SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME D'AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DE LA DIPUTACIÓ DE VALÈNCIA

Exercici 2021

RESUM

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

Atesa aquesta realitat, i en sintonia amb el seu actual pla estratègic, la Sindicatura de Comptes ha realitzat una auditoria dels controls bàsics de ciberseguretat (CBCS) de la Diputació de València.

Conclusions

L'índex de maduresa general dels CBCS mostra un valor del 51,0%, de manera que encara ha de millorar per a aconseguir l'objectiu del 80%. S'han identificat diverses deficiències significatives i en tots els controls analitzats s'han de fer esforços per a millorar-los, ja que cap aconsegueix el nivell de maduresa requerit. En particular, n'hi ha quatre que tenen un nivell de maduresa deficient, i sobre aquests s'ha de treballar amb major intensitat per a reforçar la protecció dels sistemes d'informació.

Hem pogut verificar que la Diputació no té establida una governança adequada de la ciberseguretat. Els òrgans superiors de la Diputació, com a responsables del sistema de control, han de reforçar l'actual nivell de compromís i suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

La revisió del compliment de legalitat en matèria relacionada amb la seguretat de la informació ha posat de manifest un baix nivell d'adequació a les normes legals. L'informe assenyala diversos aspectes pendents de millora sobre els quals s'ha d'actuar per a esmenar-los ràpidament.

Respecte de l'Esquema Nacional de Seguretat, la Diputació ha de realitzar els nomenaments necessaris, especialment el responsable de seguretat, i solucionar les no conformitats identificades en l'auditoria de compliment realitzada, de manera que puga obtindre la certificació de conformitat i el distintiu corresponent per a publicar-los en la seu electrònica.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i a millorar els procediments de gestió de la ciberseguretat de la Diputació. Entre aquestes aconsellem actualitzar i millorar la normativa de seguretat, implantar solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa (CBCS 1), identificar i actualitzar tots els sistemes que es troben fora del període de suport (CBCS 2) i resoldre les vulnerabilitats de nivell crític identificades (CBCS 3).

NOTA

Aquest resum pretén ajudar a la comprensió dels resultats del nostre informe i facilitar la labor als lectors i als mitjans de comunicació. Recomanem la seua lectura per a conéixer el vertader abast del treball realitzat.

Informe d'auditoria dels controls bàsics de ciberseguretat de la Diputació de València

Exercici 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. Introducció 3
2. Responsabilitats dels òrgans superiors de la Diputació en relació amb els controls de ciberseguretat 4
3. Responsabilitat de la Sindicatura de Comptes 5
4. Conclusions 5
5. Recomanacions i mesures per al compliment de la legalitat 8
Apèndix 1. Metodologia aplicada 15
Apèndix 2. Situació dels controls bàsics de ciberseguretat 32
Apèndix 3. Bones pràctiques destacables 44
Acrònims i glossari de termes 47
Tràmit d'al·legacions 50
Aprovació de l'Informe 51

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 la reunió de la Comissió de Coordinació en l'àmbit local entre el Tribunal de Comptes i els òrgans de control extern (OCEX) del 18 de novembre de 2019 es va plantejar la possibilitat de realitzar una fiscalització coordinada sobre la implantació de l'administració electrònica en les entitats locals, els resultats de la qual s'exposen en un altre informe de la Sindicatura. Atesa la importància dels controls de ciberseguretat en entorns digitalitzats, la Sindicatura va ampliar l'àmbit objectiu del treball esmentat i va incloure en els programes anuals d'actuació de 2020 i de 2021 la realització d'una auditoria dels controls bàsics de ciberseguretat de les tres diputacions provincials.

A més, la Sindicatura també està duent a terme una auditoria de l'entorn de control dels ajuntaments amb població superior a 50.000 habitants i les tres diputacions, un dels apartats de la qual es refereix als controls bàsics de ciberseguretat, en què s'integraran de manera sintètica els resultats reflectits en aquest informe.

La necessitat d'una adequada ciberhigiene

Els actuals sistemes d'informació que donen suport a tota la gestió pública, complexos i interconnectats, "estan exposats de forma cada vegada més intensa a la materialització d'amenaces del ciberespai, els ciberincidents, que segueixen una pauta de creixement en freqüència, sofisticació, abast i severitat de l'impacte".[1] Aquests ciberincidents tenen

[1] Projecte de Reial Decret pel qual es regula l'ENS, de 16 de juny de 2021.

conseqüències potencialment pertorbadores sobre els serveis que les diputacions presten als ciutadans i als ajuntaments del seu àmbit d'actuació.

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 adquireixen tot el seu 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[2] 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 LA DIPUTACIÓ EN RELACIÓ AMB ELS CONTROLS DE CIBERSEGURETAT

Els òrgans superiors de la Diputació (en particular el president o la presidenta 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.

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats, proporcionant una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control. Per a això, hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica, així com que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CBCS revisats.

L'auditoria s'ha centrat en l'anàlisi de la situació dels huit CBCS en relació amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptatòria i altres sistemes d'interés general.

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, conforme al 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 sempre detecte un incompliment significatiu quan existisca.

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

4. CONCLUSIONS

L'índex de maduresa general dels controls bàsics de ciberseguretat és insuficient i ha de millorar per a aconseguir els nivells exigits per l'ENS

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconsegueix un **índex de maduresa general del 51,0%**, 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 no formalitzats documentalment. Els resultats detallats obtinguts per a cada un dels CBCS es mostren en el quadre 1.

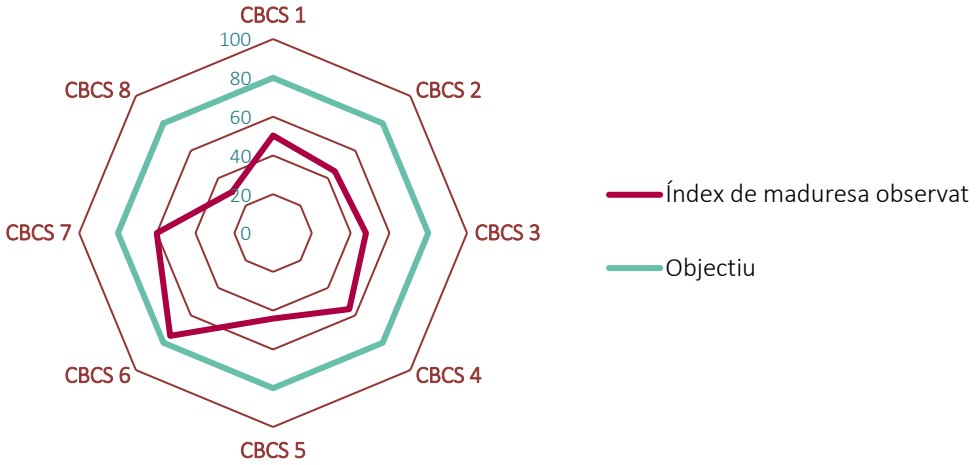
Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

Control		Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1	Inventari i control de dispositius físics	50,3%	N2	62,8%
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	45,0%	N1	56,3%
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	47,9%	N1	59,8%
CBCS 4	Ús controlat de privilegis administratius	55,5%	N2	69,3%
CBCS 5	Configuracions segures del programari i maquinari	44,1%	N1	55,1%
CBCS 6	Registre de l'activitat dels usuaris	75,0%	N2	93,8%
CBCS 7	Còpies de seguretat de dades i sistemes	60,0%	N2	75,0%
CBCS 8	Compliment normatiu i governança de ciberseguretat	30,0%	N1	37,5%
General		51,0%	N2	63,7%

L'índex de compliment dels CBCS és del 63,7%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*.

D'una forma més sintètica i gràfica, la situació observada dels controls queda reflectida en el gràfic 1.

