

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

**INFORME D'AUDITORIA DELS CONTROLS
BÀSICS DE CIBERSEGURETAT
DE LA DIPUTACIÓ D'ALACANT**

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

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

Conclusions

L'índex de maduresa general dels CBCS mostra un valor del 70,2%, que està prop de l'objectiu del 80%, tot i que encara ha de millorar. En quatre dels huit CBCS analitzats hi ha un índex de compliment del 100%, però n'hi ha altres en què existeixen clares possibilitats de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació. Per a esmenar les principals deficiències detectades s'han realitzat les recomanacions pertinents.

Hem pogut verificar que la Diputació d'Alacant té establida una adequada governança de la ciberseguretat. Els òrgans superiors de la Diputació, com a responsables del sistema de control, han de mantindre el nivell de compromís i suport actual 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 nivell raonable d'adequació a les normes legals. No obstant això, l'informe assenjala diversos aspectes pendents de millora sobre els quals s'ha d'actuar per a una ràpida esmena. En matèria de protecció de dades personals s'han de finalitzar les avaluacions d'impacte dels riscos detectats de nivell alt, que estaven en curs en el moment de l'auditoria, i respecte de l'Esquema Nacional de Seguretat cal esmenar les no conformitats identificades en l'auditoria de compliment realitzada, de manera que li permeta obtindre la certificació de conformitat i el distintiu corresponent per a la seua publicació en la seua electrònica.



També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a l'esmena de les deficiències observades i a la millora dels procediments de gestió de la ciberseguretat de la Diputació, entre les quals aconsellem actualitzar i completar el procediment de seguretat existent per a la identificació i solució de vulnerabilitats (CBCS 3) i el procediment de configuració segura dels sistemes, de manera que considere la seguretat per defecte i el criteri de mínima funcionalitat (CBCS 5). També recomanem que s'aprove formalment un procediment per al tractament dels registres d'auditoria de l'activitat dels usuaris (CBCS 6) i que s'actualitze i es complete el procediment de còpies de seguretat (CBCS7).

NOTA

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



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

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	11
Apèndix 2. Situació dels controls bàsics de ciberseguretat	27
Apèndix 3. Bones pràctiques destacables	37
Acrònims i glossari de termes	40
Tràmit d'al·legacions	42
Aprovació de l'Informe	43



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, inclòs el control intern, dels ajuntaments amb població superior a 50.000 habitants i les tres diputacions", un dels apartats del qual es refereix als controls bàsics de ciberseguretat, en el qual s'integraran de manera sintètica els resultats reflectits en aquest informe.

La necessitat d'una ciberhigiene adequada

Els sistemes d'informació actuals que donen suport a tota la gestió pública, complexos i interconnectats, "estan exposats de forma cada vegada més intensa a la materialització d'amenaques 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.

Adicionalment, la crisi provocada per l'epidèmia de COVID-19 i les mesures tecnològiques adoptades per les administracions públiques han posat de manifest amb absoluta claredat la total dependència de l'Administració pel que fa als 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 pot entendre's 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 fonamental² 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'Esquema Nacional de Seguretat (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 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:³ confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.

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

³ Vegeu l'annex I del Reial Decret 3/2010, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.



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 i proporcionar una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control. 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 controls bàsics de ciberseguretat en relació amb les aplicacions i sistemes que suporten el procés comptable-pressupostari 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 restringits 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 detecte sempre un incompliment significatiu quan existisca.

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

4. CONCLUSIONS

L'índex de maduresa general dels controls bàsics de ciberseguretat és pròxim a l'objectiu, si bé encara ha de millorar

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls bàsics de ciberseguretat aconseguix un **índex de maduresa general del 70,2%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls



parcialment establits o no formalitzats documentalment. Els resultats detallats obtinguts per a cada un dels CBCS es mostren en el quadre 1.

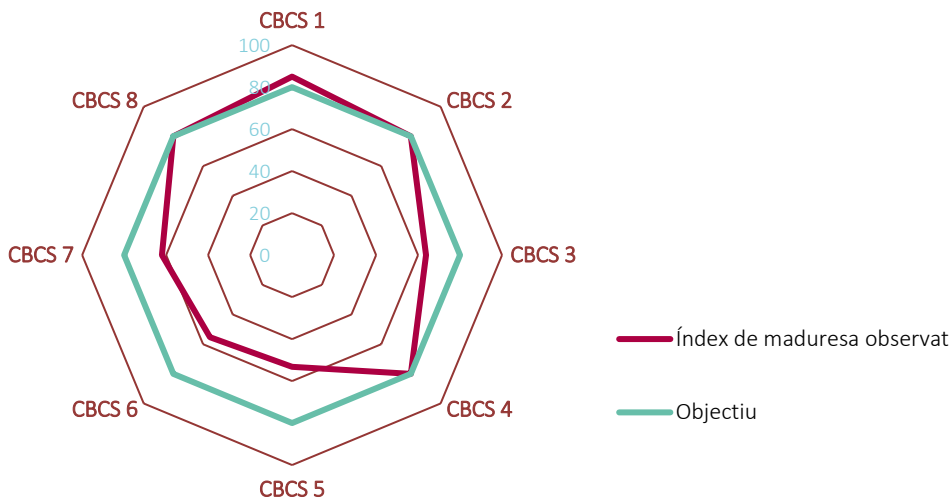
Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

