dels diferents subprocessos i tasques del control que componen el procés de còpia. S'han automatitzat, per mitjà de l'eina per a la gestió de fluxos de treball, les tasques de revisió i proves de recuperació de còpies, tasques que són assignades automàticament als membres de l'equip i realitzades sobre tots els tipus de còpia existents.	**Aplicada parcialment**	S'actualitza la redacció anterior
12	Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de: - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.	Es va publicar en la seu electrònica, l'any 2019, la certificació de conformitat amb l'ENS per al "Sistema d'informació que suporta la seu electrònica de l'Ajuntament de València i els serveis i tràmits vinculats a aquesta". No obstant això, l'auditoria de seguretat i la certificació va caducar abans del 31 de desembre del 2021, per la qual cosa no és considerada com a vàlida per a la valoració de control.	**Aplicada parcialment**	S'actualitza la redacció anterior
13	En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular ha de: - Finalitzar l'aplicació de les mesures organitzatives i tècniques necessàries apropiades per a garantir un nivell de seguretat adequat al risc. - Planificar i executar auditories en matèria de protecció de dades.	S'ha millorat de manera general la maduresa dels processos gestionats per l'Oficina de la Delegació de Protecció de Dades Personals.	**Totalment o substancialment aplicada**	S'elimina la recomanació

Actuacions en curs

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

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

- L'Ajuntament es troba en tràmits per a la creació d'una secció específica per a la gestió de la seguretat integrada en el Servei TIC. La proposta de canvi es troba pendent d'aprovació per la Junta de Govern Local i, una vegada aprovada, disposarà de dotació pressupostària pròpia per al personal i projectes específics.

- L'Ajuntament disposa d'un Pla Director de Seguretat dels Sistemes d'Informació com a instrument per a planificar les actuacions en matèria de seguretat TIC i conté una relació de 26 projectes, que s'han dissenyat i prioritzat adequadament. Alguns dels projectes ja s'han executat i la resta es troben pendents de finalització o en planificació. L'execució de la totalitat de projectes, que ha sigut acordada per la Junta de Govern Local, millorarà substancialment el nivell de seguretat de l'Ajuntament.

- L'Ajuntament està tramitant la licitació per a contractar els serveis d'una oficina de ciberseguretat. Les funcions de l'oficina inclouen la coordinació de la implantació de les mesures previstes en el Pla Director, el desenvolupament i compliment normatiu, la formació i conscienciació en ciberseguretat, la constitució d'un centre d'operacions de seguretat i el monitoratge de sistemes, entre altres.

- L'Ajuntament ha sol·licitat l'adhesió a la Xarxa Nacional de Centres d'Operacions de Ciberseguretat, iniciativa impulsada pel Centre Criptològic Nacional per a integrar i coordinar els centres d'operacions de ciberseguretat del sector públic i articular la col·laboració i l'intercanvi d'informació àgil i efectiu entre les diferents administracions públiques.

- L'Ajuntament ha adquirit, i es troben en fase de desplegament, dos mòduls addicionals per al sistema que proporciona el servei de directori que realitzen les funcions següents:

    - Gestió d'inventari de programari i maquinari, solució integrada d'inventari que permet relacionar els dos inventaris i facilita l'aplicació de controls de seguretat posteriors.

    - Gestió de pedaços i actualitzacions del programari instal·lat, incloent-hi sistemes operatius i aplicacions.

- L'Ajuntament ha adquirit dues eines per a limitar la connexió de dispositius no autoritzats, una per a la gestió de dispositius per mitjà de connexions sense fil, que es troba en fase de desplegament, i una altra a través de connexions cablejades, que es troba en una fase inicial de projecte.

- L'Ajuntament ha iniciat un projecte, que es troba en fase de proves, per a la implantació d'un sistema de gestió d'informació i esdeveniments de seguretat (SIEM). S'han definit els processos interns per a la gestió d'incidències detectades i estan sent avaluats per a la implementació definitiva.

- L'Ajuntament ha iniciat un projecte per a la licitació d'un sistema EDR per a protecció de dispositius *endpoint*, però aquest projecte es troba temporalment suspés per retards en la tramitació administrativa. Considerem que és convenient que es reactive tan prompte com siga possible.

El conjunt d'actuacions en marxa en matèria de seguretat dels sistemes d'informació en el moment de finalitzar el treball de camp de l'auditoria permetrà que, una vegada implantades i degudament gestionades, millore substancialment el nivell de ciberseguretat de l'Ajuntament de València.

APÈNDIX 1
Metodologia aplicada

Introducció

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

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

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

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

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

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

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

Objectiu de l'auditoria

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

També formulem recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control, tenint en consideració les millores introduïdes des de la nostra auditoria anterior.

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

Abast

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

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

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

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

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

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

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

Àmbit temporal

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

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

Metodologia

Hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura i recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica, 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 més detall sobre la metodologia utilitzada ens remetem a aquesta guia.

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

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

[7] Center for Internet Security, <https://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

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

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

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

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

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

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

Quadre 4. Punts d'acció d'ENISA

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

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

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

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

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

Quadre 5. Els CBCS i els seus subcontrols

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

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

Avaluació dels resultats del treball

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

Subcontrols

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

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

Quadre 6. Avaluació dels subcontrols

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

Controls

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

OCEX 5313, que al seu torn està basada en la *Guía de seguridad CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 7. Nivells de maduresa

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

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

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

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indicadors globals

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

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

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

Governança de ciberseguretat

A l'efecte d'aquest treball, s'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'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una manera responsable.[12]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Seguiment de les recomanacions

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

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

Quadre 8. Situació de les recomanacions

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

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

Comunicació i confidencialitat

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

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

APÈNDIX 2

Situació dels controls bàsics de ciberseguretat

CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

L'Ajuntament realitza activitats de control com a part d'un procés que està implantat de manera general per a tots els sistemes de l'entitat, encara que aquest procés no es troba establit en un procediment formalment aprovat.