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



A la vista dels resultats obtinguts en la revisió, es conclou que el nivell d'efectivitat en els controls analitzats és insuficient i hi ha possibilitats clares de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació, i particularment sobre aquells controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 2, CBCS 3, CBCS 5 i CBCS 8). En l'apartat 6 es realitzen les recomanacions pertinents amb aquesta finalitat.

La nostra auditoria i els indicadors reflecteixen la situació a 30 de setembre de 2021.

La Diputació de València no té establida una adequada governança de la ciberseguretat i ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació

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

A pesar de les mancances que assenyalem, hem pogut verificar l'existència d'un cert nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de la Diputació i els gestors i responsables de les àrees implicades.

Les mancances més rellevants identificades són les següents:

- La falta d'actualització del document de polítiques de seguretat de la informació.
- La falta d'activitat efectiva i continuada del comité de seguretat, que hem verificat que no s'ha reunit en els últims tres anys.
- La inexistència, actualment, de determinats rols clau en l'organització, com el responsable de seguretat, constitueix una de les deficiències més greus en termes de governança, ja que la seua responsabilitat, la gestió de la seguretat de la informació i dels serveis prestats, no pot considerar-se adequadament assumida per la resta dels responsables de l'organització. Considerem indispensable que un ens de la grandària de la Diputació amb els seus complexos sistemes d'informació dispose, almenys, d'una persona amb dedicació completa a les tasques de seguretat.

És molt convenient, per tant, solucionar de manera urgent les mancances identificades, que tenen un impacte negatiu en el nivell de seguretat de la informació, i l'explotació de les fortaleses existents, que potencialment facilitaran l'aplicació de mesures necessàries, incloses les recomanacions efectuades en aquest informe.

Són necessaris esforços per a impulsar l'aplicació de les millores destacades en l'informe amb la finalitat d'aconseguir el nivell de maduresa requerit. L'existència d'un lideratge recognoscible per tota la corporació pot fomentar els avanços en termes de conscienciació i ajudar a véncer les resistències naturals de l'organització als canvis exigits per la implantació d'una administració electrònica avançada.

Existeix un baix grau de compliment de la normativa relativa a la seguretat de la informació

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

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

Per a esmenar les deficiències de control que es detallen en l'apèndix 2, i millorar els nivells de control assenyalats en l'apartat anterior, formulem les recomanacions que s'assenyalen a continuació, per a l'atenció de les quals la Diputació haurà de dedicar els esforços i recursos necessaris. També s'assenyalen les mesures per al compliment de la legalitat que han d'adoptar-se.

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

1. Actualitzar la normativa de seguretat existent o aprovar procediments específics, de manera que recullen, amplien i representen amb fidelitat el conjunt de mesures implantades en la pràctica per al control dels dispositius físics.

2. Finalitzar la implantació de les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa, actualment en fase de planificació o inici d'execució.

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

3. Actualitzar la normativa de seguretat existent o aprovar procediments específics per al control de programari, de manera que recullen, amplien i representen amb fidelitat el conjunt de mesures ja implantades. Addicionalment, recomanem elaborar un catàleg d'aplicacions autoritzades i un pla anual de manteniment; aquest últim document està previst en la normativa aprovada existent.

4. Identificar i actualitzar tots els sistemes operatius que es troben fora del període de suport, ja que representen un risc per a la seguretat.

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

5. Modificar la normativa de seguretat existent o aprovar un procediment de seguretat específic per a la identificació i solució de vulnerabilitats, que reculla les accions que actualment es realitzen i que incloga addicionalment:

   – La priorització basada en l'anàlisi de riscos per a resoldre'ls.

- La realització de proves de penetració.

- Explotar adequadament les eines disponibles de gestió de fluxos de treball, que ja es troben configurades per a gestionar la identificació i solució de vulnerabilitats.

6. Resoldre les vulnerabilitats de nivell crític identificades.

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

7. Elaborar i aprovar un procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat, que detalle les mesures implantades actualment i considere particularment:

   - Eliminar tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat, de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.

   - Crear i utilitzar, en aquells sistemes en els quals no s'ha implantat l'ús dedicat de comptes d'administració, diferents comptes nominatius per a un mateix usuari amb diferents nivells de privilegis administratius, adequant l'assignació de permisos als diferents tipus de tasques a realitzar

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

8. Actualitzar i millorar la normativa existent o aprovar un procediment específic per a la configuració segura dels sistemes, de manera que considere la seguretat per defecte, el criteri de mínima funcionalitat i l'aplicació de mesures de gestió del procés. Per a això, proposem 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 de seguretat de les sèries 400, 500 i 600 del Centre Criptològic Nacional.

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

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

9. Actualitzar i millorar la normativa de seguretat existent o aprovar un procediment de seguretat específic per al tractament dels *logs* d'auditoria de la activitat dels usuaris, que incloga, com a mínim, els sistemes afectats, la informació que es registra, el període de retenció, les còpies de seguretat, la gestió de drets d'accés al registre i un procés per a revisar-los.

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

10. Encara que la normativa de seguretat existent recull parcialment el control de còpies de seguretat actualment implantat, hi ha diversos aspectes que cal millorar, en particular:

    - La revisió i actualització de la normativa de seguretat existent o aprovació d'un procediment de seguretat específic, que detalle adequadament el control implantat i que incloga l'ús d'eines de control de tasques o fluxos de treball en totes les seccions del servei d'informàtica.

    - L'execució d'un pla de proves periòdiques de recuperació que incloga tots els tipus de còpia.

    - La implantació efectiva de les eines i solucions que actualment estan en fase de planificació i la seua formalització en el procediment o normativa.

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

Hi ha diversos aspectes sobre els quals la Diputació ha d'actuar per a esmenar-los:

11. Per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat, la Diputació:

    - Ha d'atendre i solucionar les no conformitats identificades en l'auditoria de compliment realitzada l'any 2017.

    - Ha d'actualitzar la documentació relativa al procés d'adequació a l'ENS, incloent-hi la política de seguretat, la normativa de seguretat, el Pla d'Adequació i la Declaració d'Aplicabilitat.

    - Ha de realitzar els nomenaments necessaris per als rols definits en la Política de Seguretat, especialment el responsable de seguretat.

    - Ha de realitzar les auditories de seguretat previstes en l'article 34 del Reial Decret 3/2010.

    - 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.

12. En relació amb la protecció de dades personals, la Diputació:

    - Ha de finalitzar l'anàlisi de riscos sobre els tractaments de dades personals d'acord amb l'article 32.2 de l'RGPD.

    - Ha de realitzar les avaluacions d'impacte dels riscos detectats de nivell alt.

– Ha de realitzar auditories en matèria de protecció de dades.

13. En relació amb la Llei de Factura Electrònica, la Diputació ha de realitzar les auditories de sistemes anualment tal com exigeix aquesta norma.

Priorització de les recomanacions

A fi que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial a mitigar** i **cost estimat de la seua implantació**. No s'hi inclouen els punts 11 a 13 anteriors, ja que són mesures d'obligat compliment. S'inclouen en el gràfic les recomanacions pendents d'implementar del nostre informe anterior, amb referències A a F, que es comenten en l'apartat següent.

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

Seguiment de recomanacions anteriors

Hem realitzat un seguiment de les recomanacions sobre el control intern de l'Informe sobre auditoria operativa de la gestió i recaptació delegada en les diputacions de la Comunitat Valenciana. Exercici 2016. Tal com es mostra en el quadre següent, de les sis recomanacions realitzades en aquell informe, quatre no s'han atés i dues ho han sigut només parcialment, per la qual cosa totes continuen vigents.