Control	Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1 Inventari i control de dispositius físics	85,0%	N3	100,0%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	80,0%	N3	100,0%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	63,8%	N2	79,7%
CBCS 4 Ús controlat de privilegis administratius	82,0%	N3	100,0%
CBCS 5 Configuracions segures del programari i maquinari	53,2%	N2	66,5%
CBCS 6 Registre de l'activitat dels usuaris	55,3%	N2	69,1%
CBCS 7 Còpies de seguretat de dades i sistemes	62,0%	N2	77,5%
CBCS 8 Compliment normatiu i governança de ciberseguretat	80,0%	N3	100,0%
General	70,2%	N2	86,6%

L'índex de compliment dels CBCS és del 86,6%, que resulta de comparar l'indicador de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80% o *N3, procés definit*.

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





Per tant, encara que l'índex de maduresa general és pròxim a l'objectiu del 80% i existeix un índex de compliment del 100% en quatre dels CBCS, hi ha uns altres CBCS en què hi ha clares possibilitats de millora per a aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació. En l'apartat 6 es realitzen les recomanacions pertinents amb aquesta finalitat.

La Diputació d'Alacant té establida una governança adequada de la ciberseguretat i ha de mantindre el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació

Els òrgans superiors de 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.

Durant l'auditoria hem pogut verificar l'existència d'aquesta implicació i compromís amb la ciberseguretat per part dels òrgans superiors de la Diputació, la qual cosa, juntament amb l'existència d'uns processos de gestió adequats, ens permet afirmar que la governança de ciberseguretat aconsegueix un nivell satisfactori. Els aspectes fonamentals identificats que sustenten aquesta afirmació són:

- La participació activa de l'alta direcció en la gestió de la seguretat de la informació i en els processos establits per a gestió de riscos.
- El compromís amb la gestió i el compliment de requisits legals fonamentals relacionats amb la seguretat de la informació.
- L'assignació de recursos humans i d'inversions que permeten donar compliment als objectius estratègics en matèria de seguretat, incloent-hi el desenvolupament de projectes i la implantació de sistemes que han contribuït decisivament a l'establiment de controls organitzatius i tècnics amb un nivell de maduresa raonable, sense perjudici de les millores encara necessàries.

Els òrgans superiors de la Diputació han de mantindre l'actual nivell de compromís i suport amb la seguretat de la informació, a fi de consolidar els nivells de maduresa dels controls i solucionar les deficiències identificades.

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

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



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

Per a esmenar les deficiències de control observades, 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) i sobre el programari autoritzat (CBCS 2)

1. Actualitzar la normativa i procediments de seguretat existents de manera que representen amb fidelitat el conjunt de mesures ja implantades per al control dels dispositius físics i el programari autoritzat.
2. Identificar i actualitzar tots els sistemes que es troben fora del període de suport.

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

3. Modificar el procediment actual o aprovar un procediment de seguretat específic per a la identificació i la solució de vulnerabilitats que reculli les accions que actualment es realitzen i incloga addicionalment:
 - La prioritització basada en l'anàlisi de riscos per a resoldre'ls.
 - La realització de proves de penetració.
 - L'ús de l'eina de gestió de fluxos de treball, que ja està disponible en l'entitat, per a donar suport a les tasques que es realitzen actualment en la identificació i solució de vulnerabilitats.

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

4. 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 i que detalle les mesures actualment implantades.

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

5. Actualitzar i millorar l'actual procediment de 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, particularment dels sistemes crítics de l'entitat. Aquest procediment ha d'incloure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, 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)

6. Aprovar formalment un procediment 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 la seua revisió. Perquè la revisió dels *logs* es realitze de manera eficaç i eficient, és aconsellable centralitzar-los en sistemes dedicats a aquesta finalitat.

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

7. Encara que hi ha un procediment de còpies aprovat, hi ha diversos aspectes que cal millorar, en particular:
 - La revisió i actualització del procediment actual, detallant adequadament el control implantat i incloent-hi l'ús d'eines de control de tasques o fluxos de treball.
 - L'execució d'un pla de proves periòdiques de recuperació.
 - La implantació efectiva de les mesures addicionals que actualment estan en fase de planificació i la seua formalització en el procediment existent.

