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

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. Això origina un increment dels riscos associats als sistemes d'informació que sustenten els serveis públics i, per tant, a la informació que manegen. De fet, les entitats locals han sigut un dels objectius més afectats per les onades recents de ciberatacs.

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

Conclusions

L'índex de maduresa general dels CBCS mostra un valor del 63,7%, però encara ha de millorar per a aconseguir l'objectiu del 80%. No s'han identificat deficiències greus de control i tots els CBCS analitzats arriben a un nivell de maduresa N2, però n'hi ha 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 té establida una acceptable governança de la ciberseguretat. Els òrgans superiors de la Diputació, com a responsables del sistema de control, han de reforçar 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 assenyala diversos aspectes pendents de millora sobre els quals s'ha d'actuar per a una ràpida esmena. Respecte de l'Esquema Nacional de Seguretat, la Diputació ha de solucionar 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 seu 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 millorar els procediments de seguretat existent per a tots els controls analitzats, implantar solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa (CBCS 1), elaborar i aprovar un pla anual de manteniment i un catàleg d'aplicacions autoritzades (CBCS 2) i l'execució de proves periòdiques de recuperació de còpies de seguretat (CBCS 7).

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 conéixer el veritable abast del treball realitzat.

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

Exercici 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

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

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

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

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

La necessitat d'una adequada ciberhigiene

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

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

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

Addicionalment, la crisi provocada per l'epidèmia de COVID-19 i les mesures tecnològiques adoptades per les administracions públiques han posat de manifest amb absoluta claredat la total dependència de l'Administració 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 es pot entendre la capacitat d'una entitat per a evitar o resistir i recuperar-se d'un ciberatac en un temps raonable per a continuar prestant els seus serveis. La ciberhigiene és un principi fonamental[2] relacionat amb la seguretat de la informació i equival a establir mesures rutinàries senzilles per a minimitzar els riscos de les ciberamenaces. De manera anàloga al que ocorre amb la higiene personal, les bones pràctiques de ciberhigiene poden impulsar una major immunitat en les entitats que les apliquen, la qual cosa redueix el risc davant d'un ciberatac.

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

2. RESPONSABILITATS DELS ÒRGANS SUPERIORS DE LA DIPUTACIÓ EN RELACIÓ AMB ELS CONTROLS DE CIBERSEGURETAT

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

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

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats 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 CBCS en relació amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptatòria i altres sistemes d'interés general.

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

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

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

4. CONCLUSIONS

L'índex de maduresa general dels controls bàsics de ciberseguretat 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 aconsegueix un **índex de maduresa general del 63,7%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o no formalitzats documentalment. Els resultats detallats obtinguts per a cada un dels CBCS es mostren en el quadre 1.

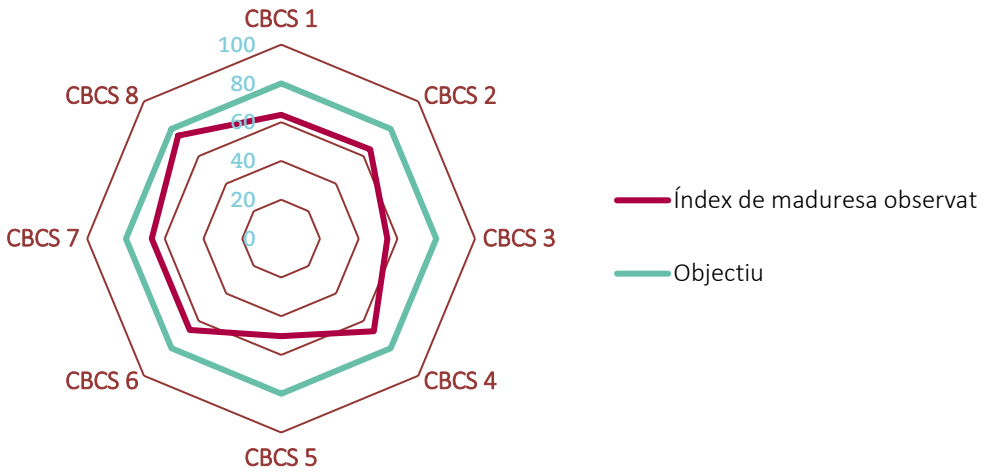
Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

Control	Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1 Inventari i control de dispositius físics	63,8%	N2	79,7%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	65,0%	N2	81,3%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	54,8%	N2	68,4%
CBCS 4 Ús controlat de privilegis administratius	67,5%	N2	84,3%
CBCS 5 Configuracions segures del programari i maquinari	50,3%	N2	62,8%
CBCS 6 Registre de l'activitat dels usuaris	66,7%	N2	83,3%
CBCS 7 Còpies de seguretat de dades i sistemes	66,7%	N2	83,3%
CBCS 8 Compliment normatiu i governança de ciberseguretat	75,0%	N2	93,8%
General	63,7%	N2	79,6%

L'índex de compliment dels CBCS és del 79,6%, 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, si bé no s'han identificat greus deficiències de control i es disposa d'un nivell de maduresa homogeni en tots els aspectes analitzats, 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 nostra auditoria i els indicadors reflecteixen la situació a 30 de setembre de 2021.

La Diputació de Castelló té establida una governança acceptable de la ciberseguretat, però ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació

Els òrgans superiors de la Diputació són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació 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'aquest 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 presenta un nivell acceptable.