Quadre 2. Seguiment de recomanacions

	Recomanacions sobre els controls generals de tecnologies de la informació de l'informe anterior	Situació a 30 de setembre de 2021	
A	Proposem a la Diputació de València aprovar procediments que garantisquen els principis de segregació de funcions i de mínims privilegis per a les funcions assignades en el Departament de Sistemes d'Informació.	Hem verificat que no han sigut aprovats procediments o normatives que regulen específicament la segregació de funcions i l'aplicació del principi de mínim privilegi.	**No aplicada**
B	Recomanem a la Diputació de València la realització periòdica de proves de les interfícies per a garantir la integritat, validesa i la completesa de la informació.	Sense variació.	**No aplicada**
C	És convenient que la Diputació de València aprove un procediment per a la revisió d'incidències de seguretat i d'accessos a la informació i la implantació d'eines que faciliten l'anàlisi de les incidències i les activitats rellevants del sistema d'informació.	Hem verificat que no han sigut aprovats procediments o normatives que regulen específicament la revisió d'incidències de seguretat i d'accessos a la informació. Hem verificat que s'ha iniciat un projecte, en col·laboració amb la Direcció General de Tecnologies de la Informació i les Comunicacions (DGTIC) de la Generalitat i el Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV), per al monitoratge, emmagatzematge i interpretació dels registres d'activitat de determinats sistemes i serveis crítics que són oferits per la Diputació als ajuntaments.	**Aplicada parcialment**
D	Proposem a la Diputació de València aprovar formalment un procediment de gestió d'usuaris, i que la gestió de les funcionalitats dels usuaris es base en perfils predefinits segons el lloc de treball, aplicant el principi d'assignar les mínimes capacitats per a poder fer les tasques assignades. El procediment ha d'incloure la revisió periòdica d'usuaris que permeta mantindre en el temps el principi assenyalat.	Hem verificat que no han sigut aprovats procediments o normatives que regulen específicament la gestió d'usuaris i l'assignació de privilegis a aquests.	**No aplicada**

	Recomanacions sobre els controls generals de tecnologies de la informació de l'informe anterior	Situació a 30 de setembre de 2021	
E	La Diputació de València hauria de configurar polítiques de control d'accessos a sistemes i aplicacions perquè s'ajusten a les bones pràctiques generalment acceptades i a les exigències de l'ENS. D'acord amb la informació facilitada en la data d'emissió d'aquest informe, la Diputació de València ha millorat les polítiques de control d'accessos a l'aplicació Estima, encara que considerem que s'ha de reforçar encara més fins a aconseguir els paràmetres exigits per l'ENS.	Hem verificat que s'han implantat determinades millores en el procés d'autenticació dels usuaris. No obstant això, el conjunt de mesures implantades per al control dels accessos a aplicacions i sistemes no aconsegueix els nivells exigits per l'ENS.	**Aplicada parcialment**
F	Recomanem a la Diputació de València aprovar al més prompte possible un pla de continuïtat de l'activitat i de recuperació davant desastres, documentats per escrit i aprovats formalment per la Direcció. Prèviament serà necessari realitzar una anàlisi de riscos o una anàlisi d'impacte en els serveis prestats per a establir la criticitat i prioritat dels actius de l'entitat (serveis, informació, aplicacions, dispositius de xarxa i servidors, etc.), així com els punts i terminis necessaris per a la recuperació de la informació i els sistemes.	Hem verificat que no s'ha elaborat i aprovat un pla de continuïtat de l'activitat i de recuperació davant desastres.	**No aplicada**

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 han sigut iniciades o planificades actuacions en matèria de ciberseguretat en diversos àmbits que atendrien algunes de les recomanacions anteriors. Aquestes actuacions es troben alineades amb els objectius de la Diputació per a l'adequació a l'ENS i algunes s'han iniciat a conseqüència de les observacions realitzades en el transcurs d'aquesta auditoria. La implantació efectiva d'aquestes actuacions tindrà un impacte positiu en el nivell de ciberseguretat de l'entitat.

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

- Implantació d'un nou control d'accés a xarxa que comportarà una millora rellevant en el control d'actius físics no autoritzats.

- Implantació d'un nou sistema per a la gestió centralitzada dels comptes d'administradors locals, que limita els riscos en cas de compromís d'un equip.

- Implantació d'un sistema que proporciona les característiques tècniques necessàries per a millorar els processos de còpia de seguretat actuals, segons els nous requisits identificats.

- Implantació d'una estratègia d'adopció massiva de sistemes en núvol. Aquest model permet una major escalabilitat, tant de la infraestructura tecnològica com de les aplicacions de gestió, per a fer front a demandes que no són assumibles amb un desplegament exclusivament local.

- Implantació d'una gestió avançada i auditoria de sistema de fitxers i directori actiu, per mitjà de l'ús combinat d'eines comercials i del Centre Criptològic Nacional, que possibilite un manteniment més eficient i segur dels permisos d'accés a informació per part dels usuaris, i que mantinga la informació xifrada i classificada, de manera que proporcione una protecció addicional contra els atacs de *ransomware*.

- Implantació d'un sistema per al monitoratge, emmagatzematge i interpretació dels registres d'activitat de determinats sistemes i serveis crítics que la Diputació ofereix als ajuntaments, en el marc d'un projecte en col·laboració amb la Direcció General de Tecnologies de la Informació i les Comunicacions (DGTIC) de la Generalitat i el Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV).

- Posada en marxa de diverses iniciatives per a promoure la conscienciació en matèria de seguretat de la informació entre el personal de la Diputació.

APÈNDIX 1
Metodologia aplicada

Introducció

Cada vegada més un major nombre d'aspectes de la gestió pública es realitzen amb el suport de complexos sistemes informatitzats, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de tota mena 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 les diputacions en particular, no són alienes a aquesta preocupació per la ciberseguretat en la seua pròpia operatòria, per la qual cosa han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat, que és d'obligat compliment.

És imperatiu que els responsables de les diputacions 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 ocorreguts que es realitza en els informes INES[3] del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs estiguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan correctament implementades.

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) –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.

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

Objectiu de l'auditoria

El nostre objectiu ha sigut obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats, proporcionant una avaluació tant sobre el seu disseny[4] com sobre la seua eficàcia operativa[5] per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport, 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.

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.

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 recaptatòria, així com els controls que tenen implantats.

[4] 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, si és capaç de complir l'objectiu de control.

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

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

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

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls en 2021. L'auditoria es va iniciar al desembre de 2020 i el treball de camp va finalitzar el 30 de setembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe, ja que fins llavors és admesa qualsevol evidència addicional disponible. Per tant, amb caràcter general l'Informe reflecteix la situació en aquell moment, ja que és freqüent que, des que s'inicia el treball de camp, determinades deficiències observades i assenyalades als gestors siguen esmenades i són considerades d'aquesta manera en les conclusions i en els indicadors.

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

Metodologia

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

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

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

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

La guia pràctica de fiscalització dels OCEX 5313

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

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS. No obstant això, atesa l'amplitud de l'ENS, que està format per 75 mesures de seguretat, per a la seua inclusió en els CBCS es va seleccionar una sèrie limitada de controls. Per a triar els més rellevants es va atendre el marc conceptual establit per la prestigiosa organització Center for Internet Security (CIS)[6], que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. El seu avantatge principal és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant ciberatacs al voltant del 85%. Si s'implementen els vint controls el risc es pot reduir un 94%.

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

Atés que l'ENS és d'obligat compliment per a tots els ens públics, s'ha tingut especial cura a fer 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 de l'ENS següents:

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

Quadre 3. Els CBCS i l'ENS

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

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

Els CBCS com a mesures de ciberhigiene

L'European Union Agency for Cybersecurity (ENISA) assenyala[7] que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen", reduint els ciberiscos.[8]

Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats als quals s'enfronta hui dia.[9]

En aquest sentit, ENISA estableix deu punts d'acció per a una adequada ciberhigiene. 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.