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

Encara que el grau de compliment és elevat, hi ha diversos aspectes sobre els quals la Diputació ha d'actuar per a esmenar-los:

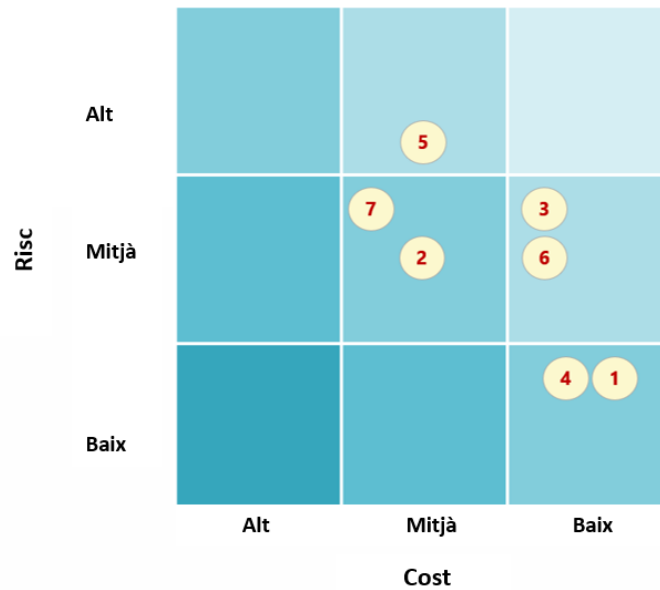
8. Per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat, la Diputació ha d'atendre i solucionar les no conformitats de nivell MAJOR identificades en l'auditoria de compliment realitzada, que li permetrà obtindre la certificació de conformitat i el distintiu corresponent per a fer-ne la publicació en la seua electrònica.
9. En relació amb la protecció de dades personals, la Diputació ha d'aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 del Reglament General de Protecció de Dades, solucionar les no conformitats identificades en les auditories realitzades i finalitzar les avaluacions d'impacte dels riscos detectats de nivell alt.
10. 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 següent es mostra la classificació de les recomanacions segons els criteris combinats de risc potencial que cal mitigar i cost d'implantar-les. No s'hi inclouen els punts 8 a 10 anteriors, ja que són mesures de compliment obligat.

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





APÈNDIX 1

Metodologia aplicada



Introducció

Cada vegada un major nombre d'aspectes de la gestió pública es realitzen amb el suport de complexos sistemes informatitzats, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de 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 mateixa operatòria, per la qual cosa han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat, que és de compliment obligat.

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 INES⁴ del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs 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.

⁴ 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 disseny⁵ com sobre la seua eficàcia operativa⁶ per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport, 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 al 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 els controls que tenen implantats. En aquest cas no s'han revisat els sistemes que sustenten la gestió tributària i recaptatòria, sistemes sí inclosos en el treball realitzat en les altres dues diputacions, ja que aquesta gestió és assumida per l'organisme autònom SUMA.

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

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



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

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

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls 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 siguin 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'obtenir una seguretat limitada sobre la situació dels CBCS revisats.

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

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 establert per la prestigiosa organització Center for Internet Security (CIS),⁷ que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. El seu principal avantatge és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los el màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant ciberatacs al voltant del 85%. Si s'implementen els vint controls el risc es pot reduir un 94%.

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

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

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



Quadre 2. 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	op.exp.2 op.exp.4
CBCS 4 Ús controlat de privilegis administratius	op.acc.4 op.acc.5
CBCS 5 Configuracions segures del programari i maquinari	op.exp.2 op.exp.3
CBCS 6 Registre de l'activitat dels usuaris	op.exp.8 op.exp.10
CBCS 7 Còpies de seguretat de dades i sistemes	mp.info.9
CBCS 8 Compliment normatiu i governança de la ciberseguretat	

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

Els CBCS com a mesures de ciberhigiene

L'European Union Agency for Cybersecurity (ENISA) assenyala⁸ que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen" i reduir els ciberriscos.⁹

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

En aquesta direcció, ENISA estableix deu punts d'acció per a una adequada ciberhigiene. Com s'observa en el quadre 3, dels set CBCS, sense comptar el de compliment normatiu, cinc són coincidents amb els punts d'acció prioritaris recomanats per ENISA com a bones pràctiques de ciberhigiene.