No obstant això, els òrgans superiors de la Diputació han de reforçar l'actual nivell de suport i compromís amb la seguretat dels sistemes d'informació, a fi d'aconseguir els nivells de maduresa dels controls requerits per l'ENS i solucionar les deficiències identificades. Amb aquesta finalitat resulta necessari impulsar de manera proactiva iniciatives per a millorar la ciberhigiene i la ciberresiliència.

En aquest sentit, els òrgans de govern tenen responsabilitat no sols en el compliment legal, sinó que han de liderar i ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat. L'existència d'un lideratge recognoscible per tota la corporació pot fomentar els avanços en termes de conscienciació i permetre véncer les naturals resistències que puguen existir en l'organització als canvis necessaris.

D'altra banda, i si bé hem verificat l'alt nivell de compromís dels gestors i responsables de la seguretat, la seua dedicació és compartida entre múltiples competències, atés que cap dels rols existents disposa de dedicació completa a la seguretat de la informació i la protecció de les dades, que considerem indispensable en un ens de la grandària de la Diputació amb els seus complexos sistemes d'informació. Aquesta falta de rols amb dedicació exclusiva impedeix que el conjunt d'accions i mesures implantats puguen constituir-se com a processos d'execució contínua i són percebuts com a accions puntuals, cosa que dificulta l'establiment d'un sistema de gestió de la seguretat de la informació efectiu.

És necessària, per tant, la incorporació de recursos amb dedicació exclusiva a la seguretat o la reassignació de responsabilitats, de manera que siga possible una gestió continuada de les mesures i processos de seguretat.

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

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

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

2. Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa i finalitzar la implantació de mesures compensatòries actualment en fase de desplegament.

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

3. Actualitzar la normativa i procediments de seguretat existents o aprovar procediments específics per al control de programari, de manera que recullen, amplien i representen amb fidelitat el conjunt de mesures ja implantades. Addicionalment, recomanem elaborar un pla anual de manteniment i un catàleg d'aplicacions autoritzades, documents previstos en el procediment aprovat existent.

4. 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)

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

   – La priorització basada en l'anàlisi de riscos per a la seua resolució.

- 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)

6. Modificar i millorar el procediment de gestió d'usuaris i privilegis actualment aprovat, de manera que detalle les accions actualment implantades. D'altra banda, aplicar els principis i mesures detallats en el procediment, en particular els següents:

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

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

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

7. 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 que permeten assegurar l'eficàcia del control. 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 incloure la gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat, en el procediment existent, o desenvolupar un procediment específic. Aquest procediment ha de preveure les mesures actualment implantades en determinats sistemes crítics i el monitoratge i revisió periòdica dels canvis no autoritzats en la resta de sistemes.

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

8. Modificar i millorar el procediment actualment aprovat per al tractament dels registres d'activitat dels usuaris, de manera que detalle les accions actualment implantades. També s'han d'aplicar de manera efectiva els principis i mesures detallats en el procediment, particularment els següents:

   - Establir les mesures necessàries per a complir els períodes de retenció especificats en el procediment vigent.

- Incloure la totalitat de sistemes de l'entitat en les eines de gestió de registres d'activitat disponibles.

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

9. Encara que hi ha un procediment de còpies aprovat, hi ha diversos aspectes que cal millorar, en particular:

   - Ha d'incloure's de forma detallada el control realment implantat i recollir l'ús d'eines de control de tasques o fluxos de treball.

   - L'execució de proves periòdiques de recuperació planificades.

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:

10. 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 la seua publicació en la seu electrònica.

11. En relació amb la protecció de dades personals, la Diputació ha de planificar i executar les auditories de compliment en matèria de protecció de dades i 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 .

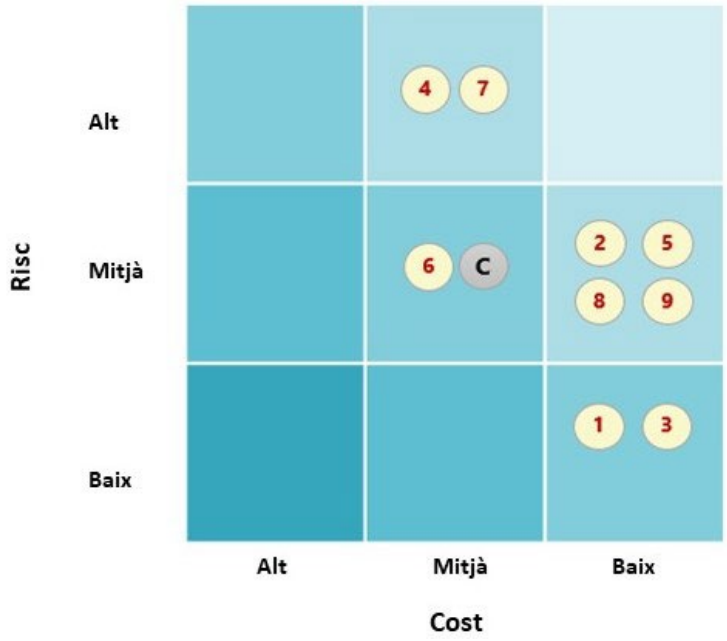
12. En relació amb la Llei de Factura Electrònica, la Diputació ha de realitzar les auditories de sistemes anualment tal com exigeix aquesta norma.

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 a mitigar** i **cost estimat de la seua implantació**. No s'inclouen els punts 10 a 12 anteriors, ja que són mesures d'obligat compliment.

També s'inclou en el gràfic la recomanació pendent d'implementar del nostre informe anterior, amb la referència C, que es comenta en l'apartat següent.