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

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

[9] 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 els pedaços s'han posat adequadament	CBCS 2
3. Utilitzar guies de configuració segura i fortificació per a tots els dispositius	CBCS 5
4. Gestionar les dades que entren i ixen de la xarxa	–
5. Escanejar tots els correus electrònics entrants	–
6. Minimitzar els usuaris administradors	CBCS 4
7. Realitzar còpies de seguretat de dades regularment i fer proves de restauració	CBCS 7

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

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

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

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

Quadre 5. Els CBCS i els seus subcontrols

Control	Objectiu del control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots els dispositius de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats	L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
		CBCS 1-2: Control d'actius físics no autoritzats	L'entitat disposa de mesures de seguretat per a controlar (detectar i restringir) l'accés de dispositius físics no autoritzats.
CBCS 2 Inventari i control de programari autoritzat	Gestionar activament tot el programari en els sistemes, de manera que només es puga instal·lar i executar programari autoritzat.	CBCS 2-1: Inventari de programari autoritzat	L'entitat disposa d'un inventari de programari complet, actualitzat i detallat.
		CBCS 2-2: Programari suportat pel fabricant	El programari utilitzat per l'entitat té suport del fabricant. En cas contrari, es marca en l'inventari com fora de suport.
		CBCS 2-3: Control de programari no autoritzat	L'entitat disposa de mecanismes que impedeixen la instal·lació i execució de programari no autoritzat.
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats	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 realitza 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 facilita el seu 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'incidències 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 seua consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de *logs*.	Els *logs* de tots els sistemes són revisats periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels *logs* d'auditoria, de manera que se'n facilite la revisió.
		CBCS 6-4: Monitoratge i correlació	L'entitat disposa d'un SIEM (*security information and event management*) o una eina d'analítica de *logs* per a realitzar correlació i anàlisi de *logs*.
CBCS 7 Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú.	CBCS 7-1: Realització de còpies de seguretat	L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema.
		CBCS 7-2: Realització de proves de recuperació	Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmeses a través de la xarxa.
CBCS 8 Compliment normatiu i governança de ciberseguretat	L'entitat compleix els requisits legals i reglamentaris que li són aplicables i té establida una governança de ciberseguretat adequada.	CBCS 8-1: Compliment de l'ENS	L'entitat compleix els requeriments establits en l'ENS.
		CBCS 8-2: Compliment de la LOPD/RGPD	L'entitat compleix els requeriments establits en la LOPD/RGPD.
		CBCS 8-3: Compliment de la Llei 25/2013	L'entitat compleix els requeriments establits en la Llei 25/2013, de 27 de desembre.

Avaluació dels resultats del treball

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

Subcontrols

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

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

Quadre 6. Avaluació dels subcontrols

Avaluació	Descripció
Control efectiu	Cobreix al 100% amb 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	A grans trets, compleix l'objectiu de control, si bé pot haver-hi uns 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 les

GPF-OCEX 5313, que al seu torn estan basades en la *Guia de seguretat CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 7. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El control no s'està aplicant en aquest moment.
N1 Inicial / ad hoc	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant 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 els 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 una mica 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 sobre la 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'ha tingut en compte els resultats obtinguts en la revisió dels subcontrols que el formen.

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

Confidencialitat	És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.
Integritat	És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, i s'assegura 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, amb el criteri del principi de proporcionalitat.

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[10]

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 el *N3, procés definit,* i un índex de maduresa del 80%.

[10] *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 han sigut adaptats per a la seua aplicació als CBCS, ja que permeten dur a terme un resum de l'estat de les mesures de seguretat dels ens auditats:

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

- L'**índex de compliment** analitza igualment el nivell de maduresa aconseguit, però en relació amb l'exigència aplicable en cada cas, tenint en compte la categoria del sistema. 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 adreça 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.[11]

Els principals elements d'una governança adequada 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 als 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**.[12]

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.

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

[12] Vegeu apartat 66 d'*Análisis N.º 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.[13] L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació[14] 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 ha de ser difosa entre la totalitat dels membres de l'organització, així com, si és el cas, a proveïdors i tercers.

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

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

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

  La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,[15] que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat, i és la màxima autoritat en l'organització respecte a les decisions de seguretat que afecten els sistemes que manegen informació o presten algun servei. La seua composició ha de constar en la PSI.

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

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

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

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

[13] *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.

[14] *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información*, apartat 3.4.

[15] *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'apèndix 5 de l'"Informe sobre auditoria operativa de la gestió i recaptació delegada en les diputacions de la Comunitat Valenciana. Exercici 2016".

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

Total 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 efecte 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 continua sense aplicar-se.
Sense validesa en el marc actual	S'hi inclouen aquelles recomanacions que, encara que vàlides i pertinents quan es va emetre l'informe i per a l'exercici fiscalitzat, i fins i tot en cas que hagen sigut acceptades i reconegudes per l'ens fiscalitzat, no poden aplicar-se en el context actual, per no donar-se 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 30 de setembre 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, així com amb qualsevol deficiència significativa dels controls interns que identifiquem en el transcurs de l'auditoria.

Com 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 la Diputació 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 a la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.

Situació del control

Hem verificat que la Diputació realitza diverses accions per a mantindre actualitzat l'inventari i control d'actius físics de l'entitat, però aquestes no s'han detallat en un procediment formalment aprovat i la normativa existent únicament especifica la necessitat de disposar d'un inventari d'actius.

La Diputació disposa de diverses eines per a l'administració dels actius que permeten inventariar automàticament els elements.

L'electrònica de xarxa es troba inventariada per una eina propietària del fabricant que permet, addicionalment, l'administració de tots els dispositius.

Els equips d'usuaris, servidors i resta de dispositius es troben inventariats per mitjà d'una eina que es troba integrada amb el servei de directori i la plataforma de virtualització, en una implementació particularment efectiva que permet l'obtenció automàtica de dades dels actius. Per a elements que no es troben en domini o no són màquines virtuals, l'inventari es realitza manualment o per mitjà de la instal·lació d'un agent.

Addicionalment, hem verificat que existeix un adequat procés de gestió i aprovació de nous actius i de retirada o substitució d'actius existents, procés que es troba adequadament establit en el gestor de fluxos de treball. La configuració de les diferents eines juntament amb el procés de gestió definit permet confirmar que els inventaris existents es troben acceptablement actualitzats per a tots els seus elements.

D'altra banda, malgrat que es troba en fase d'execució un projecte destinat a la implantació d'un sistema de control d'accés a la xarxa, aquest sistema no es troba operatiu i en l'actualitat no s'apliquen controls compensatoris que detecten, impedisquen o limiten l'activitat dels dispositius físics no autoritzats en la xarxa interna de la Diputació.

Existeix cert nivell de control sobre l'inventari i el control d'actius físics, i la seua valoració global aconsegueix un **índex de maduresa del 50,3%,** que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 1 del 62,8%**.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

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

Situació del control

Hem analitzat la gestió que realitza la Diputació sobre l'inventari i control de programari i hem verificat que el procés implantat no ha sigut detallat en un procediment formalment aprovat i la normativa existent únicament especifica la necessitat de disposar d'un inventari d'actius.

Hi ha determinades aplicacions que proporcionen suport a processos essencials que es troben virtualitzades, de manera que el seu inventariat i control està centralitzat en l'eina de gestió d'aplicacions virtualitzades.

Per a aquelles aplicacions instal·lades directament en els equips d'usuari, la Diputació disposa d'un inventari de gestió automatitzada per a l'administració de l'actiu programari gestionat pel Servei d'Informàtica. L'inventari inclou el programari instal·lat en els dispositius de l'entitat, la versió, el nombre de llicències disponibles i nombre de llicències instal·lades, entre altra informació, i es troba relacionat amb l'inventari d'actius físics de l'entitat.