Hem verificat que s'han realitzat determinats canvis respecte a la situació de l'inventari i control de dispositius físics que vam observar en l'auditoria anterior, però part d'aquests canvis estaven en implantació i no poden considerar-se totalment efectius per a la valoració del control.

S'ha adquirit, per al sistema que proporciona el servei de directori, un mòdul addicional que realitza l'inventariat automàtic de tots els elements que disposen d'agent. Aquesta solució integrada d'inventari permet relacionar els inventaris de programari i maquinari de l'entitat i facilita l'aplicació de controls de seguretat posteriors, millorant les capacitats de l'eina d'inventari actualment en ús. La instal·lació de l'agent i l'inventari de nous elements es troben recollits adequadament en les guies d'instal·lació de nou equipament.

No obstant això, ens han indicat que la nova eina d'inventari, que es troba operativa i en producció des de l'any 2021, no s'ha desplegat completament i en el moment de la revisió únicament realitza la gestió d'una part dels equips de l'entitat.

A més, s'ha adquirit i desplegat una eina per al *ticketing* i la gestió de fluxos de treball, incloent-hi la gestió de dispositius de l'entitat, i en el moment de la revisió s'estava realitzant la migració de tasques des de l'eina anterior.

Quant al control de dispositius no autoritzats, l'Ajuntament disposa d'una eina que permet l'autenticació d'usuaris que es connecten a la xarxa corporativa amb mode sense fil.

Sobre el control de dispositius que es connecten a la xarxa corporativa per mitjà de connexions cablejades, s'ha adquirit recentment una eina que permetrà restringir l'accés únicament als dispositius que es troben registrats en aquesta. Hem verificat que el projecte per a implantar-la es trobava en la fase inicial d'execució.

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 52,5%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 1 del 65,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 36,6%. Per tant, s'ha produït una millora de 15,9 punts en l'índex de maduresa del control.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

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

Situació del control

L'Ajuntament ha realitzat determinats canvis en aquest control des de la revisió anterior, però les accions efectuades com a part del procés de gestió del programari no s'han establit en un procediment aprovat.

El mòdul adquirit per a l'inventari automàtic de tots els elements gestionats pel servei de directori fa l'inventariat de programari de tots els dispositius amb agent, tal com s'ha indicat en el control anterior. Aquesta eina permet, addicionalment la gestió de llicències, actualitzacions i pedaços, i la realització de revisions periòdiques de programari per a identificar la instal·lació de programari no autoritzat. No obstant això, la nova eina d'inventariat no s'ha desplegat completament.

Hem verificat que s'han actualitzat dues terceres parts dels equips que en l'auditoria anterior estaven fora del període de suport, i ha quedat pendent la resta.

A més s'ha planificat, com a part de les actuacions incloses en el Pla Director de Seguretat, la contractació del subministrament d'un sistema EDR per a protecció de dispositius *endpoint* que limita l'execució de programari no autoritzat. No obstant això, aquesta iniciativa no s'ha considerat per a la valoració del control, per les raons assenyalades en el CBCS 5.

Hi ha un cert nivell de control sobre l'inventari i control de programari autoritzat, que aconsegueix un **índex de maduresa del 62,5%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 2 del 78,1%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 56,5%. Per tant, s'ha produït una lleu millora de 6 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 seua identificació i resolució, però no s'ha desenvolupat, i formalment aprovat, un procediment a aquest efecte.

L'Ajuntament ha realitzat el desplegament de l'eina microCLAUDIA del CCN en els sistemes i equips d'usuari de l'entitat, la qual cosa proporciona protecció contra codi nociu de tipus *ransomware*. Hem verificat que la instal·lació s'ha realitzat de manera massiva i es troba desplegada en tots els dispositius d'usuari.

També ha desplegat les solucions CARMEN i SAT-INET, proporcionadas pel CCN-CERT i gestionadas pel CSIRT-CV, que permeten identificar l'existència d'usos indeguts o intents d'intrusió i realitzen la detecció en temps real d'amenaces i incidents existents en el trànsit que flueix entre la xarxa interna. Aquestes eines es troben plenament operatives i es realitza la gestió d'alertes subministrades per les dues sondes.

L'Ajuntament ha adquirit, per al sistema que proporciona el servei de directori, un mòdul addicional que realitza la gestió centralitzada de pedaços i actualitzacions de tot el programari instal·lat en els equips gestionats, incloent-hi sistemes operatius i totes les aplicacions instal·lades. No obstant això, l'eina no s'ha desplegat completament i únicament fa la gestió d'una part dels equips de l'entitat.

Addicionalment, l'Ajuntament ha realitzat diversos exercicis de *hacking* ètic a fi d'avaluar l'estat de seguretat dels sistemes d'informació. A més, s'ha contractat i planificat la realització de diversos exercicis de caixa negra per a executar-los al llarg de 2022.

La valoració global del control dona un **índex de maduresa del 67,5%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 3 del 84,4%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 55,5%. 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

L'Ajuntament no ha fet canvis significatius en l'ús controlat de privilegis administratius respecte de la situació observada en la revisió anterior. S'efectuen accions per al control dels comptes d'administració, i si bé hi ha determinades mesures adequades per al control de comptes, aquestes no es troben implantades de manera homogènia en tots els sistemes i no han sigut formalment establides en un procediment aprovat.

Únicament s'han realitzat millores relatives a la utilització de doble factor d'autenticació en determinats sistemes crítics de l'entitat. A més, hi ha un projecte per a l'ús de doble factor d'autenticació en altres sistemes, que es troba en fase de proves i no està operatiu en el moment de la revisió.