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



Seguiment de recomanacions anteriors

Hem realitzat un seguiment de les recomanacions sobre el control intern de l'Informe sobre auditoria operativa de la gestió i recaptació delegada en les diputacions de la Comunitat Valenciana. Exercici 2016. Tal com es mostra en el quadre següent, de les tres recomanacions realitzades en aquell informe, només una no s'ha atés.

Quadre 2. Seguiment de recomanacions

	Recomanacions sobre els controls generals de tecnologies de la informació de l'informe anterior	Situació a 30 de setembre de 2021	
A	La Diputació ha d'aplicar estrictament els procediments aprovats per a la gestió d'usuaris i drets d'accés, particularment en la gestió de baixes d'usuaris, a fi d'evitar la dependència de controls manuals per part del Departament d'Informàtica. Igualment, recomanem que s'execute periòdicament i segons un procés automatitzat una revisió de l'activitat dels usuaris dels sistemes crítics de la Diputació, a fi d'identificar usuaris incorrectament habilitats i verificar l'assignació correcta de privilegis.	Hem verificat que s'han implantat mesures per a la comunicació automàtica de les baixes per part de personal al Servei d'Informàtica. Aquestes comunicacions són gestionades per a la desactivació d'usuaris en el sistema. Addicionalment, s'han automatitzat anàlisis periòdiques per a la identificació d'usuaris que disposen d'una configuració anòmala de comptes i mecanismes d'autenticació.	**Totalment o substancialment aplicada**
B	Recomanem a la Diputació de Castelló aprovar al més prompte possible un pla de continuïtat de l'activitat i de recuperació davant desastres, documentats per escrit i aprovats formalment per la Direcció. Prèviament serà necessari realitzar una anàlisi de riscos o una anàlisi d'impacte en els serveis prestats per a establir la criticitat i prioritat dels actius de l'entitat (serveis, informació, aplicacions, dispositius de xarxa i servidors, etc.), així com els punts i terminis necessaris per a la recuperació de la informació i els sistemes. La Diputació de Castelló ha iniciat un procés de contractació pública per al projecte de desenvolupament d'aquest pla de continuïtat, que d'acord amb els terminis establits haurà de finalitzar la seua execució en el primer quadrimestre del 2019. Una vegada establit i aprovat el pla de continuïtat, se n'hauran de realitzar proves periòdiques per a verificar que funciona correctament en cas de desastre i deixar documentades aquestes proves.	Hem verificat que el Comité de Seguretat ha aprovat un pla de continuïtat de negoci que recull els aspectes necessaris, incloent-hi la identificació de serveis essencials, les responsabilitats, l'anàlisi de l'impacte, les estratègies de recuperació, les fases del pla de continuïtat i un pla de proves. En el moment de redacció d'aquest informe s'està realitzant la formació als intervinents i gestionant l'execució del pla de proves inclòs en el pla de continuïtat.	**Totalment o substancialment aplicada**
C	La Diputació hauria de configurar polítiques de control d'accessos al sistema Estima perquè s'ajuste a les bones pràctiques generalment acceptades i a les exigències de l'ENS.	Hem constatat que la recomanació està pendent d'aplicació.	**No aplicada**

Actuacions en curs

Encara que no s'han tingut en compte en el càlcul dels indicadors mostrats en l'apartat 4, hem verificat que en el moment de finalització del treball de camp de l'auditoria han sigut iniciades o planificades actuacions en matèria de ciberseguretat en diversos àmbits, que atendrien bona part de les recomanacions anteriors. Aquestes actuacions es troben en la seua majoria recollides en el pla de la Diputació per a la correcció de no conformitats amb l'ENS o s'han iniciat a conseqüència de les observacions realitzades en el transcurs d'aquesta auditoria. La implantació efectiva d'aquestes tindrà un impacte positiu en el nivell de ciberseguretat de l'entitat.

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

- La implantació efectiva d'un pla de continuïtat del negoci (PCN). Aquest pla ha sigut elaborat i aprovat, i en el moment de redacció d'aquest informe s'està realitzant la formació pertinent i gestionant l'execució del pla periòdic de proves inclòs en el PCN.

- La implantació d'un sistema de provisió d'aplicacions i escriptoris virtualitzats en la totalitat de l'organització (vegeu apèndix 3, "Bones pràctiques destacables"). El desplegament del sistema, que actualment afecta dos terços de l'organització, està planificat per a ser completat a la fi de l'any 2021.

- La implantació d'un sistema d'autenticació de doble factor en la totalitat de l'organització (vegeu apèndix 3, "Bones pràctiques destacables"). El sistema ha sigut implantat per a un terç del personal. S'ha licitat un projecte per a la provisió de certificats a la totalitat d'empleats i es troba en estudi la seua integració amb el sistema de provisió d'aplicacions i escriptoris virtualitzats.

- La implantació d'un sistema de gestió d'incidències i informació de seguretat (SIEM). S'ha contractat la implantació del SIEM proporcionat pel Centre Criptològic Nacional, que analitzarà els registres d'activitat dels sistemes més rellevants des del punt de vista de la seguretat. El projecte es troba en l'actualitat en fase de planificació.

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 dels quals són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials –i en molts casos, reals– tant econòmiques com en la prestació dels serveis públics.

Les entitats locals, i les diputacions en particular, no són alienes a aquesta preocupació per la ciberseguretat en la seua pròpia operatòria, per la qual cosa han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat, que és 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 INES[3] del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs estiguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan correctament implementades.

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

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

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

disseny[4] com sobre la seua eficàcia operativa[5] per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control.

Els procediments realitzats en una auditoria de seguretat limitada són reduïts en comparació amb els que es requereixen per a obtindre una seguretat raonable, però s'espera que el nivell de seguretat siga, d'acord amb el judici professional de l'auditor, significatiu per als destinataris de l'Informe.