Quant a la gestió del programari no autoritzat, l'entitat compta amb mesures orientades a impedir-ne l'ús que en conjunt poden considerar-se parcialment efectives.

La gestió del llicenciament, l'autorització per a la instal·lació i ús de nou programari i el manteniment d'unes certes aplicacions, es realitzen per mitjà d'un procés que es troba adequadament establit en el gestor de fluxos de treball, però que no ha sigut formalitzat en un procediment aprovat ni es disposa d'un pla de manteniment.

S'ha evidenciat l'existència d'un elevat nombre d'equips amb sistemes operatius fora del període de suport del fabricant, incloent-hi servidors i equips d'usuari, fet que suposa un greu risc per als sistemes d'informació i constitueix una deficiència de control molt significativa.

Hi ha un nivell insuficient de control sobre l'inventari i control de programari autoritzat, que aconsegueix un **índex de maduresa del 45,0%,** 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 organitzada correctament. Això representa un **índex de compliment del CBCS 2 del 56,3%**.

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 les accions dutes a terme per la Diputació per a la gestió de vulnerabilitats i pedaços de sistemes i hem observat que, encara que existeix una normativa aprovada que recull determinades obligacions respecte al control, el document no descriu adequadament la gestió realment implantada.

La identificació i solució de vulnerabilitats es realitza per part del personal del Servei d'Informàtica, si bé es disposa de contractes amb tercers que proporcionen suport per a l'actualització de determinats sistemes.

La Diputació utilitza diversos mitjans per a la identificació de vulnerabilitats, com la subscripció a comunicacions de fabricants o organismes de referència o la realització d'auditories per part del CSIRT-CV, Centre de Seguretat TIC de la Comunitat Valenciana.

Les vulnerabilitats són prioritzades i resoltes per mitjà d'un procés informal que no es troba adequadament descrit en la normativa existent. Únicament una part del procés complet es troba suportada per l'ús d'eines de gestió de fluxos de treball, la qual cosa impedeix gestionar completament el control.

Sobre l'aplicació de pedaços i actualitzacions, es realitza en general de manera automatitzada per mitjà de diverses eines de gestió centralitzada de pedaços, en el cas d'aquells tipus de sistemes amb nombrosos actius. Hem verificat que el control es troba adequadament implantat i gestionat per a la major part dels sistemes.

Hem verificat que, a causa de l'existència de sistemes que no disposen de suport del fabricant, han sigut detectades múltiples vulnerabilitats de nivell crític que es troben pendents de resolució o sobre les quals no es disposa del pedaç de seguretat corresponent. Aquesta situació constitueix una greu deficiència de control i un elevat risc per als sistemes d'informació de la Diputació.

Hi ha un nivell insuficient de control sobre la gestió de vulnerabilitats, de manera que la valoració global del control aconsegueix un **índex de maduresa del 47,9%,** que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 3 del 59,8%**.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

Hem analitzat les accions realitzades per al control dels comptes d'administració i hem verificat que, encara que s'han aplicat determinades mesures, aquestes no s'han detallat en un procediment formalment aprovat i la normativa existent únicament especifica determinats aspectes que no descriuen adequadament el control.

La gestió de l'assignació de privilegis administratius en els sistemes revisats es realitza amb diferent grau d'efectivitat depenent del sistema i de manera independent per a cada un, atés que no ha sigut aprovat ni implantat un procediment que establisca les polítiques comunes de gestió de privilegis administratius de manera general en la Diputació. Hem verificat que el control complet s'aplica de manera particularment eficaç sobre el sistema que proporciona suport a la gestió tributària i recaptatòria.

Amb caràcter general, es fa un ús adequat de comptes nominatius per als usuaris amb privilegis administratius. No obstant això, en determinats sistemes revisats s'ha detectat l'ús de comptes no nominatius compartits, la qual cosa dificulta la traçabilitat de les accions en cas d'incidents. Aquesta deficiència es troba parcialment compensada per un inventariat i control adequats en l'ús d'aquests comptes.

S'ha evidenciat una provisió adequada de privilegis en els serveis i sistemes de la Diputació, que inclou un procés d'autorització per mitjà del gestor de fluxos de treball per part del responsable del sol·licitant i el responsable del Servei d'Informàtica. No obstant això, no s'ha establit un procés periòdic de revisió, la qual cosa implica un risc d'incompliment dels principis d'assignació de privilegis per canvis en servei i constitueix una deficiència de control.

Es realitza una aplicació correcta de l'ús dedicat de comptes d'administració en els sistemes revisats i els usuaris administradors disposen de comptes diferenciats per a tasques que requerisquen diferents nivells de privilegis administratius. Aquesta mesura ha sigut implantada recentment.

La Diputació no disposa d'una política que definisca específicament els mecanismes d'autenticació dels sistemes de l'entitat, de manera que, si bé s'han establit en determinats sistemes requisits d'autenticació i una política de contrasenyes robusta, aquests criteris no s'apliquen de manera homogènia en tots els sistemes de l'entitat.

Finalment, encara que aquests registres es troben activats en tots els sistemes revisats i són emmagatzemats i centralitzats en sistemes de gestió de *logs*, no existeix un procés de revisió sistemàtic.

Existeix cert nivell de control sobre els comptes amb privilegis administratius, per la qual cosa la valoració global del control existent aconsegueix un **índex de maduresa del 55,5%,** 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 d'aquest CBCS 4 del 69,3%**.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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

Situació del control

Hem analitzat les accions realitzades per al control de la configuració segura en aplicacions i dispositius i hem verificat que no es troben completament recollides en la normativa aprovada existent, que no tenen el detall necessari i no representa amb total fidelitat el control implantat.

L'entitat realitza accions per a configurar la seguretat en determinats sistemes, però aquestes accions no són suficients per a garantir l'efectivitat del control. S'ha verificat que es disposa de plantilles i protocols informals per a la configuració de determinats dispositius que prevegen l'aplicació de certes configuracions que proporcionen un determinat nivell de seguretat. No obstant això, aquestes plantilles i protocols no tenen caràcter de fortificació ni la seguretat per defecte és el seu objecte.

Addicionalment, hem identificat l'aplicació d'un conjunt de configuracions específiques per a la protecció de les connexions remotes segons les recomanacions del CSIRT-CV, a conseqüència de la implantació majoritària del teletreball en resposta a la crisi sanitària de la COVID-19.

Sobre el monitoratge de les configuracions existents, hem verificat que s'han establit mesures que permeten gestionar les configuracions de determinats dispositius crítics de l'entitat, però aquestes mesures no permeten monitorar possibles modificacions no autoritzades de les configuracions.

La valoració global del control existent sobre les configuracions segures és que l'organització aconsegueix un **índex de maduresa del 44,1%,** que es correspon amb un **nivell de maduresa *N1, inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o

la seua gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 55,1%**.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

Hem analitzat les accions de la Diputació per al registre de l'activitat dels usuaris en els diferents sistemes i hem verificat que les mesures aplicades no es troben completament recollides en la normativa aprovada existent, que no tenen el detall necessari i no representen amb total fidelitat el control implantat.

Hem verificat que el registre d'activitat es troba activat en tots els sistemes revisats. Si bé es manté la configuració per defecte en alguns sistemes, hem verificat que s'han aplicat, en determinats sistemes crítics, configuracions específiques per a retenció de registres conforme a les necessitats identificades i segons les recomanacions del fabricant.

La Diputació disposa de diversos sistemes per a la gestió centralitzada de registres d'activitat de determinats grups d'actius, la qual cosa suposa una millora sobre la configuració bàsica per defecte dels *logs* d'auditoria. No obstant això, la revisió d'aquests registres d'activitat es realitza de manera informal, no procedimentada.