Hem verificat que l'Ajuntament no ha creat, per als usuaris administradors dels sistemes crítics de l'entitat, comptes sense privilegis d'administració destinats al seu ús en l'operativa ordinària, de manera que es limite l'ús dels comptes amb privilegis d'administració únicament a les tasques que ho requerisquen. Aquesta mancança suposa un risc per a l'entitat i incompleix el principi de mínim privilegi.

Hi ha un insuficient nivell de control sobre els comptes amb privilegis administratius i la valoració global del control suposa un **índex de maduresa del 47,0%**, que es correspon amb un **nivell de maduresa N1, inicial/ad hoc**; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment d'aquest CBCS 4 del 58,7%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 44,6%. Per tant, s'ha produït una lleu millora de 2,4 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 realitzat diverses millores respecte a les configuracions segures de programari i maquinari que vam observar en l'auditoria anterior, però aquests canvis no s'han aplicat a tots els sistemes com a part d'un procés definit i no s'ha aprovat un procediment que detalle el control aplicat.

Hem verificat que s'han realitzat millores significatives en l'arquitectura de la xarxa de dades de l'entitat, mantenint l'equipament físic disponible, però implementant canvis en la configuració de la xarxa que proporcionen millores de rendiment, de seguretat en les comunicacions i possibiliten l'aplicació de futurs controls addicionals.

S'han desenvolupat noves guies d'instal·lació d'equips d'usuari que es troben adequadament detallades i preveuen l'aplicació de determinades configuracions de seguretat, incloent-hi la gestió d'actualitzacions, pedaços i vulnerabilitats.

Hem verificat que l'Ajuntament ha iniciat un projecte per a la licitació d'un sistema EDR per a protecció de dispositius *endpoint*. No obstant això, a causa de retards en la gestió administrativa, aquest projecte es troba temporalment suspés, en espera de la renovació de l'Acord Marc del Sistema Estatal de Contractació Centralitzada del Ministeri d'Hisenda i Funció Pública per a formalitzar l'adquisició.

No s'han aplicat millores en la configuració de la resta de sistemes de l'entitat, com ara servidors i altres sistemes crítics, que hauria de formar part d'un procés sistemàtic formalment aprovat.

L'Ajuntament ha adquirit, com a part d'un projecte de renovació d'elements crítics de l'electrònica de xarxa, una eina que disposa, entre altres funcions, de la capacitat per a supervisar i garantir la conformitat de manera permanent d'acord amb les polítiques corporatives o la normativa dels equips de xarxa, però no hem verificat que l'Ajuntament explote adequadament aquesta funcionalitat.

Per a la resta dels actius, l'Ajuntament no ha implantat un procés de gestió contínua de la configuració dels sistemes, no realitza la gestió de manera manual ni disposa de les eines necessàries per a la gestió automàtica de configuracions.

La valoració global del control aconsegueix un **índex de maduresa del 31,4%**, que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, hi ha un nivell insuficient de control en l'aplicació de configuracions segures en dispositius i programari, i per tant s'han de dedicar esforços i recursos per a millorar-la. Això representa un **índex de compliment del CBCS 5 del 39,2%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 12,4%. Per tant, s'ha produït una millora de 19 punts en l'índex de maduresa del control.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

L'Ajuntament ha realitzat determinades millores respecte a la situació observada en l'auditoria anterior, però els canvis no es troben completament operatius en el moment de la revisió i no s'ha aprovat un procediment que detalle les accions aplicades en el control.

L'Ajuntament ha habilitat la recol·lecció de *logs* en tots els sistemes crítics de l'entitat i disposa de diverses eines, específiques per a cada sistema o grups de dispositius, per a la centralització i tractament d'aquests. Aquestes eines són adequadament gestionades i explotades pels administradors i operadors dels sistemes.

A més, des de l'auditoria anterior, l'Ajuntament ha iniciat un projecte per a la implantació d'un SIEM i un centre d'operacions de seguretat. El projecte es trobava en fase de proves en el moment de realitzar l'auditoria i hem verificat que el sistema SIEM recol·lecta registres de 4 dels sistemes crítics de l'entitat. S'han definit els processos interns de gestió d'incidències i esdeveniments detectats pel sistema, que estan sent avaluats per a la implementació definitiva.

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

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 56,5%. Per tant, s'ha produït una lleu millora de 3,5 punts en l'índex de maduresa del control.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

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

Situació del control

L'Ajuntament ha implementat millores respecte a la situació observada en l'auditoria anterior sobre la gestió i control dels processos de còpia.

L'Ajuntament disposa de dos sistemes diferents per a la realització i gestió de còpies de seguretat i utilitza cada un segons el sistema i tipus de còpia que cal implementar. Les polítiques de còpia es troben definides pel departament TIC o pels responsables dels serveis, depenent del sistema a salvaguardar.

Les còpies es troben emmagatzemades en ubicacions redundants i addicionalment es disposa de còpies en cinta per a determinats sistemes, de manera que es proporcionen diferents nivells de protecció depenent del tipus de còpia.

Hem verificat que des de la nostra auditoria anterior s'han implementat millores respecte a la gestió i control de les còpies realitzades. S'ha definit una matriu d'assignació de responsabilitats, que defineix els responsables per a la realització i la revisió de còpies i independitza el procés de còpia de perfils concrets.

A més, hem verificat que els diferents subprocessos i tasques del control s'han inclòs en l'eina corporativa per a la gestió de fluxos de treball, la qual cosa proporciona un nivell de maduresa addicional al control i permet una gestió més eficaç per part dels responsables de les còpies.