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

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

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



Quadre 3. 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 4. Els CBCS i els seus subcontrols**

Control	Objectiu del control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots els dispositius de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats	L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
		CBCS 1-2: Control d'actius físics no autoritzats	L'entitat disposa de mesures de seguretat per a controlar (detectar i restringir) l'accés de dispositius físics no autoritzats.
CBCS 2 Inventari i control de programari autoritzat	Gestionar activament tot el programari en els sistemes, de manera que només es puga instal·lar i executar programari autoritzat.	CBCS 2-1: Inventari de programari autoritzat	L'entitat disposa d'un inventari de programari complet, actualitzat i detallat.
		CBCS 2-2: Programari suportat pel fabricant	El programari utilitzat per l'entitat té suport del fabricant. En cas contrari, es marca en l'inventari com fora de suport.
		CBCS 2-3: Control de programari no autoritzat	L'entitat disposa de mecanismes que impedeixen la instal·lació i execució de programari no autoritzat.
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per a obtenir informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats	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'exploració de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6 Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels logs d'auditoria)	Recollir, gestionar i analitzar logs d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de logs d'auditoria	El log d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
		CBCS 6-2: Emmagatzematge de logs: Retenció i protecció	Els logs es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la 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 es revisen 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 (sistema de gestió d'incidències i informació de seguretat) o una eina d'anàlisi de logs per a realitzar correlació i anàlisi de logs.
CBCS 7 Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú.	CBCS 7-1: Realització de còpies de seguretat	L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema.
		CBCS 7-2: Realització de proves de recuperació	Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmeses a través de la xarxa.
CBCS 8 Compliment normatiu i governança de ciberseguretat	L'entitat compleix els requisits legals i reglamentaris que li són aplicables i té establida una adequada governança de ciberseguretat.	CBCS 8-1: Compliment de l'ENS	L'entitat compleix els requeriments establits en l'ENS.
		CBCS 8-2: Compliment de la LOPD/RGPD	L'entitat compleix els requeriments establits en la LOPD/RGPD.
		CBCS 8-3: Compliment de la Llei 25/2013	L'entitat compleix els requeriments establits en la Llei 25/2013, de 27 de desembre.



Avaluació dels resultats del treball

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

Subcontrols

Els CBCS són controls globals compostos per diversos controls detallats o subcontrols (tal com es pot veure en el quadre 4 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 5. Avaluació dels subcontrols

Avaluació	Descripció
Control efectiu	<p>Cobreix al 100% amb l'objectiu de control i:</p> <ul style="list-style-type: none">- El procediment està formalitzat (documentat i aprovat) i actualitzat.- El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	<p>A grans trets, compleix l'objectiu de control, si bé pot haver-hi uns certs aspectes no coberts al 100% i:</p> <ul style="list-style-type: none">- Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.).- Les proves realitzades per a verificar la implementació són satisfactòries.- S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	<p>Cobreix de manera molt limitada l'objectiu de control i:</p> <ul style="list-style-type: none">- Se segueix un procediment, encara que aquest pot no estar formalitzat.- El resultat de les proves d'implementació i d'eficàcia no és satisfactori. <p>Cobreix en línies generals l'objectiu de control, però:</p> <ul style="list-style-type: none">- No se segueix un procediment clar.- Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	<p>No cobreix l'objectiu de control.</p> <p>El disseny cobreix l'objectiu de control, però el resultat de la revisió realitzada posa de manifest que la implementació o l'eficàcia operativa del control no són satisfactòries (s'han detectat incompliments significatius i generalitzats).</p>



Controls

Per a determinar la situació global de cada control de ciberseguretat hem utilitzat el **model de nivell de maduresa** dels processos de control d'acord amb el que s'estableix en 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 6. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El control no s'està aplicant en aquest moment.
N1 Inicial / ad hoc	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. <i>L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depèn de la competència i bona voluntat de les persones i és difícil preveure la reacció davant una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depèn de tindre personal d'alta qualitat.</i>
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. <i>L'eficàcia del procés depèn de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta quan es repeteixen les mateixes circumstàncies. És impredecible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.</i>
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. <i>Es disposa d'un catàleg de processos que es manté actualitzat. Aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant 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 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.</i>
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. <i>Es disposa d'un sistema de mesures i mètriques per a conèixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura. En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.</i>



Nivell	Índex	Descripció
N5 Optimitzat	100	<p>Se segueixen bones pràctiques en un cicle de millora contínua.</p> <p><i>El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.</i></p> <p><i>S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, i s'utilitzen com a indicadors en la gestió de la millora dels processos.</i></p> <p><i>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.</i></p>

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:

- Aconseguir els seus objectius.
- Protegir els actius al seu càrrec.
- Complir les seues obligacions diàries de servei.
- Respectar la legalitat vigent.
- 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:

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

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

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

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

¹¹ *Guía de seguridad de las TIC. CCN-STIC 824. Informe Nacional de l'Estat de Seguretat dels Sistemes TIC.*



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

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

Indicadors globals

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

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

Governança de ciberseguretat

A l'efecte d'aquest treball, s'entendrà per governança de la seguretat de la informació i les comunicacions o de ciberseguretat (termes que utilitzem de manera indistinta en aquest informe) el conjunt de responsabilitats i activitats realitzades per l'alta direcció amb l'objectiu de proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una manera responsable.¹²

Els principals elements d'una 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 els processos de gestió per a garantir que les estratègies i programes de seguretat de la informació estiguen alineats amb els objectius de l'entitat. 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. 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

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



l'execució de les activitats establides per l'alta direcció correspon als gestors, a la direcció executiva.