La Diputació ha iniciat el projecte col·laboratiu vSOC (Centre d'Operacions de Seguretat Virtual) amb la Direcció General de Tecnologies de la Informació i les Comunicacions (DGTIC), per a la gestió centralitzada de la seguretat d'entitats locals. Aquest projecte, articulat per mitjà de la participació del CSIRT-CV, inclou l'ús de l'eina Gloria del Centre Criptològic Nacional, sistema SIEM per al monitoratge, emmagatzematge i interpretació de dades, que recull i analitza els registres d'activitat de determinats sistemes de la Diputació i de serveis crítics que són oferits als ajuntaments.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització 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 6 del 93,8%**.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

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

Situació del control

La Diputació realitza diverses accions en relació amb les còpies de seguretat de les dades i sistemes i la responsabilitat sobre aquestes accions es troba recollida en la normativa de seguretat, però no existeix un procediment aprovat que detalle el control implantat.

Les diferents seccions que componen el Servei d'Informàtica realitzen còpies de seguretat sobre els actius que gestionen de manera independent. Els recursos i mitjans tècnics són compartits per tota l'organització, però la gestió sobre la realització de còpies la realitza de manera autònoma cada secció, de manera que s'ha verificat una gestió amb un nivell de maduresa molt desigual entre les diferents seccions.

La Diputació disposa d'un conjunt d'eines i sistemes per a la realització de còpies que disposa de característiques tècniques adequades i cobreix les necessitats de l'organització quant al procés de realització de còpies de seguretat establit. Les polítiques de còpia aplicades s'han desenvolupat d'acord amb les necessitats identificades pel servei d'informàtica, però no s'ha realitzat un exercici de definició de necessitats per part dels responsables funcionals dels serveis.

Hem verificat que la gestió i revisió de còpies realitzada per la Secció de Sistemes i Comunicacions és un procés manual que es realitza de manera correcta però que no es troba suportat per eines de control de tasques o fluxos de treball, fet que no garanteix l'eficàcia del control en tots els casos.

La gestió sobre les còpies realitzada per la Secció de Bases de Dades es troba suportada per un ús particularment adequat de l'eina de control de tasques o fluxos de treball. A més, es troben en avançat estat d'elaboració un conjunt de guies i procediments que detallen adequadament el control implementat.

Es realitzen de manera sistemàtica proves de recuperació planificades en un entorn de preproducció, encara que únicament s'hi inclouen determinats tipus de còpies. Addicionalment, es realitzen i registren freqüents recuperacions satisfactòries de diversos tipus de còpies en cas de pèrdua de dades o serveis.

El conjunt d'eines i sistemes disponibles per a la realització de còpies inclou diferents mecanismes destinats a la seua protecció que poden considerar-se efectius davant de determinades amenaces. No obstant això, hem verificat que es troba en fase de planificació un projecte que proporcionarà un nivell de seguretat addicional a determinats tipus de còpia.

La valoració global del control existent sobre les còpies de seguretat és que la Diputació 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 7 del 75,0%**.

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

La Diputació ha realitzat diferents accions orientades a donar compliment al que exigeix el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica:

- En 2013, el Ple de la Diputació va aprovar la Política de Seguretat de la Informació (PSI), el contingut de la qual s'adequa als requisits establits per l'ENS.
- A conseqüència de l'aprovació de la PSI, es van designar els responsables previstos en la política i va ser creat el Comité de Seguretat.
- S'ha desenvolupat la normativa associada a la PSI, que inclou una normativa específica per als usuaris dels sistemes d'informació i una altra normativa per al personal tècnic dels sistemes.
- El Comité de Seguretat va aprovar la Declaració d'Aplicabilitat i el Pla d'Adequació.
- S'ha emplenat i remés Informe de l'Estat de la Seguretat (Informe INES) fins a l'any 2018.
- S'han realitzat auditories de compliment previstes en l'article 34 fins a l'any 2017, en les quals s'han identificat no conformitats.

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

- No s'han desenvolupat procediments operatius de seguretat que completen el marc normatiu existent.
- No s'han solucionat les nombroses no conformitats identificades en les auditories, ni s'ha certificat el compliment de l'ENS.

- Des de l'any 2018, i a causa del nomenament com a delegat de protecció de dades del funcionari que ostentava el rol de responsable de seguretat, s'ha produït el cessament de les activitats relatives al compliment de les obligacions respecte a l'Esquema Nacional de Seguretat i, com a resultat, ens han indicat que des de l'any 2018:

  - No s'han actualitzat els documents que suporten el procés d'adequació a l'ENS ni la política de seguretat.

  - No s'han remés els informes de l'estat de la seguretat.

  - No s'han celebrat reunions del Comité de Seguretat TIC.

  - No ha sigut nomenat un nou responsable de seguretat.

Compliment RGPD

Quant al compliment en matèria de protecció de dades personals, la Diputació ha realitzat diverses accions que han sigut revisades durant aquest treball d'auditoria:

- La Diputació ha nomenat delegat de protecció de dades i ho ha notificat a l'Agència Espanyola de Protecció de Dades, tal com exigeix l'article 37 de l'RGPD.

- S'ha elaborat un registre d'activitats del tractament, que inclou el detall necessari. A més, aquest registre ha sigut publicat i és accessible per mitjans electrònics.

- Es troba en fase de redacció un plec per a la contractació d'un servei de consultoria i suport tècnic en matèria de seguretat de la informació al departament de protecció de dades i seguretat de la informació.

- S'han establit iniciatives per part del Departament de Protecció de Dades i Seguretat de la Informació que han sigut guardonades amb el premi de Protecció de Dades 2018, "Bones pràctiques en privacitat i protecció de dades personals sobre iniciatives per a adaptar-se al Reglament Europeu de Protecció de Dades", que atorga l'Agència Espanyola de Protecció de Dades. Les iniciatives identificades són:

  - L'elaboració i difusió d'una guia de teletreball, que, en resposta a la regulació del teletreball i a la crisi sanitària de la COVID-19, detalla els aspectes que cal considerar des de la perspectiva de la protecció de dades i la seguretat de la informació.

  - L'execució de projecte DivalData, que consta d'un conjunt d'iniciatives destinades a les entitats locals per a dotar-les d'eines amb les quals se'ls pretén facilitar el compliment de la normativa actual de protecció de dades.

No obstant això, s'han identificat les mancances següents:

- No ha sigut finalitzat una anàlisi de riscos sobre els tractaments de dades personals conforme a l'article 32.2 de l'RGPD.

- No s'han realitzat les avaluacions d'impacte dels riscos detectats de nivell alt.
- No s'han realitzat auditories en matèria de protecció de dades des de l'any 2017.

Compliment legalitat del registre de factures

Està pendent de realitzar l'auditoria del registre de factures de 2020 exigida 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 és que la Diputació aconsegueix un **índex de maduresa del 30,0%**, que es correspon amb un **nivell de maduresa N1**, que indica que existeixen incompliments significatius generalitzats de la normativa, i hi ha aspectes que s'han de millorar.

Governança de ciberseguretat

La Diputació de València té establida una governança insuficient de la seguretat de la informació.

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

Si bé en l'auditoria hem observat l'existència d'un cert nivell de compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de la Diputació i els gestors i responsables de les àrees implicades, **existeixen mancances rellevants que indiquen que la governança no és adequada**. Les mancances més rellevants identificades, que dificulten l'establiment d'un sistema de gestió de la seguretat de la informació (SGSI) efectiu, són les següents:

- La **falta d'actualització de polítiques i formalització d'objectius estratègics** de l'entitat, la qual cosa invalida la utilitat de les polítiques existents, atés que aquestes no es corresponen amb les necessitats reals de l'organització.
- La **inexistència de determinats rols clau** en l'organització, com el responsable de seguretat, o la falta d'activitat efectiva i continuada dels rols existents quant als processos relacionats amb la seguretat de la informació.