S'han automatitzat diferents tasques de revisió, incloent-hi recuperacions i comprovacions d'integritat, que són assignades automàticament als membres de l'equip de treball i realitzades sobre tots els tipus de còpia existents, màquines virtuals, bases de dades i emmagatzematge de fitxers.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 75,0%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 93,8%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 63,3%. Per tant, s'ha produït una millora d'11,7 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 2019, l'Ajuntament ha efectuat les accions següents relatives al compliment exigit pel Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica:

- S'ha actualitzat la categorització del sistema segons les últimes directrius de les guies del CCN.

- L'Ajuntament va realitzar en 2019, després de la publicació del nostre informe, l'auditoria de seguretat prevista en l'article 34 del Reial Decret 3/2010. No obstant això, han transcorregut més de dos anys des de la seua realització, per la qual cosa ha de realitzar-se novament per a verificar el compliment dels requeriments dl'ENS.

- Es va publicar en la seu electrònica, l'any 2019, la certificació de conformitat i els distintius corresponents previstos en l'ENS per al "Sistema d'informació que suporta la seu electrònica de l'Ajuntament de València i els serveis i tràmits vinculats a aquesta". No obstant això, aquesta certificació va caducar abans del 31 de desembre del 2021, per la qual cosa no és considerada per a la valoració de control.

D'altra banda, la política de seguretat de la informació i la normativa relacionada es troben desactualitzades. L'Ajuntament està treballant en la licitació d'un servei d'oficina de ciberseguretat, un servei del qual hem verificat que inclou, entre altres funcions, el desenvolupament normatiu requerit per a aconseguir el compliment de la legislació vigent.

A més, no s'ha constituït formalment el comité de seguretat de la informació, no han sigut nomenats els responsables de la informació i del servei i hi ha una incompatibilitat en el nomenament del responsable de seguretat, rol que és actualment exercit pel cap del Servei TIC.

Compliment de l'RGPD

Quant al compliment en matèria de protecció de dades personals, des de la revisió realitzada l'any 2019 l'Ajuntament ha efectuat accions que han millorat el nivell de compliment.

Les millores identificades es basen en l'aplicació de mesures organitzatives i tècniques per part de l'Oficina de la Delegació de Protecció de Dades Personals. Algunes de les mesures aplicades són:

- Realització de cursos de formació obligatoris per al personal de l'Ajuntament.

- L'assessorament als serveis municipals i elaboració d'informes s'ha incrementat de manera important en els últims 3 anys.

- Col·laboració amb el servei municipal de contractació per mitjà de l'elaboració d'informes quan pot haver-hi tractament de dades per tercers i establiment, en cas necessari, dels detalls de l'encàrrec del tractament.

- S'ha establit un procés per a mantindre degudament actualitzat l'inventari d'activitats de tractament de dades personals, per mitjà de l'encreuament d'informació municipal de manera continuada.

- S'ha realitzat una auditoria interna per part de la mateixa Oficina de la Delegació de Protecció de Dades Personals.

L'Oficina de la Delegació de Protecció de Dades Personals de l'Ajuntament ha organitzat els anys 2019 i 2022 una trobada nacional de DPD de l'Administració local, amb la finalitat de compartir coneixement i difondre la cultura de la protecció de dades personals. A més, ha col·laborat amb el Comité Tècnic de la Societat de la Informació, Innovació Tecnològica i Agenda Digital de la Federació Espanyola de Municipis i Províncies a fi de fomentar un model d'autoavaluació del compliment normatiu.

En conseqüència, atés el grau de maduresa dels processos gestionats per l'Oficina de la Delegació de Protecció de Dades Personals, es donen per complides les recomanacions efectuades en l'informe anterior.

Compliment de legalitat del registre de factures

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

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió ha millorat respecte a l'informe emés l'any 2019, i l'Ajuntament aconsegueix un **índex de maduresa del 70,0%**, que es correspon amb un **nivell de maduresa N2**, que indica que hi ha un nivell raonable d'adequació a la normativa, però hi ha aspectes pendents de millora sobre els quals s'ha d'actuar per a esmenar-los.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 54,8%. Per tant, s'ha produït una millora de 15,2 punts en l'índex de maduresa del control.

Governança de ciberseguretat

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 processos de gestió adequats, ens permet concloure que la governança de ciberseguretat aconsegueix un nivell acceptable. Els aspectes fonamentals que sustenten aquesta afirmació són:

- 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. No obstant això, com hem indicat abans, s'ha d'actualitzar.

- L'existència d'un Pla Director de Ciberseguretat, que estableix el conjunt d'actuacions a mitjà termini, considerant prioritats en la implantació, el cost de les mesures i els indicadors per al mesurament de l'avanç en la implementació. El Pla ha sigut aprovat per la Junta de Govern Local l'any 2021.

- L'existència d'una iniciativa, encara pendent d'aprovació per la Junta de Govern Local, per a la creació d'una secció específica en el Servei TIC per a la gestió de la seguretat, dotant-la dels recursos necessaris.

- La participació activa de l'alta direcció, particularment el regidor delegat, en la gestió de la seguretat de la informació i en l'elaboració i aprovació del Pla Director de Ciberseguretat.

- L'existència de rols clau, particularment el responsable de seguretat i el DPD. Hem verificat que existeixen i exerceixen de manera efectiva i continuada les funcions establides.

- L'existència d'una oficina de la Delegació de Protecció de Dades Personals que, addicionalment a les seues atribucions ordinàries, realitza accions per a la difusió i conscienciació de la protecció de dades personals en l'àmbit de l'Administració local.

- 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 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.