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 informació¹⁴ 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 capacitat.

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.

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.



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

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.

Atés que la informació utilitzada en l'auditoria té un caràcter sensible i pot afectar la seguretat dels sistemes d'informació, els resultats amb el màxim detall de cada un dels controls revisats només es comuniquen amb caràcter confidencial als responsables de 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 en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.

Situació del control

La Diputació realitza diverses accions efectives per a mantindre actualitzat l'inventari d'actius físics i controlar les connexions de dispositius a la xarxa corporativa. La responsabilitat de l'inventari de dispositius s'estableix en la normativa de seguretat, que ha sigut formalment aprovada.

Els actius de l'entitat estan inventariats per mitjà de diverses eines. Els equips d'usuari són gestionats amb una eina que detecta automàticament els equips amb agent instal·lat. Per a la resta d'actius, que per la seua naturalesa no permeten instal·lació d'agent, es disposa de diferents eines per a l'inventari automatitzat dels elements. Hem verificat que la configuració de les diferents eines garanteix que els inventaris existents es troben actualitzats. A més, hem verificat que existeix un adequat procés de gestió i aprovació de nous actius i de retirada o substitució d'actius existents.

Quant a les mesures que constitueixen el control, aquestes es troben detallades en diverses guies i procediments operatius i administratius, però aquests documents no es troben totalment actualitzats i els falta l'aprovació formal.

Per al control d'accés de dispositius a la xarxa corporativa, la Diputació ha implantat mesures tecnològiques adequades i eficaces, que permeten assegurar que tots els actius connectats a la xarxa corporativa es troben controlats i autoritzats.

Hi ha un control raonable sobre l'inventari i el control d'actius físics, i la seua valoració global aconsegueix un **índex de maduresa del 85,0%**, que es correspon amb un **nivell de maduresa N3, procés definit**; és a dir, els processos estan estandarditzats i formalment documentats. Això representa un **índex de compliment del CBCS 1 del 100,0%**.

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 hi ha implantat un procés adequat, que ha sigut parcialment recollit en un document de bones pràctiques TIC i en el procediment de seguretat associat, que ha sigut formalment aprovat. No obstant això, aquests procediments es troben desactualitzats i no representen amb total fidelitat el control implantat.

La major part de les aplicacions que proporcionen suport als processos essencials es troben virtualitzades, de manera que el seu inventari i control està centralitzat en l'eina de gestió d'aplicacions virtualitzades.

Per a aquelles aplicacions instal·lades directament en els equips d'usuari, l'inventari de programari es manté actualitzat automàticament per mitjà de l'ús de la mateixa eina que gestiona l'inventari de dispositius físics amb agent i que relaciona els dos inventaris. L'inventari inclou el programari instal·lat, la versió, el nombre de llicències disponibles i nombre de llicències instal·lades, entre altra informació.

L'entitat disposa d'un pla de manteniment detallat i realitza una gestió efectiva de manteniments, contractes i llicències. Encara que s'ha detectat l'existència d'un determinat nombre d'equips amb programari fora del període de suport del fabricant, aquest nombre és molt reduït respecte del total i suposa un risc limitat. Segons ens han informat, la seua permanència respon a necessitats operatives, atés que hi ha determinades aplicacions que únicament són compatibles amb aquest programari.

L'entitat compta amb determinades mesures per a impedir l'ús de programari no autoritzat que considerem efectives.

Existeix un nivell raonable de control sobre l'inventari i control de programari autoritzat, que aconsegueix un **índex de maduresa del 80,0%**, que es correspon amb un **nivell de maduresa N3, procés definit**; és a dir, els processos estan estandarditzats i formalment documentats. Això representa un **índex de compliment del CBCS 2 del 100,0%**.

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

Objectiu del control

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

Situació del control

Hem analitzat les accions dutes a terme per la Diputació per a la gestió de vulnerabilitats i hem observat que aquestes accions formen part d'un procés que es troba parcialment recollit en un procediment formalment aprovat.



La identificació i solució de vulnerabilitats la realitza el personal del servei d'informàtica, si bé es disposa de contractes amb proveïdors que proporcionen suport per a determinades tasques relatives a l'actualització dels sistemes.

La Diputació utilitza diversos mitjans per a la identificació de vulnerabilitats, com la subscripció a comunicacions de fabricant o organismes de referència o l'ús d'eines específiques per a la detecció de vulnerabilitats. Les vulnerabilitats són prioritzades i resoltes per mitjà d'un procés informal que no es troba inclòs en el procediment existent. El procés complet no es troba suportat per una eina de gestió de fluxos de treball que en facilite la gestió.