Abast

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

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

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

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

- controlador de domini
- programari de virtualització
- equips d'usuari (una mostra)

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

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

- elements de la xarxa de comunicacions (una mostra)
- elements de seguretat (una mostra)

Àmbit temporal

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

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

Metodologia

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

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

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

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

La guia pràctica de fiscalització dels OCEX 5313

La guia pràctica de fiscalització dels OCEX GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat", va ser aprovada per la Conferència de Presidents dels Òrgans de Control Extern el 12 de novembre de 2018, i forma part del *Manual de fiscalització* de la Sindicatura

de Comptes, que pot consultar-se en el nostre web. Per a major detall sobre la metodologia utilitzada ens remetem a aquesta guia.

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

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

També considerem d'interés, per a comprendre millor la importància dels CBCS, la lectura del nostre informe "Auditoria dels controls bàsics de ciberseguretat dels majors ajuntaments de la Comunitat Valenciana. Exercicis 2019 i 2020", en l'apartat 5 del qual hi ha, per a cada un dels controls, un apartat denominat **"Per què és important aquest control bàsic de ciberseguretat"**.

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

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

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

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

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

Els CBCS com a mesures de ciberhigiene

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

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

En 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.

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

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

[9] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* (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.

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 obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats	Hi ha un procés per a identificar les vulnerabilitats dels components del sistema que assegura que aquestes són identificades en temps oportú.
		CBCS 3-2: Priorització	Les vulnerabilitats identificades són analitzades i prioritzades per a la seua resolució atés el risc que suposen per a la seguretat del sistema.
		CBCS 3-3: Resolució de vulnerabilitats	Es realitza un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que aquestes es resolen en el temps previst en el procediment.
		CBCS 3-4: Pedaços	L'entitat disposa de procediments i eines que permeten aplicar els pedaços de seguretat publicats pels fabricants en un temps raonable.
CBCS 4 Ús controlat de privilegis administratius	Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'ús i configuració de privilegis administratius en ordinadors, xarxes i aplicacions.	CBCS 4-1: Inventari i control de comptes d'administració	Els privilegis d'administració estan limitats adequadament i l'entitat disposa d'un inventari de comptes d'administració que facilita el seu correcte control.
		CBCS 4-2: Canvi de contrasenyes per defecte	Les contrasenyes per defecte dels comptes que no s'utilitzen o bé són estàndard es canvien abans de l'entrada en producció del sistema.
		CBCS 4-3: Ús dedicat de comptes d'administració	Els comptes d'administració només es realitzen per a les tasques que són estrictament necessàries.
		CBCS 4-4: Mecanismes d'autenticació	Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes.
		CBCS 4-5: Auditoria i control	L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades.

Control	Objectiu del control	Subcontrol	
CBCS 5 Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors	Establir, implantar i gestionar la configuració de seguretat, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de previndre atacs per mitjà de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6 Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria)	Recollir, gestionar i analitzar *logs* d'incidències que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de *logs* d'auditoria	El *log* d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
		CBCS 6-2: Emmagatzematge de *logs*: Retenció i protecció	Els *logs* es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la seua consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de *logs*.	Els *logs* de tots els sistemes 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'analítica de *logs* per a realitzar correlació i anàlisi de *logs*.
CBCS 7 Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú.	CBCS 7-1: Realització de còpies de seguretat	L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema.
		CBCS 7-2: Realització de proves de recuperació	Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmeses a través de la xarxa.
CBCS 8 Compliment normatiu i governança de ciberseguretat	L'entitat compleix els requisits legals i reglamentaris que li són aplicables i té establida una 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	Cobreix al 100% amb l'objectiu de control i: - El procediment està formalitzat (documentat i aprovat) i actualitzat. - El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	A grans trets, compleix l'objectiu de control, si bé pot haver-hi uns certs aspectes no coberts al 100% i: - Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.). - Les proves realitzades per a verificar la implementació són satisfactòries. - S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	Cobreix de manera molt limitada l'objectiu de control i: - Se segueix un procediment, encara que aquest pot no estar formalitzat. - El resultat de les proves d'implementació i d'eficàcia no és satisfactori. Cobreix en línies generals l'objectiu de control, però: - No se segueix un procediment clar. - Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	No cobreix l'objectiu de control. El disseny cobreix l'objectiu de control, però el resultat de la revisió realitzada posa de manifest que la implementació o l'eficàcia operativa del control no són satisfactòries (s'han detectat incompliments significatius i generalitzats).

Controls

Per a determinar la situació global de cada control de ciberseguretat hem utilitzat el **model de nivell de maduresa** dels processos de control d'acord amb el que s'estableix en la GPF-OCEX 5313, que al seu torn 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. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. *L'eficàcia del procés depén de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.*
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. *Es disposa d'un catàleg de processos que es manté actualitzat. Aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant els incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor d'allò desconegut (o no planificat).* *L'èxit és més que bona sort: es mereix.* *Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2 i que sí que es gestiona en el nivell 3.*
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. *Es disposa d'un sistema de mesures i mètriques per a conéixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.* *En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.*
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. *El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.* *S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, i s'utilitzen com a indicadors en la gestió de la millora dels processos.* *En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes sobre la base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.*

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

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

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

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

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

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

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

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

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

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

La categoria d'un sistema d'informació, en matèria de seguretat, modula l'equilibri entre la importància de la informació que maneja, dels serveis que presta i l'esforç de seguretat requerit, en funció dels riscos 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:[10]

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

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

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

Indicadors globals

A l'efecte de l'ENS, la guia CCN-STIC-824 inclou una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics.