  La inexistència d'un responsable de seguretat constitueix probablement la deficiència més greu en termes de governança, ja que la seua responsabilitat, la gestió de la seguretat de la informació dels serveis prestats, no pot considerar-se adequadament assumida per la resta dels responsables de l'organització.

  De la mateixa manera, hem verificat que cap dels recursos existents en el Servei d'Informàtica disposa de dedicació completa a la seguretat de la informació, atés que

la seua dedicació és compartida entre múltiples competències. Aquesta falta de rols amb dedicació exclusiva impedeix que el conjunt d'accions i mesures implantades puguen constituir-se com a processos d'execució contínua i siguen percebuts com a accions puntuals, cosa que dificulta l'establiment d'un SGSI efectiu.

- La **falta d'activitat continuada del Comité de Seguretat**. Hem verificat que, si bé el comité de seguretat ha sigut formalment constituït, aquest no ha tingut activitat en els últims tres anys ni hi ha grups de treball auxiliars que hagen assumit totalment o parcialment les funcions del comité en aquest període.

  Aquesta falta d'activitat de l'òrgan, clau en el govern de la seguretat en tant que promou la presa de mesures, la millora contínua i la coordinació dels esforços de les diferents àrees, impedeix l'organització efectiva de la seguretat en l'entitat.

- La **falta de compliment normatiu**. Tal com es detalla en subapartats anteriors, existeix un insuficient nivell de compliment de la legalitat en matèria relacionada amb la seguretat de la informació.

No obstant això, sí que s'han identificat alguns aspectes positius:

- Suport en forma d'inversions i l'articulació de mesures per a la gestió de riscos. Hem verificat l'increment de les inversions previstes per a l'exercici 2022 (en el moment de redactar aquest informe estava pendent de la seua incorporació definitiva al pressupost) que permetran el desenvolupament de projectes i la implantació de sistemes que tindran un potencial impacte positiu en el nivell de seguretat de l'organització.

- La coordinació per part dels responsables de les àrees implicades en la seguretat de la informació amb òrgans de referència, a fi de promoure projectes comuns, millores en la gestió de la seguretat, i coordinar el tractament d'incidents.

Resulta, per tant, necessària la solució urgent de les mancances identificades, que tenen un impacte negatiu en el nivell de seguretat de la corporació. En aquest sentit, els òrgans de govern tenen la responsabilitat de liderar i ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat.

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 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 la auditoria i que destaquen en relació amb l'estat de la qüestió 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, han sigut considerats en l'avaluació dels CBCS. No obstant això, alguns no formen part dels CBCS tal com estan definits en la GPF-OCEX 5313, però els comentem per les raons indicades adés. 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.

Coordinació amb organismes de referència en ciberseguretat

L'entitat ha establit una coordinació particularment efectiva amb la Direcció General de Tecnologies de la Informació i les Comunicacions (DGTIC) de la Generalitat i el Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV).

Aquesta coordinació s'ha materialitzat en diversos àmbits:

- La gestió d'incidents de seguretat. Durant la realització del treball ens han informat de la materialització de determinades amenaces a les quals van fer front de manera conjunta els tècnics de la Diputació i el personal del CSIRT-CV. Les mesures adoptades durant la gestió dels incidents van ser efectives, de manera que van minimitzar el seu impacte, sense conseqüències rellevants en l'operativa de l'entitat. La implantació de les recomanacions emeses pel CSIRT-CV, juntament amb les d'aquest informe, reduirà la probabilitat de materialització d'amenaces de naturalesa similar.

- L'execució de projectes col·laboratius. Particularment el projecte vSOC (Centre d'Operacions de Seguretat Virtual), impulsat per la DGTIC i per mitjà de la participació del CSIRT-CV, per a la implantació d'un sistema de monitoratge, emmagatzematge i interpretació de dades de determinats sistemes i serveis crítics que la Diputació ofereix als ajuntaments. Considerem que la coordinació de diferents entitats en aquestes qüestions és essencial.

- L'assessorament tècnic en la implantació de mesures per a permetre el teletreball durant el període de pandèmia. La Diputació ha aplicat un conjunt de configuracions específiques per a la protecció de les connexions remotes segons les recomanacions del CSIRT-CV, a conseqüència de la implantació majoritària del teletreball en resposta a la crisi sanitària de la COVID-19.

Explotació de l'eina de gestió automatitzada de bitllets en determinats processos de l'entitat

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

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

- La integració amb el servei de directori i la plataforma de virtualització, que permet l'obtenció automàtica de dades dels actius i facilita l'actualització i gestió de l'inventari.

- El registre automàtic en l'eina de les vulnerabilitats identificades com a resultat de les auditories periòdiques del CSIRT-CV, cosa que facilita la seua gestió i resolució.

- La integració de processos de gestió de determinades còpies de seguretat, en una implementació particularment adequada de les tasques relacionades, creació de registres en la base de dades de coneixements de l'eina i suport documental per a formalització dels processos de gestió.

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 la Diputació (en particular, el president o la presidenta i la Junta de Govern). Són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions i una governança de ciberseguretat adequada.

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

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

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

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

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

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

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i descriuran: *a*) l'ús correcte d'equips, serveis i instal·lacions; *b*) el que es considerarà ús indegut, i *c*) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat ha d'estar a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular d'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 té origen i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desplegament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

Política de seguretat de la informació: És un document d'alt nivell que defineix el que significa "seguretat de la informació" en una organització d'acord amb l'article 11 del Reial Decret 3/2010 i articula la gestió continuada de la seguretat. Ha de ser aprovada per la junta de govern d'un ajuntament 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 i indiquen el 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.

Prova de penetració: És un atac a un sistema informàtic amb la intenció de trobar les debilitats de seguretat i tot el que hi podria tindre accés, la seua funcionalitat i dades.

Sistema de gestió d'incidències i informació de seguretat: Un SIEM, del terme anglés *security information and event management*, és un sistema que centralitza l'emmagatzematge i la interpretació de les dades rellevants de seguretat. Permet una anàlisi de la situació des d'un punt de vista unificat que facilita la detecció de tendències i patrons no habituals.

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

TRÀMIT D'AL·LEGACIONS

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

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

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

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

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

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

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*h* del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2020 i 2021 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 2 de febrer de 2022, va aprovar aquest informe de fiscalització.

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 202200123	FECHA DE ENTRADA 14/01/2022 8:34
ÁREA Fiscalización - Alegaciones	PROCEDIMIENTO PAA2021/25 Auditoría de los controles básicos de ciberseguridad de las diputaciones
DATOS DEL PRESENTADOR Nombre: MYRIAM VITON GARCIA NIF / CIF: E-mail: Entidad: DIPUTACIÓ PROVINCIAL DE VALÈNCIA	
FIRMA DIGITAL 68186F9F3DA3C6386CB49E6BD1CAF3AC4A76B050	
DOCUMENTOS ENVIADOS Fichero1: 25418608C_2022114_cl_Certificado convocatoria.pdf Fichero2: 25418608C_2022114_cl_alegacion firmada.pdf	

Muy Sr. Mío:

Habiendo tenido entrada en el Registro de la Diputación de València el pasado 27 de diciembre de 2021 el borrador del Informe realizado por la Sindicatura de Cuentas de los controles básicos de ciberseguridad de la Diputación de Valencia, ejercicio 2021 otorgando plazo de alegaciones a esta misma Diputación hasta el 17 de enero de 2022, se adjuntan las correspondientes alegaciones previo a la emisión del Informe Definitivo.

Estimat senyor:

Havent tingut entrada en el Registre de la Diputació de València el passat 27 de desembre de 2021 l'esborrany de l'Informe realitzat per la Sindicatura de Comptes dels controls bàsics de ciberseguretat de la Diputació de València, exercici 2021 atorgant termini d'al·legacions a aquesta mateixa Diputació fins al 17 de gener de 2022, s'adjunten les corresponents al·legacions previ a l'emissió de l'Informe Definitiu.