A més, es disposa de controls avançats per a previndre atacs per mitjà de sistemes de prevenció d'intrusions habilitats en diversos punts de la xarxa de l'entitat, que considerem adequadament dissenyats i gestionats, i permeten compensar possibles vulnerabilitats no identificades o resoltes en els sistemes de l'organització.

L'aplicació de pedaços i actualitzacions es realitza en general de manera automatitzada per mitjà de diverses eines de gestió centralitzada, en el cas d'aquells sistemes amb nombrosos actius. Per a l'actualització de sistemes que suporten processos crítics de l'entitat, les actualitzacions es realitzen de manera manual i inclouen la realització de proves en entorns de preproducció prèviament al seu desplegament.

Hi ha un cert nivell de control sobre la gestió de vulnerabilitats, i la valoració global del control aconseguix un **índex de maduresa del 63,8%**, que 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 han sigut formalitzats documentalment. Això representa un **índex de compliment del CBCS 3 del 79,7%**.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

Hem analitzat la gestió realitzada per la Diputació dels comptes amb privilegis d'administració en els diferents sistemes i hem verificat que existeix un control efectiu d'aquests comptes, però únicament determinades accions del procés es troben recollides en un procediment aprovat.

S'ha confirmat l'existència d'usuaris administradors únicament nominatius en els sistemes revisats i l'assignació d'aquests privilegis només a usuaris que ho requereixen, fent una adequada aplicació del principi de mínim privilegi. Addicionalment, hem verificat l'existència de diversos processos de revisió i control d'usuaris i privilegis, que són efectius i permeten garantir l'eficàcia del control.



S'ha confirmat l'existència d'identificadors diferenciats per a un mateix usuari, depenent del tipus de tasca a exercir en el sistema, a fi de limitar l'ús d'identificadors amb privilegis administratius a les tasques que no en requereixen.

S'han establert formalment els requisits d'autenticació en una política de contrasenyes, que s'ha implementat adequadament en els sistemes Windows i en aquells que han implementat SSO (*single-sign-on*) amb el directori actiu, fet que ha proporcionat una política d'autenticació homogènia en tots els sistemes revisats.

Hi ha un nivell raonable de control sobre els comptes amb privilegis administratius, per la qual cosa la valoració global del control existent aconseguix un **índex de maduresa del 82,0%**, que es correspon amb un **nivell de maduresa N3, procés definit**; és a dir, els processos estan estandarditzats i formalment documentats. Això representa un **índex de compliment d'aquest CBCS 4 del 100,0%**.

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 de l'entitat per a la configuració segura dels sistemes i hem observat que no es troben completament recollides en el procediment aprovat existent, que no té el detall necessari. A més, l'aplicació d'aquestes accions no es gestiona ni revisa, de manera que l'efectivitat del control és dependent del personal i de la seua elevada capacitat tècnica.

Hem verificat que s'han establert configuracions i que es disposa de plantilles per a la configuració de determinats sistemes que, si bé no tenen com a únic objecte la seguretat, sí que tenen en consideració les recomanacions quant a la seguretat dels fabricants, d'organismes de referència i de serveis específics de suport i revisió.

D'altra banda, l'entitat disposa d'un entorn de preproducció utilitzat per a la gestió de canvis i per a la realització de proves de seguretat en determinats sistemes crítics.

Sobre el monitoratge de les configuracions existents, hem verificat que s'han establert 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 el control de configuracions segures és que l'organització aconseguix un **índex de maduresa del 53,2%**, que es correspon amb un



nivell de maduresa N2, repetible però intuïtiu; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 5 del 66,5%**.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

Hem analitzat els procediments aplicats per la Diputació per al registre de l'activitat dels usuaris en els diferents sistemes i hem verificat que, encara que es disposa d'uns certs procediments relacionats amb aquest control, aquests no són complets i no han sigut documentats formalment.

Hem verificat que el registre d'activitat es troba activat en els sistemes revisats, que són emmagatzemats localment per cada sistema, i disposen d'una configuració específica quant a temps de retenció que és aplicada en cada sistema en funció de la seua criticitat.

Adicionalment, la Diputació disposa d'una eina per a la gestió centralitzada de registres d'activitat de determinats actius que facilita la seua gestió i revisió. No obstant això, aquesta eina no integra tots els sistemes rellevants des del punt de vista de la ciberseguretat i la revisió d'aquests registres d'activitat es realitza de manera informal, no procedimentada.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 55,3%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu;** és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 6 del 64,7%**.

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, encara que aquestes no es troben completament recollides en el procediment aprovat. Les polítiques de còpia aplicades s'han desenvolupat d'acord amb les necessitats identificades pel departament TIC. Adicionalment, per a determinats processos crítics de



l'entitat, s'ha realitzat una anàlisi de requisits conjunta amb els responsables funcionals d'aquests processos.