No obstant això, s'han identificat mancances significatives que minven o limiten la capacitat de l'organització per a gestionar la seguretat, que han d'esmenar-se:

- La inexistència de determinats rols clau en l'organització per a la gestió de la seguretat, com els responsables de la informació i del servei, i **particularment la inexistència d'un comité de seguretat**. Hem verificat l'existència de grups de treball per a la gestió de la seguretat, però aquests no estaven formalment constituïts com a comité de seguretat i a més no han tingut activitat efectiva des de la nostra auditoria anterior.

- Hem identificat una falta d'agilitat administrativa en la gestió de les contractacions que minva la capacitat de reacció i limita les oportunitats de millora.

- Existeix una incompatibilitat en el nomenament del responsable de seguretat, atés que la seua figura recau sobre el cap del Servei TIC. El responsable de seguretat ha de determinar les mesures que cal aplicar i el cap del Servei TIC ha d'implementar-les.

APÈNDIX 3
Bones pràctiques destacables

Introducció

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

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

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

Planificació estratègica de la seguretat

L'Ajuntament ha elaborat un Pla Director de Seguretat dels Sistemes d'Informació com a instrument de planificació de les actuacions horitzontals en matèria de seguretat TIC.

Aquest pla disposa del contingut necessari, materialitzat en una relació de 26 projectes. Així mateix, per a cada un dels projectes detalla una estimació de la prioritat en la

implementació, l'esforç humà requerit, els costos econòmics, l'impacte del projecte en nivell de seguretat i la seua duració.

El Pla ha sigut desenvolupat per especialistes independents després de la realització d'una anàlisi diferencial, per a conéixer les diferències entre el model de seguretat actual de l'organització i el proposat per l'ENS, i una anàlisi de riscos, per a identificar les amenaces que poden afectar els actius de l'entitat i la freqüència d'ocurrència d'aquestes amenaces.

A més, el Pla s'ha articulat de manera adequada, elaborat pel Servei TIC i aprovat per la Junta de Govern Local. Aquesta aprovació implica el compromís per part dels òrgans de govern en la dotació de crèdit adequat i suficient en les aplicacions pressupostàries del Servei de Tecnologies de la Informació i Comunicació, així com l'ampliació de la seua plantilla, per a fer possible l'execució de totes les mesures previstes.

Aquesta planificació estratègica de les actuacions proporciona un marc d'actuació a mitjà termini que assegura l'atenció a les necessitats prioritàries respecte a la seguretat i evita una gestió basada principalment en la consideració de necessitats sobrevingudes.

Creació d'una oficina de seguretat

L'Ajuntament ha disposat la creació d'una oficina de seguretat, per mitjà de la contractació d'un servei que assumirà responsabilitats de supervisió i oferirà orientació al Servei TIC i a la resta de serveis i unitats de l'Ajuntament, a més de garantir que els processos de ciberseguretat estiguen implementats i siguen operatius.

Aquest servei es troba organitzat en tres àmbits: govern, centre d'operacions de seguretat i resposta a incidents.

Sobre el govern, es faran tasques relatives al compliment normatiu, gestió de riscos, desenvolupament normatiu i formació en ciberseguretat.

Quant al centre d'operacions de seguretat, s'assumirà el monitoratge de sistemes i xarxes, l'escaneig de vulnerabilitats, la gestió de pedaços i la realització d'auditories tècniques.

Sobre la resposta a incidents de ciberseguretat, l'oficina identificarà i informarà sobre amenaces, proporcionarà eines d'anàlisi forense i realitzarà la gestió de ciberintrusions.

En relació amb el Pla Director de Seguretat dels Sistemes d'Informació, l'oficina de seguretat coordinarà la implantació de les mesures previstes i realitzarà el mesurament del grau d'avanç en la implantació del Pla, del qual es donarà compte semestralment a la Junta de Govern Local.

Automatització dels processos de gestió de còpies de seguretat

L'Ajuntament ha establit un procés de gestió de còpies de seguretat que inclou l'automatització de determinades mesures de control, que són periòdicament assignades de manera aleatòria als membres de l'equip.

La creació de les tasques es fa per mitjà d'un *script* de l'eina de gestió de fluxos de treball, que realitza consultes als sistemes de l'entitat per a identificar les còpies existents i genera tasques per a la realització de diferents tasques de revisió sobre còpies seleccionades de manera aleatòria.

Les tasques de revisió inclouen diferents tipus de comprovacions, incloent-hi recuperacions i comprovacions d'integritat, i són realitzades sobre tots els tipus de còpia existents, màquines virtuals, bases de dades i emmagatzematge de fitxers.

Aquesta gestió, controlada a través de l'eina de gestió de fluxos de treball i automatitzada per mitjà de *scripts*, proporciona un nivell de maduresa addicional, independitza les tasques de membres concrets de l'equip, estandarditza els treballs que cal realitzar i estableix indicadors que permeten el mesurament de l'acompliment del control.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

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

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

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

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

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

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

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

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

EDR:[17] Un sistema EDR, sigla en anglés d'*endpoint detection and response*, és un sistema de protecció dels equips i infraestructures de l'empresa. Combina l'antivirus tradicional juntament amb eines de monitoratge i intel·ligència artificial per a oferir una resposta ràpida i eficient davant els riscos i les amenaces més complexes.

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

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

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

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

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

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

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

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir amb el regidor delegat d'Agenda Digital i Administració Electrònica, el secretari municipal de l'Àrea II i el cap del Servei de Tecnologies de la Informació i Comunicacions, perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

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

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

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

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

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

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*h* del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 15 de desembre de 2022, va aprovar aquest informe d'auditoria.