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

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

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

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

Governança de ciberseguretat

A l'efecte del present 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 forma responsable.[11]

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

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

És més que una mera qüestió tècnica, per la qual cosa **exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització**.[12]

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

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]

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

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

[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.

L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació[14] que ha de materialitzar-se en aspectes com ara:

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

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

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

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

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

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

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

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

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

Seguiment de les recomanacions

En aquest treball s'ha realitzat el seguiment de les recomanacions recollides en l'apèndix 5 de l'"Informe sobre auditoria operativa de la gestió i recaptació delegada en les diputacions de la Comunitat Valenciana. Exercici 2016".

[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.

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

Quadre 8. Situació de les recomanacions

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

En el quadre 2 es mostren les recomanacions contingudes en l'informe esmentat amb els comentaris relatius al seguiment realitzat i la situació a 30 de setembre de 2021.

Comunicació i confidencialitat

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

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

APÈNDIX 2
Situació dels controls bàsics de ciberseguretat

CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

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

Situació del control

Hem verificat que la Diputació realitza accions per a mantindre actualitzat l'inventari i control d'actius físics de l'entitat que es troben emparades per la normativa de seguretat vigent, que estableix formalment la responsabilitat de l'inventariat de dispositius.

La Diputació disposa de diverses eines i inventaris destinats a administrar els actius físics i pot considerar-se que, en conjunt, proporcionen un control adequat sobre aquests actius. Els equips d'usuari i l'equipament de xarxa són gestionats per mitjà de dues aplicacions que realitzen el descobriment automàtic dels elements, bé per mitjà de la instal·lació d'un agent en la fortificació inicial, bé per mitjà de la detecció automàtica. Per a la resta dels actius es disposa d'inventaris de gestió manual.

Addicionalment, hem verificat que existeix un procés adequat de gestió i aprovació de nous actius i retirada o substitució d'actius existents. A més, la Diputació ha configurat les eines d'inventariat per a relacionar els actius físics amb les licitacions i contractes de manteniment corresponents.

D'altra banda, no es disposa d'un sistema o control integral que impedisca la connexió de dispositius físics no autoritzats a la xarxa, però es troben en fase de desplegament determinades mesures i configuracions que, en conjunt, poden compensar parcialment l'absència d'aquests controls. Addicionalment, es disposa de diferents controls compensatoris robustos que detecten, impedeixen o limiten l'activitat dels dispositius físics no autoritzats en determinades zones crítiques o vulnerables de la xarxa.

Hi ha cert nivell de control sobre l'inventari i el control d'actius físics, i la seua valoració global aconsegueix un **índex de maduresa del 63,8%,** que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 1 del 79,7%**.

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 instal·lar-lo i executar-lo.

Situació del control

Hem analitzat la gestió que realitza la Diputació sobre l'inventari i control de programari i hem verificat que, si bé la responsabilitat de l'inventariat de programari es troba establida en la normativa de seguretat vigent, el control implantat no s'ha detallat completament en el conjunt de procediments formalment aprovats.

La Diputació ha implantat una elaborada solució basada en la virtualització de llocs de treball i aplicacions que és utilitzada per a la provisió de la major part d'aplicacions. La configuració específica aplicada permet una gestió eficient de l'inventari d'aplicacions, així com de les seues vulnerabilitats, versions, llicències i drets d'accés dels usuaris.

Per a la resta de programari utilitzat, la Diputació disposa d'un inventari de gestió automatitzada per a l'administració dels actius de programari instal·lats en els equips d'usuari. L'inventari inclou la informació suficient per a una gestió adequada de versions i llicències.

D'altra banda, s'ha evidenciat l'existència d'un reduït nombre d'equips, servidors i equips d'usuari, amb sistemes operatius fora del període de suport del fabricant, fet que suposa un risc per als sistemes d'informació.

La gestió del llicenciament i el manteniment d'aplicacions es realitza per mitjà d'un procés adequat, però que no està formalitzat, atés que no s'ha elaborat i aprovat un pla anual de manteniment del programari.

L'entitat compta amb mesures orientades a impedir l'ús de programari no autoritzat que poden considerar-se raonablement efectives, a més de disposar d'un procés d'autorització per a la instal·lació i ús de nou programari.

Hi ha cert nivell de control sobre l'inventari i control de programari autoritzat, que aconsegueix un **índex de maduresa del 65,0%,** que es correspon amb un **nivell de maduresa *N2*, *repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 2 del 81,3%**.

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

Objectiu del control

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

Situació del control

Hem analitzat la gestió de vulnerabilitats realitzada per la Diputació i hem observat que es realitzen diferents accions a fi d'identificar i remeiar vulnerabilitats, accions que es troben parcialment recollides en un procediment formalment aprovat.

La identificació i solució de vulnerabilitats es realitza sobre tots els sistemes que hem revisat, bé per part de tercers per mitjà de contractes de manteniment, bé directament per part del personal del Servei d'Informàtica.

La identificació de vulnerabilitats realitzada per la mateixa Diputació s'articula per mitjà de la subscripció a llistes de difusió de fabricants i organismes de referència, i a través d'una eina que permet la identificació automàtica de vulnerabilitats dels sistemes crítics.

La priorització i resolució es gestionen de manera informal, però no es troben recollides en el procediment aprovat. El procés complet no es troba totalment definit ni està suportat per eines de gestió de fluxos de treball, la qual cosa impedeix una gestió totalment eficaç.