Hem verificat que la gestió i control de còpies 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. Aquest fet no implica necessàriament una aplicació incorrecta del control de còpies, però sí que impedeix garantir-ne l'eficàcia en tots els casos.

Els procediments actuals inclouen diferents mecanismes efectius destinats a la protecció de les còpies de seguretat, si bé és necessària l'aplicació de mesures addicionals per a augmentar la protecció davant de determinats riscos als quals es troben exposats els sistemes d'informació. En aquest sentit, la Diputació no disposa d'una ubicació redundat per a les còpies realitzades en format disc, que s'emmagatzemen en l'únic CPD disponible. L'emmagatzematge en el mateix CPD principal proporciona protecció limitada davant de determinades amenaces, però hi ha altres riscos físics sobre els quals no proporciona la protecció adequada.

Ens han informat durant la realització de l'auditoria que s'ha iniciat un projecte de construcció d'un segon CPD, que cobrirà la insuficiència anteriorment assenyalada.

No es realitzen de manera sistemàtica proves de recuperació planificades, si bé hem confirmat que es realitzen i registren freqüents recuperacions satisfactòries de diversos tipus de còpies per demanda dels usuaris. Addicionalment, es realitzen recuperacions diàries dels sistemes crítics de l'entitat a entorns de preproducció, com a part del procés de gestió de canvis implantat.

La valoració global del control existent sobre les còpies de seguretat és que la Diputació aconsegueix un **índex de maduresa del 62,0%**, que es correspon amb un **nivell de maduresa N2, repetible però intuïtiu**; és a dir, els controls es realitzen, però existeixen controls parcialment establits o els procediments no han sigut formalitzats documentalment. Això representa un **índex de compliment del CBCS 7 del 77,5%**.

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 2012 la presidència 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. Segons ens han informat, s'ha actualitzat i elaborat una nova versió de la Política de Seguretat que es troba pendent d'aprovació.
- S'han designat els responsables previstos en la PSI i s'ha creat el Comité de Seguretat.
- S'ha desenvolupat la normativa associada a la PSI, que inclou aspectes per a l'ús dels sistemes i dispositius, la política d'accés a internet i correu electrònic, etc. Aquest conjunt de documents es va aprovar formalment pel Comité de Seguretat el 12/02/2020.
- En 2013 el Comité de Seguretat va aprovar la Declaració d'Aplicabilitat i el Pla d'Adequació, basats en la categorització d'actius i anàlisis de riscos.
- S'ha formalitzat i remés Informe de l'Estat de la Seguretat (Informe INES).
- S'han realitzat auditories de compliment previstes en l'article 34, en les quals s'han identificat diverses no conformitats de nivell major.

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

- No s'ha implantat la totalitat de les mesures de seguretat i accions previstes en la Declaració d'Aplicabilitat i el Pla d'Adequació.
- No s'han solucionat les no conformitats identificades, per la qual cosa no s'ha certificat el compliment de l'ENS.

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 realitzat el nomenament de delegat de protecció de dades i aquest nomenament s'ha notificat a l'Agència, com exigeix l'RGPD en l'article 37.
- S'ha elaborat un registre d'activitats del tractament, que inclou el detall necessari. A més, aquest registre s'ha publicat i és accessible per mitjans electrònics.
- S'ha realitzat una anàlisi de riscos sobre els tractaments de dades personals conforme a l'article 32.2 de l'RGPD.



- Es va realitzar una auditoria a final de 2019 en matèria de protecció de dades en la qual s'especifiquen les mesures tècniques i organitzatives que s'han adoptat per a donar compliment a les obligacions de la legislació vigent en aquesta matèria i les no conformitats detectades.

No obstant això, no s'han finalitzat les avaluacions d'impacte dels riscos detectats de nivell alt, que estan en curs en el moment de l'auditoria.

Compliment legalitat del registre de factures

Estan pendents de realitzar les auditories del registre de factures de 2019 i 2020 exigides per la Llei 25/2013, de 27 de desembre.

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió és que la Diputació aconsegueix un **índex de maduresa del 80,0%**, que es correspon amb un **nivell de maduresa N3**, que indica que existeix un compliment raonable de la normativa, encara que hi ha aspectes que s'han de millorar.

Governança de ciberseguretat

La Diputació d'Alacant té establida una governança adequada de la seguretat de la informació i un suport raonable de l'alta direcció, incloent-hi una assignació adequada de recursos humans i pressupostaris dedicats a la seguretat de la informació.

Durant el treball de revisió de controls, hem pogut verificar l'existència d'un conjunt de procediments, pràctiques i compromisos amb la ciberseguretat, per part dels responsables implicats i la direcció de l'entitat, que permeten determinar que la governança de ciberseguretat aconsegueix un nivell satisfactori.