ANNEX I

Al·legacions presentades

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

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

JUSTIFICANTE DE PRESENTACIÓN EN REGISTRO ELECTRÓNICO

NÚMERO DE REGISTRO 202205371	FECHA DE ENTRADA 07/12/2022 9:12
ÁREA Fiscalización - Alegaciones	PROCEDIMIENTO PAA2020/35 Seguimiento de las 11 auditorías de los controles básicos de ciberseguridad cuyo trabajo de campo se ha realizado en 2019 (una vez transcurrido un año desde su finalización)
DATOS DEL PRESENTADOR Nombre: VICENTE RODRIGO INGRESA NIF / CIF: E-mail: Entidad: VALÈNCIA	
FIRMA DIGITAL 61DEA66A52010738C81DE44998E05480BF04525B	
DOCUMENTOS ENVIADOS Fichero1: 79140179P_2022127_20221207 Informe alegaciones.pdf	

SINDICATURA DE COMPTES

Al·legacions que es formulen a l'esborrany de l'Informe de seguiment de les recomanacions realitzades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019. Situació a 31 de desembre de 2021.

Primera al·legació.

Apartat "CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS" de l'esborrany de l'Informe, pàgina 37.

Contingut de l'al·legació:

De la lectura de este apartado se puede dar a entender que el ayuntamiento no dispone de una herramienta de control de inventario de equipos cuando esto no es realmente cierto. El ayuntamiento dispone de una herramienta de control de inventario de equipos que lleva varios años en producción y que llamamos SGI, y es la misma herramienta con la que gestionamos el *ticketing*. Recientemente, se ha adquirido un nuevo software, que debe sustituir al anterior y que tiene mejores prestaciones, pero este nuevo software todavía no se ha terminado de implantar.

Documentació justificativa de l'al·legació:

Se adjuntan algunas capturas de pantalla de la herramienta actual en la que se puede ver el resultado de la búsqueda y consulta de los datos inventariados de un PC:

Les imatges s'han eliminat per raons de seguretat

[redacted]

[redacted]

Segona al·legació.

Apartat "CBCS 1. INVENTARIO Y CONTROL DE DISPOSITIVOS FÍSICOS" de l'esborrany de l'Informe, pàgina 37, paràgraf penúltim.

Contingut de l'al·legació:

El párrafo siguiente: "*En cuanto al control de dispositivos no autorizados, el Ayuntamiento dispone de una herramienta que permite la autenticación de usuarios que se conectan a la red corporativa de manera inalámbrica, pero no ha sido desplegada completamente y no se encontraba en operación en el momento de la revisión.*" alegar que sí que está desplegada completamente, de forma que todos los usuarios que se conectan a la wifi corporativa lo hacen con usuario y contraseña. Es decir, no es posible que un usuario se conecte a la wifi corporativa sin introducir ni usuario ni contraseña.

Documentació justificativa de l'al·legació:

Se adjuntan capturas de pantalla con el procedimiento de registro que cada usuario debe hacer, en la intranet municipal, antes de que pueda conectarse a la wifi corporativa:

[redacted]

[redacted]

Tercera al·legació

Apartat "Sobre el inventario y control de software autorizado (CBCS 2)" de l'esborrany de l'Informe, pàgina 9

Contingut de l'al·legació:

Los usuarios de los pc's del ayuntamiento no disponen de privilegios de administración, y por lo tanto, no pueden instalarse una aplicación sin intervención de un técnico del Servicio de Tecnologías de la Información y la Comunicación (SerTIC).

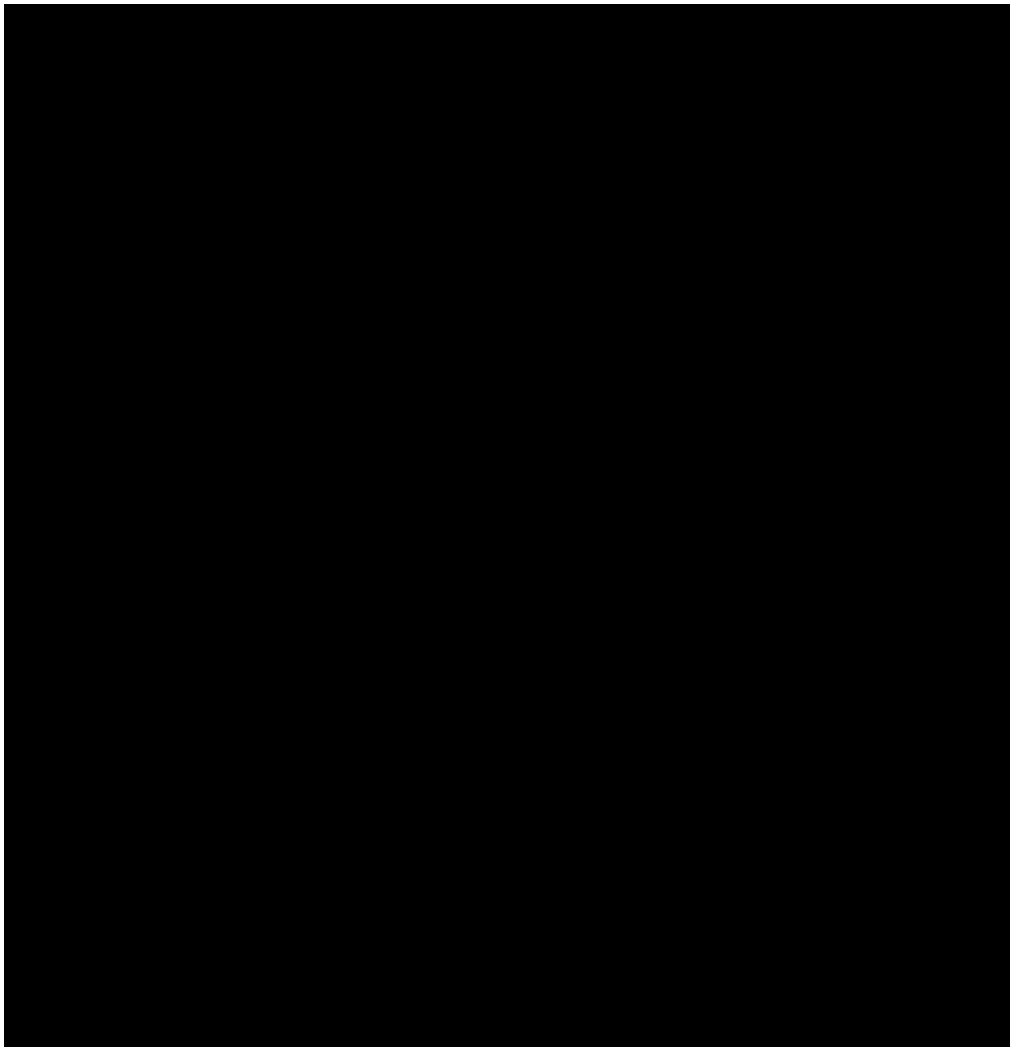
Además, existe un sistema automatizado para la distribución de aplicaciones (ZENworks) y también de actualizaciones y parches en los equipos de usuario.