SÍNDIC MAJOR

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

VICENT CUCARELLA TORMO

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica

Alegaciones que se formulan al borrador del Informe de Auditoría de los controles básicos de ciberseguridad de la Diputación de Valencia, ejercicio 2021

Primera alegación (y única) al texto:

- Apartado 4 CONCLUSIONES del borrador del Informe, página 8, párrafo "*La Diputación de Valencia no tiene establecida una adecuada gobernanza de la ciberseguridad y debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información"*

- Apartado "Indicadores" del Apéndice 2: Situación de los controles básicos de Ciberseguridad del CBCS 8. CUMPLIMIENTO NORMATIVO Y GOBERNANZA DE CIBERSEGURIDAD, página 43, párrafo *"Del mismo modo, hemos verificado que ninguno de los recursos existentes en el Servicio de Informática dispone de dedicación completa a la seguridad de la información, dado que su dedicación es compartida entre múltiples competencias. Esta carencia de roles con dedicación exclusiva impide que el conjunto de acciones y medidas implantados puedan constituirse como procesos de ejecución continua y sean percibidos como acciones puntuales, dificultando el establecimiento de un SGSI efectivo"*

Contenido de la alegación:

Aún siendo conscientes los órganos de gobierno de la Diputación de Valencia de que se hace necesario establecer una adecuada gobernanza de la ciberseguridad en esta institución y dedicar los recursos necesarios para ello, sin embargo, en cuanto a los recursos asignados al departamento de TI y a la seguridad de los sistemas de Información sí se ha intentado evolucionar los recursos humanos del año 2020 al año 2021, incrementando de dos a tres el número de personas dedicadas a la seguridad de los sistemas de información, aunque hasta el momento no haya sido posible cubrir ese puesto de trabajo tal y como se detalla a continuación:

En el pleno extraordinario de la Diputación de 30 de diciembre de 2019 se creó un puesto nuevo de TÉCNICO SUPERIOR DE SEGURIDAD clasificado como A1 20 A3 con las siguientes funciones a realizar:

- Participar y liderar proyectos de análisis, diseño, desarrollo e implantación de plataformas y herramientas de seguridad de sistemas y redes, junto con el personal del servicio de Informática implicado en estas mismas labores.
- Coordinar al Servicio de Informática con la Delegación de Protección de Datos y con los organismos o servicios externos que auditan o supervisan la seguridad TIC, para la resolución de las incidencias relacionadas con la seguridad.
- Liderar la aplicación de las normativas de seguridad y la definición de los procedimientos de seguridad internos en las infraestructuras informáticas de la corporación.

- Colaborar en las auditorías de seguridad que periódicamente evalúan los sistemas informáticos de la Diputación de Valencia.

No obstante, si bien la finalidad con la creación de este nuevo puesto era pasar de tener 2 personas dedicadas en el año 2020 a tener 3 personas dedicadas en el año 2021 (adicional a un recurso externo contratado), no ha sido posible cubrir esta vacante por causas que se quedan fuera del alcance de la organización.

Se publicó la convocatoria para cubrir este nuevo puesto en Comisión de Servicios durante el año 2020 (expediente 11227/20/PER) pero no se presentaron candidatos. Posteriormente, en el pleno de la Diputación de 16 de febrero de 2021 se modifica su clasificación a A1 20 C1, mejorando las condiciones retributivas respecto del puesto creado inicialmente. Volvió a publicarse la convocatoria para cubrirlo en Comisión de Servicios durante el ejercicio 2021 (expediente 1696/21/PER), presentándose un único candidato que no cubría el perfil, por lo que se declaró desierta.

Así pues, se quiere enfatizar que teniendo presente la importancia que tiene la Seguridad de Información para nuestra organización y pese a no disponer de todos los recursos humanos para una mejor gestión de la misma, se han continuado realizando nuevas actuaciones encaminadas a mejorar la Seguridad Informática, siendo ello posible debido a la gran implicación del personal ya dedicado a ello.

Documentación justificativa de la alegación (se adjunta):

- Certificado del Jefe de Servicio de Gestión y Desarrollo de los Recursos Humanos de la Diputación de Valencia.

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica

ANNEX II

Informe sobre les al·legacions presentades

ANÀLISI DE LES AL·LEGACIONS EFECTUADES PER LA DIPUTACIÓ DE VALÈNCIA A L'ESBORRANY DE L'INFORME D'AUDITORIA DE CIBERSEGURETAT DE L'EXERCICI 2021

Per mitjà d'un escrit de la Sindicatura de 27 de desembre de 2021 es va remetre a la Diputació de València l'esborrany de l'Informe d'auditoria, perquè hi efectuara les al·legacions que considerara oportunes. Amb data 14 de gener de 2022 es van rebre pel registre electrònic les al·legacions formulades, respecte de les quals s'assenyala el que segueix:

Única al·legació

Apartat 4, "Conclusions", de l'esborrany de l'Informe, segon subapartat

"La Diputació de València no té establida una adequada governança de la ciberseguretat i ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació."

Apartat "Indicadors" del "CBCS 8. Compliment normatiu i governança de ciberseguretat" de l'apèndix 2, "Situació dels controls bàsics de ciberseguretat", pàgina 43, segon paràgraf

"De la mateixa manera, hem verificat que cap dels recursos existents en el Servei d'Informàtica disposa de dedicació completa a la seguretat de la informació, atés que la seua dedicació és compartida entre múltiples competències. Aquesta falta de rols amb dedicació exclusiva impedeix que el conjunt d'accions i mesures implantades puguen constituir-se com a processos d'execució contínua i siguen percebuts com a accions puntuals, cosa que dificulta l'establiment d'un SGSI efectiu."

Comentaris

En l'al·legació s'indica que la Diputació és conscient de la necessitat d'"establir una adequada governança de la ciberseguretat en aquesta institució i dedicar-hi els recursos necessaris".

No obstant això, en l'al·legació s'assenyala que sí que s'han intentat millorar els recursos humans de l'any 2020 a l'any 2021, incrementant de dos a tres el nombre de persones dedicades a la seguretat dels sistemes d'informació assignades al departament de TI i a la seguretat dels sistemes d'informació. Aquest compromís s'ha materialitzat per mitjà de la creació d'un nou lloc de tècnic superior de seguretat, però "no ha sigut possible cobrir aquesta vacant per causes que queden fora de l'abast de l'organització".

En la realització de l'auditoria hem pogut comprovar que, en l'actualitat, efectivament el departament de TI disposa de recursos personals la dedicació dels quals a les tasques relacionades amb la seguretat de la informació suposen, en conjunt, un esforç aproximat equivalent a dues persones. També hem comprovat que en 2019 es va crear el lloc de

"tècnic superior de seguretat" amb dedicació plena a aquesta matèria. Però la realitat és que en la data d'aquest informe el lloc segueix sense estar cobert.

Considerem, per consegüent, que l'al·legació presentada no comporta una modificació en el contingut de l'informe. La creació del nou lloc de "tècnic superior de seguretat" suposa una actuació encertada, però la cobertura i la dotació efectiva de responsabilitats d'aquest lloc constitueixen un requisit imprescindible per a aconseguir els nivells requerits quant a governança de la seguretat i recursos humans necessaris.

Conseqüències en l'Informe

No es modifica.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe auditoria CBCS Diputació de València 2021 val - SEFYCU 3048322

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

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

Código Seguro de Verificación (CSV): KUAA R2VZ C7XX YKFU Z3TN

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

Resumen de firmas y/o sellos electrónicos de este documento

Huella del documento para el firmante	Texto de la firma	Datos adicionales de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrónica - ACCV - 08/02/2022 7:36 VICENT CUCARELLA TORMO