Els aspectes fonamentals que s'han identificat són els següents:

- La participació activa de la direcció en l'establiment de polítiques i objectius estratègics de l'entitat, superant pràctiques habituals que solen restringir-se a la mera aprovació o signatura de la documentació associada.
- La definició i nomenament de rols, i la creació d'òrgans de govern de la seguretat de la informació. Hem verificat que existeixen i exerceixen de manera efectiva i continuada les funcions establides.
- La determinació dels requisits legals aplicables. Tal com es detalla en els subapartats anteriors, existeix un raonable nivell de compliment de la legalitat en matèria relacionada amb la seguretat de la informació.
- El compromís i participació activa de l'alta direcció en els processos que tenen com a objectiu el tractament de riscos que amenacen la seguretat dels actius d'informació, i en l'articulació de mesures per a mitigar aquests riscos, aspecte que té gran importància atés el creixement constant dels ciberatacs a les entitats públiques.



APÈNDIX 3

Bones pratiques 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 la normativa (ENS) o en les guies professionals corresponents, que se sintetitzen en el quadre 4 d'aquest informe. En un altre cas, l'entitat ha d'adoptar mesures per a millorar la seua ciberseguretat.

Adicionalment a la valoració dels controls bàsics de ciberseguretat, és convenient destacar determinats aspectes, pràctiques, solucions tècniques o sistemes que s'han identificat o revisat durant la realització de 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.

Desplegament d'un sistema network access control (NAC)

L'entitat ha desplegat un sistema NAC que es troba basat en l'ús del protocol/norma 802.1X en els dispositius d'accés de l'electrònica de xarxa. La solució implantada realitza de manera dinàmica l'autenticació dels dispositius que requereixen accés a la xarxa corporativa i que, en cas d'autenticació positiva, assigna el dispositiu a la subxarxa adequada. La solució es troba integrada amb el directori actiu de l'entitat, fet que facilita la gestió del manteniment



del sistema, atés que únicament es permet l'accés d'aquells actius que pertanguen al domini de la Diputació.

Gestió d'usuaris i comptes d'empleats

Per a abordar aquesta mesura de seguretat bàsica, la Diputació ha implantat aplicacions i activitats que, en conjunt, constitueixen un avançat procés de gestió d'usuaris i comptes d'empleats de l'entitat. El procés complet es troba suportat per la gestió conjunta del Servei d'Informàtica i el Departament de Personal.

Per a la gestió del procés s'utilitzen dues aplicacions de desenvolupament propi, que permeten i faciliten la gestió dels drets d'accés dels usuaris per part dels seus responsables, i automatitzen la relació entre els usuaris del directori actiu (DA) i la informació del Departament de Personal, creant automàticament els usuaris de DA davant noves incorporacions i revisant les situacions administratives dels empleats per a una configuració adequada dels usuaris del DA. A més, s'han establert tasques periòdiques de revisió d'usuaris i privilegis que impedeixen que, davant un error del procés ordinari, s'incomplisquen els principis de seguretat.

Protecció de punt final

La Diputació ha adquirit i implantat una eina de protecció de punt final que disposa d'un conjunt de solucions que proporcionen un elevat nivell de protecció en els equips dels usuaris. El conjunt de solucions, que requereixen un important esforç de configuració i manteniment per a aconseguir els nivells d'efectivitat potencialment disponibles, han sigut adequadament implantades i desenvolupades pel personal de la Diputació, en un projecte que es troba en fase de finalització i l'èxit del qual resideix en una correcta assignació de recursos humans interns per a les tasques de configuració i desplegament.

Gestió de la configuració de privilegis administratius en el directori actiu (DA)

La Diputació realitza una avançada gestió de privilegis d'administració sobre els sistemes Windows i el DA. L'efectivitat de la gestió es basa en una aplicació adequada del principi del mínim privilegi, una eficaç gestió d'usuaris i comptes d'empleats, i una elaborada configuració del DA. La configuració del DA s'ha adoptat d'acord amb les recomanacions del fabricant, en el marc d'un servei contractat per a la posada en operació dels sistemes. Aquesta configuració es basa en la pertinència a grups del domini i en l'assignació dinàmica de permisos d'administració.



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

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.

Governança de ciberseguretat: És el procés d'establir i mantindre un marc de referència, i donar suport a l'estructura i els processos de gestió per a garantir que les estratègies i programes de seguretat de la informació estiguen alineats amb els objectius de l'entitat. A



l'efecte de 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 conèixer-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.

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.

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.

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 d'auditoria es va discutir amb el diputat responsable d'innovació i agenda digital i els responsables corresponents de l'àrea, per al seu coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

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

Transcorregut el termini esmentat no s'han rebut al·legacions.



APROVACIÓ DE L'INFORME

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



Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Informe d'auditoria dels controls bàsics de ciberseguretat de la Diputació d'Alacant_2021_val - SEFYCU 2935270

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 QQY7 VKH2 QYA2 CEDH

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 - 25/11/2021 8:03
VICENT CUCARELLA TORMO