Sobre l'aplicació de pedaços i actualitzacions de seguretat, s'apliquen de manera sistemàtica per mitjà d'una eina per al desplegament centralitzat d'actualitzacions i pedaços en el cas de sistemes amb nombrosos actius, i de manera manual en la resta de sistemes, inclosos els sistemes crítics.

Existeix un determinat nombre de sistemes crítics sobre els quals la Diputació ha identificat vulnerabilitats que no han sigut resoltes, la qual cosa suposa un risc rellevant. La Diputació ens ha indicat que s'ha acceptat el risc d'aquestes vulnerabilitats perquè s'ha experimentat, durant l'aplicació de pedaços i actualitzacions, diversos incidents amb afecció a l'operativa d'aquests sistemes crítics i la seua resolució pot suposar un risc major que el que es pretén eliminar.

Hi ha cert nivell de control sobre la gestió de vulnerabilitats, de manera que la valoració global del control aconsegueix un **índex de maduresa del 54,8%,** que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 3 del 68,4%**.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

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

Situació del control

Hem analitzat les accions que realitza la Diputació per al control dels comptes d'administració i hem verificat que existeix un control parcialment efectiu, però únicament determinades accions del procés es troben recollides en un procediment aprovat.

La gestió de privilegis administratius en els sistemes revisats es realitza amb diferent grau d'efectivitat depenent del sistema i de manera independent per a cada un, atés que el procediment que estableix les polítiques comunes de gestió de privilegis administratius no s'ha implantat de manera general en la Diputació. Hem verificat una correcta aplicació del principi del mínim privilegi en la gestió de privilegis administratius realitzada pel Servei d'Informàtica.

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

L'ús dedicat de comptes d'administració es troba correctament implantat en l'entitat per a la major part dels sistemes i els administradors disposen de comptes diferenciats depenent de les tasques a realitzar. No obstant això, en les aplicacions que suporten els processos de gestió comptable i recaptatòria, aquests comptes no es creen ni s'utilitzen de manera adequada.

S'han establit formalment requisits d'autenticació en una política de contrasenyes, que ha sigut adequadament implementada en els sistemes Windows i en aquells que han implementat SSO (*single sign-on*) amb el controlador de domini, integració que ha sigut realitzada de manera particularment efectiva en la Diputació i que ha proporcionat una política d'autenticació homogènia en aquests sistemes. En la resta dels sistemes, no es realitza una configuració de requisits d'autenticació d'acord amb la política establida.

Finalment, els registres d'activitat dels usuaris administradors es troben activats i emmagatzemats en tots els sistemes revisats i la Diputació disposa de diverses aplicacions i sistemes que permeten centralitzar aquests registres d'activitat, la qual cosa facilita la seua gestió i revisió.

Hi ha cert nivell de control sobre els comptes amb privilegis administratius, per la qual cosa la valoració global del control existent aconsegueix un **índex de maduresa del 67,5%**, que es correspon amb un **nivell de maduresa *N2*, *repetible però intuïtiu***; és a dir, els controls

es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment d'aquest CBCS 4 del 84,3%**.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

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

Situació del control

Hem analitzat les accions de la Diputació per al control de la configuració segura en aplicacions i dispositius i hem verificat que existeix un procediment formalment aprovat. No obstant això, aquest procediment no disposa del detall suficient i no representa amb total fidelitat el control implantat.

Hem verificat que s'han establit configuracions i 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 uns certs criteris de fortificació i proporcionen un nivell de seguretat homogeni en els sistemes. No obstant això, no s'han identificat mesures de gestió que permeten assegurar la correcta elaboració i aplicació de configuracions segures, fet que, si bé no implica necessàriament una aplicació incorrecta del control, sí que impedeix assegurar-ne l'eficàcia en tots els casos.

Sobre el monitoratge de les configuracions existents, hem verificat que s'han establit mesures que permeten gestionar les configuracions de determinats dispositius crítics de l'entitat i monitorar canvis no autoritzats i assegurar la integritat de les configuracions d'aquests sistemes.

La valoració global del control sobre les configuracions segures és que l'organització aconsegueix un **índex de maduresa del 50,3%,** que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 5 del 62,8%**.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

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

Situació del control

Hem analitzat les accions i mesures aplicades per la Diputació per al registre de l'activitat dels usuaris en els diferents sistemes i hem verificat que, encara que es disposa d'un procediment formalment aprovat, aquest no descriu amb total exactitud el control implantat.

Hem verificat que el registre d'activitat es troba activat en tots els sistemes revisats, si bé es manté la configuració per defecte que defineix el fabricant i no s'han aplicat configuracions o mesures específicament destinades al compliment dels requisits detallats en el procediment aprovat.

No obstant això, la Diputació disposa de diversos sistemes per a la gestió de registres d'activitat de determinats actius, la qual cosa suposa una millora notable de la configuració bàsica per defecte dels registres d'auditoria. Aquestes eines integren la major part dels sistemes rellevants des del punt de vista de la ciberseguretat i faciliten la retenció i protecció dels registres.

La centralització de registres d'activitat en sistemes externs simplifica l'anàlisi de les dades disponibles en cas d'incident de seguretat, si bé hem verificat que la revisió d'aquests registres d'activitat es realitza de manera reactiva i informal.

Els sistemes disponibles per a la gestió de registres no poden ser considerats un SIEM per les seues especificacions tècniques i funcionals, però poden considerar-se una mesura de seguretat compensatòria parcialment eficaç. No obstant això, la Diputació ha contractat recentment un projecte per al desplegament d'una solució SIEM del CCN, que integrarà informació de determinats sistemes crítics des del punt de vista de la seguretat i que es troba en fase de planificació.