Documentació justificativa de l'al·legació:

Se adjunta captura de pantalla de un ejemplo de usuario con la lista de aplicaciones autorizadas y que se distribuyen automáticamente en el primer inicio:

Aquí se distinguen entre las aplicaciones que se distribuyen para todos los usuarios del ayuntamiento (“Aplic. Ayuntamiento”), las que solo se distribuyen a usuarios concretos (“Aplic. Específicas”) o las que se distribuyen a los usuarios de un servicio del ayuntamiento (“Aplic. Servicio”). El grupo de aplicaciones “Soporte” está restringido a usuarios del SerTIC.

Se adjunta también captura de pantalla de la herramienta donde se configuran los parches y actualizaciones que deben distribuirse:



Cuarta al·legació

Apartat "Sobre el uso controlado de privilegios administrativos (CBCS 4)" de l'esborrany de l'Informe, pàgina 10

Contingut de l'al·legació:

Los usuarios de los pc's del ayuntamiento no disponen de privilegios de administración, y por lo tanto, no pueden instalarse una aplicación sin intervención de un técnico del SerTIC. Esto se configura de manera centralizada mediante ZENworks y las políticas de Windows.

Documentació justificativa de l'al·legació:

Se adjunta captura de pantalla de las políticas de Windows de un usuario ejemplo gestionadas desde ZENworks:

Quinta al·legació

Apartat "Actuaciones en curso" de l'esborrany de l'Informe, pàgina 17

Contingut de l'al·legació:

Dado que el informe se ha elaborado con datos a 31 de diciembre de 2021, destacar que la Junta de Gobierno Local aprobó el 23/12/2021 el Plan Director de Ciberseguridad.

Aunque las medidas de dicho plan han comenzado a aplicarse durante el 2022, sí que nos gustaría que figurase de manera más destacada en el apartado "4. CONCLUSIONES", que el ayuntamiento aprobó el 23/12/2021 dicho plan.

Documentació justificativa de l'al·legació:

Ya se aportó acta de la Junta de Gobierno Local de 23/12/2021, pero puede localizarse la misma en la web municipal https://www.valencia.es en la siguiente ruta:

"*Ayuntamiento*", "*Actividad Órganos de Gobierno*", "*Junta de Gobierno Local*", "*2021*", "*23 de Diciembre de 2021 (Ordinaria)*"

(no se puede adjuntar enlace directo porque es dinámico)

ANNEX II

Informe sobre les al·legacions presentades

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

Per mitjà de l'escrit d'aquesta Sindicatura de 25 de novembre de 2022 es va remetre a l'Ajuntament de València l'esborrany de l'Informe d'auditoria, perquè efectuara les al·legacions que considerara oportunes. Amb data 7 de desembre de 2022 es van rebre pel registre electrònic les al·legacions formulades respecte de les quals s'assenyala el que segueix:

Primera al·legació

Apartat "CBCS 1. Inventari i control de dispositius físics" de l'esborrany de l'Informe, apèndix 2

Comentaris

L'al·legació indica que de la lectura de l'Informe es pot entendre que l'Ajuntament no disposa d'una eina de control d'inventari d'equips, però en realitat sí que existeix una eina que es troba en producció.

L'apartat detalla principalment les novetats identificades en els controls, per la qual cosa no s'ha inclòs referència expressa a l'eina existent, però sí a l'adquisició d'un nou programari que millora les prestacions de l'eina actual.

No obstant això, s'accepta l'al·legació i es matisa la redacció de l'apartat incloent-hi una referència a l'eina actualment en ús.

Conseqüències en l'Informe

Modificar el paràgraf 4 de l'apartat "CBCS 1. Inventari i control de dispositius físics" de l'apèndix 2 i redactar-lo com segueix:

> "S'ha adquirit, per al sistema que proporciona el servei de directori, un mòdul addicional que realitza l'inventariat automàtic de tots els elements que disposen d'agent. Aquesta solució integrada d'inventari permet relacionar els inventaris de programari i maquinari de l'entitat i facilita l'aplicació de controls de seguretat posteriors, millorant les capacitats de l'eina d'inventari actualment en ús. La instal·lació de l'agent i l'inventari de nous elements es troben recollits adequadament en les guies d'instal·lació de nou equipament."

Segona al·legació

Apartat "CBCS 1. Inventari i control de dispositius físics" de l'esborrany de l'Informe, apèndix 2

Comentaris

L'al·legació indica que l'eina per a autenticació d'usuaris que es connecten a la xarxa corporativa amb mode sense fil sí que està desplegada completament.

Durant la visita per a la revisió de controls, se'ns va indicar que la solució d'autenticació per a dispositius sense fils, basada en l'ús de protocol 802.1x, no es trobava operativa, encara que l'adquisició de les llicències necessàries s'havia produït dins del període de revisió. En l'al·legació no s'inclou el detall suficient per a confirmar que la solució es trobava plenament funcional en data de 31 de desembre de 2021.

Verificada la informació rebuda, s'accepta parcialment l'al·legació, es matisa la redacció de l'apartat, però es manté la valoració del control.

Conseqüències en l'Informe

Modificar el paràgraf 6 de l'apartat "CBCS 1. Inventari i control de dispositius físics" de l'apèndix 2 i redactar-lo com segueix:

> "Quant al control de dispositius no autoritzats, l'Ajuntament disposa d'una eina que permet l'autenticació d'usuaris que es connecten a la xarxa corporativa amb mode sense fil."

Modificar el quadre 2, "Seguiment de recomanacions", segona recomanació, "Situació a 31 de desembre de 2021 respecte a l'informe anterior", i redactar-lo com segueix:

> "S'han adquirit dues eines, una per a la gestió de dispositius per mitjà de connexions sense fils i una altra per mitjà de connexions cablejades. No obstant això, aquesta última es troba en una fase inicial de projecte."

Tercera al·legació

Apartat 5, "Recomanacions i mesures necessàries per al compliment de la legalitat", subapartat "Sobre l'inventari i control de programari autoritzat (CBCS 2)", de l'esborrany de l'Informe

Comentaris

L'al·legació indica que els usuaris de l'Ajuntament no poden instal·lar aplicacions sense intervenció d'un tècnic del SerTIC, atés que no disposen de privilegis d'administració.

Durant la realització del treball vam poder verificar l'existència de les mesures de control que es detallen en l'al·legació. No obstant això, la recomanació expressa la necessitat

d'elaborar i aprovar un procediment que detalle i formalitze, entre altres aspectes, l'explotació d'aquestes mesures que ja es troben implantades.

A més, l'al·legació indica que existeix un sistema automatitzat per a la distribució d'aplicacions i també d'actualitzacions i pedaços en els equips d'usuari.

L'existència d'aquestes eines es troba recollida en l'apartat corresponent de l'apèndix 2. No obstant això i com hem indicat, la recomanació expressa la necessitat que el procediment, que ha de ser elaborat i aprovat, detalle l'explotació d'aquestes mesures existents.

No afecta la nostra conclusió.

Conseqüències en l'Informe

Mantindre la redacció de l'Informe.

Quarta al·legació

Apartat 5, "Recomanacions i mesures necessàries per al compliment de la legalitat", subapartat "Sobre l'ús controlat de privilegis administratius (CBCS 4)", de l'esborrany de l'Informe

Comentaris

L'al·legació indica que els usuaris de l'Ajuntament no poden instal·lar aplicacions sense intervenció d'un tècnic del SerTIC, atés que no disposen de privilegis d'administració.

Tal com s'indica en el punt anterior, durant la realització del treball vam poder verificar l'existència de les mesures de control relatives a la gestió de privilegis. No obstant això, les recomanacions expressen la necessitat d'elaborar i aprovar procediments que detallen i formalitzen l'explotació de mesures que ja es troben implantades.

No afecta la nostra conclusió.

Conseqüències en l'Informe

Mantindre la redacció de l'Informe.

Cinquena al·legació

Apartat 5, "Recomanacions i mesures necessàries per al compliment de la legalitat", subapartat "Actuacions en curs", de l'esborrany de l'Informe

Comentaris

L'al·legació indica que el Pla Director de Ciberseguretat va ser aprovat per la Junta de Govern Local el 23 de desembre de 2021, dins del període de revisió de l'Informe. I se sol·licita que figure de manera més destacada en l'apartat 4, "Conclusions", la data d'aprovació d'aquest pla.

L'Informe detalla l'any d'aprovació del Pla Director de Ciberseguretat en el paràgraf 3 del subapartat "Governança de la ciberseguretat" de l'apèndix 2.

No obstant això, s'accepta l'al·legació i es modifica la redacció de les conclusions de l'Informe perquè reflectisca aquesta dada.

Conseqüències en l'Informe

Modificar la redacció del paràgraf cinqué de la conclusió sobre la governança de l'apartat 4, "Conclusions":

> "Hi ha projectes i iniciatives que es troben en fase d'execució o de planificació que, en cas de finalitzar-se i gestionar-se de manera efectiva, tindran un impacte positiu des del punt de vista operatiu i de la seguretat. A més, hi ha una planificació estratègica de la seguretat de la informació que s'ha materialitzat en el Pla Director de Seguretat dels Sistemes d'Informació, aprovat per la Junta de Govern el 23 de desembre de l'any 2021, que orienta de manera coherent les accions en aquesta matèria."

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe seguiment recomanacions CBCS Ajuntament València 2019_val - SEFYCU 3745172

Podeu accedir a aquest document en format PDF-PAdES i comprovar la seua autenticitat en la Seu Electrònica usant el codi CSV següent:

URL (adreça en Internet) de la Seu Electrònica: https://sindicom.sedipualba.es/

Codi Segur de Verificació (CSV): KUAA 3CV2 RWLD EFPJ 7NN9

En aquesta adreça podeu obtenir més informació tècnica sobre el procés de firma, així com descarregar les firmes i els segells en format XAdES corresponents.

Resum de firmes i/o segells electrònics d'aquest document

Empremta del document per a la persona firmant	Text de la firma	Dades addicionals de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrònica - ACCV - 29/12/22 08:08 VICENT CUCARELLA TORMO