La valoració global del control existent sobre el registre de l'activitat dels usuaris és que l'organització aconsegueix un **índex de maduresa del 66,7%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 6 del 83,3%**.

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 per al control de la còpia de seguretat de les dades i sistemes que es troben recollides en un procediment aprovat. No obstant això, aquest procediment es troba desactualitzat i no representa amb total fidelitat el control implantat.

Addicionalment, l'entitat compta amb un pla de continuïtat de negoci que considera la realització de còpies de seguretat com a part de les estratègies de recuperació davant de determinats escenaris

La Diputació ha finalitzat recentment el desplegament d'una solució de còpia que disposa de les característiques tècniques adequades, i cobreix les necessitats de l'organització quant al procés de realització de còpies de seguretat establit. Les polítiques de còpia aplicades han sigut desenvolupades d'acord amb les necessitats identificades des del departament TIC.

Hem verificat que la gestió i revisió 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, fet que, si bé no implica necessàriament una aplicació incorrecta del control de còpies, sí que impedeix assegurar l'eficàcia del control en tots els casos.

La solució tècnica inclou diferents mecanismes destinats a la protecció de les còpies de seguretat que poden considerar-se efectius davant d'una diversitat d'amenaces.

No es realitzen de manera sistemàtica proves de recuperació planificades com a part d'un procés de proves, si bé hem confirmat que es realitzen i registren freqüents recuperacions satisfactòries de diversos tipus de còpies en cas de pèrdua de dades o serveis.

La valoració global del control existent sobre les còpies de seguretat és que la Diputació aconsegueix un **índex de maduresa del 66,7%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 83,3%**.

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:

- La Diputació ha elaborat una política de seguretat de la informació (PSI) que ha sigut revisada, actualitzada i aprovada pel Ple de la Diputació. Actualment es troba en vigor la versió 5 i el seu contingut s'adequa als requisits establits per l'ENS.

- 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.
- La Diputació ha determinat categoritzar de nivell ALT els seus sistemes, valorant la importància de la informació manejada i dels serveis prestats en les dimensions de seguretat corresponents. No obstant això, a l'efecte d'aquesta auditoria i a fi de mantindre criteris homogenis amb la resta de les diputacions auditades l'hem considerat com de nivell mitjà.
- Es disposa de declaració d'aplicabilitat.
- S'ha emplenat i remés Informe de l'Estat de la Seguretat (Informe INES).
- Des de l'any 2016 s'han executat diversos projectes d'assistència tècnica per a adequació a l'ENS, amb assistència d'un proveïdor extern, en el marc dels quals es va realitzar l'any 2018 una auditoria de compliment, prevista en l'article 34 de l'ENS, en la qual es van identificar diverses no conformitats i s'han iniciat accions per a solucionar-les. Únicament ha sigut identificada una no conformitat de caràcter major, per absència de pla de continuïtat. Aquest pla ha sigut elaborat i aprovat i la seua implantació efectiva es troba en fase de finalització, incloent-hi la formació al personal i la realització de les proves periòdiques previstes en el pla.

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

- No s'ha solucionat la totalitat de no conformitats identificades en l'auditoria de compliment, 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 creat una oficina provincial de protecció de dades i seguretat, amb l'objectiu de desenvolupar les funcions previstes en la normativa nacional i comunitària relatives al delegat de protecció de dades, tant per a la mateixa Diputació com per als ajuntaments de la província de menys de 20.000 habitants que així ho sol·liciten.
- 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 dut a terme un procés d'anàlisi de riscos de manera conjunta amb l'ENS, adaptant els criteris de determinació del risc en el tractament de les dades al que s'estableix en l'article 32 del Reglament (UE) 2016/679.

No obstant això, no s'ha realitzat cap auditoria específica en matèria de protecció de dades.

Compliment legalitat del registre de factures

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

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió és que la Diputació aconsegueix un **índex de maduresa del 75,0%**, que es correspon amb un **nivell de maduresa N2**, que indica que hi ha un compliment raonable de la normativa, encara que hi ha aspectes que s'han de millorar.

Governança de ciberseguretat

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 acceptable.

Els aspectes fonamentals identificats que sustenten aquesta afirmació són:

- El compromís amb la gestió i el compliment de requisits legals relacionats amb la seguretat de la informació.
- Tal com es detalla en els subapartats anteriors, existeix un nivell raonable de compliment de la legalitat en matèria relacionada amb la seguretat de la informació.
- La definició i nomenament de rols, i la creació d'òrgans de govern de la seguretat de la informació. Hem verificat que existeixen i que exerceixen de manera efectiva i continuada les funcions establides.
- El tractament adequat per part de la direcció dels objectius estratègics de seguretat identificats pel Servei d'Informàtica, la qual cosa contribueix a l'assumpció d'aquests objectius com a part de l'estratègia general de l'entitat
- L'assignació de recursos humans i d'inversions a fi de donar compliment als objectius estratègics en matèria de seguretat, sense perjudici de les millores encara necessàries.

Els òrgans superiors de la Diputació han de reforçar l'actual nivell de suport i compromís amb la seguretat dels sistemes d'informació, a fi d'aconseguir els nivells de maduresa dels controls requerits per l'ENS i solucionar les deficiències identificades. Amb aquesta finalitat resulta convenient impulsar de manera **proactiva** iniciatives per a la millora de la ciberhigiene i la ciberresiliència.[16]

[16] Segons la Proposta de Directiva del Parlament Europeu i del Consell relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat i per la qual es deroga la Directiva 2016/1148, de 26 de novembre de 2021, "**adoptar un plantejament proactiu davant les ciberamences és vital en la gestió de riscos de ciberseguretat** i hauria de possibilitar que les

En aquest sentit, els òrgans de govern tenen responsabilitat no sols en el compliment legal, sinó que han de liderar i ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat. L'existència d'un lideratge recognoscible per tota la corporació pot fomentar els avanços en termes de conscienciació i potenciar el venciment de les resistències naturals de l'organització als canvis necessaris.

Tal com assenyalen les millors pràctiques, l'alta direcció de l'entitat, entre altres comeses, ha de ser responsable[17] de fixar els objectius estratègics, organitzar adequadament els seus elements constituents, les seues relacions internes i externes, dirigir l'activitat i les persones, promoure la millora contínua i comunicar la importància d'una gestió eficaç de la seguretat de la informació.[18]

autoritats competents puguen previndre de manera efectiva que les ciberamenaces es materialitzen en incidents reals que puguen causar pèrdues materials o morals considerables".

[17] *Guía de seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad. Responsabilidades y funciones.* CCN, març de 2019.

[18] *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información*.

APÈNDIX 3
Bones pràctiques destacables

Introducció

Amb caràcter general, si una entitat aconsegueix una valoració del 80% en l'índex de maduresa d'un control significa que està aplicant de manera raonable les bones pràctiques en matèria de seguretat de la informació establides en la normativa (ENS) o en les guies professionals corresponents, que se sintetitzen en el quadre 4 d'aquest informe. En altre cas l'entitat ha d'adoptar mesures per a millorar la seua ciberseguretat.

Addicionalment 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.

Sistema de provisió d'aplicacions i escriptoris virtualitzats

L'entitat ha desplegat una solució de virtualització d'aplicacions i escriptoris virtuals particularment avançada. L'eficàcia de la solució està basada en:

- La generació de diversos perfils d'usuari en la plataforma de virtualització, que proporciona suport a totes les casuístiques generals identificades i de mecanismes per a proporcionar suport a requisits que no es troben en aquestes casuístiques generals.

- La gestió correcta de l'assignació d'usuaris al perfil o perfils corresponents, que proporciona el servei requerit i facilita l'aplicació dels principis de mínim privilegi i necessitat de conéixer.

- La implantació del sistema de provisió virtual a la totalitat d'equips d'usuari de l'entitat (pendent de finalització, amb data prevista al desembre de 2021).

- La configuració dels equips d'usuari com a clients lleugers, que són configurats de manera segura segons les recomanacions d'organismes de referència i fabricants, que limita les vulnerabilitats dels equips i minimitza els riscos.

Aquest sistema de provisió d'aplicacions proporciona avantatges concrets sobre diferents aspectes que tenen afecció directa en la seguretat:

- Permeten una gestió integral en la provisió d'aplicacions, ja que maximitza l'eficiència de les actuacions, atés que aquestes es realitzen una única vegada per cada un dels perfils de provisió d'aplicacions.

- Permeten una gestió integral d'actualitzacions i correcció de vulnerabilitats, ja que maximitza l'eficiència del seu tractament i limita la superfície d'exposició, atés que el nombre d'aplicacions, versions d'aquestes i instal·lacions es troba molt reduït respecte a la provisió directa en equips d'usuari.

- Permet limitar el risc per connexió d'equips físics no autoritzats. Si bé no s'han implantat mesures específiques per a impedir aquesta connexió, la provisió d'aplicacions i sistemes virtualitzats permet aplicar mesures compensatòries que limiten el risc d'un incident potencial per connexió de dispositius no autoritzats a l'entitat.

Sistema d'autenticació i inici de sessió unificat

L'entitat ha desplegat un conjunt de mesures, algunes de les quals pendents de completar, que proporcionen de manera conjunta autenticació de doble factor i inici de sessió únic a la major part de sistemes i aplicacions que suporten els processos crítics.

Aquesta solució està basada en l'ús de certificats digitals emmagatzemats en targetes criptogràfiques i està sent integrada amb l'aplicació de virtualització que suporta el sistema de provisió d'aplicacions i escriptoris virtualitzats.

La integració del sistema d'autenticació amb el sistema de provisió d'aplicacions, juntament amb l'inici de sessió unificat implantat en les aplicacions virtualitzades, proporciona un nivell de seguretat addicional i permet satisfer els requisits establits en l'Esquema Nacional de Seguretat per a sistemes de nivell mitjà.

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

SIEM: Sistema de gestió d'incidències i informació de seguretat.

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

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

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

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

Ciberseguretat: És la capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o accions il·lícites o malintencionades que comprometen la disponibilitat, autenticitat, integritat i confidencialitat de les dades

emmagatzemades o transmeses, així com dels serveis que aquestes xarxes i sistemes ofereixen o fan accessibles.

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

Governança de ciberseguretat: 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 conéixer-la, en particular d'aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, ha d'estar disponible en la intranet corporativa de l'entitat a través d'una adreça URL. La normativa de seguretat de cada entitat té origen i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desplegament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

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

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

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

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

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

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, l'esborrany previ de l'Informe de fiscalització es va discutir amb la diputada responsable de participació, transparència i noves tecnologies i els responsables corresponents, perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

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

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

APROVACIÓ DE L'INFORME

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

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe auditoria CBCS Diputació de Castelló_2021_val - SEFYCU 3022675

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 RR3F E3CK ZLCN T2VL

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 - 25/01/2022 8:12 VICENT CUCARELLA TORMO