SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SÍNTESI DE LES AUDITORIES DE CIBERSEGURETAT DELS QUINZE MAJORS AJUNTAMENTS I DE LES TRES DIPUTACIONS DE LA COMUNITAT VALENCIANA

Exercici 2021

RESUM

Totes les administracions públiques desenvolupen les seues activitats en entorns d'administració electrònica cada vegada més avançats tecnològicament, el funcionament dels quals es basa en interconnexions per mitjà de xarxes complexes, la qual cosa origina un fort augment dels riscos provinents del ciberespai.

Atés l'escenari anterior i en sintonia amb els seus plans estratègics, la Sindicatura de Comptes ha realitzat auditories sobre la situació en 2021 dels controls bàsics de ciberseguretat (CBCS) en els quinze majors ajuntaments de la Comunitat Valenciana i les tres diputacions. Una part important del treball s'ha dedicat a analitzar l'evolució de la situació dels CBCS i el seguiment de les recomanacions realitzades en els informes de 2019/2020 dels quinze ajuntaments.

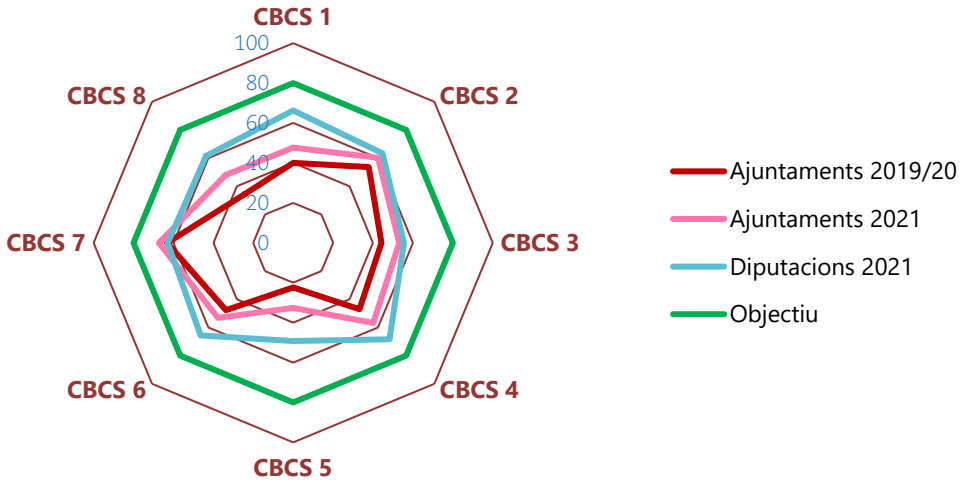
Després de la publicació de díhuit informes individuals en el nostre lloc web, la Sindicatura ha realitzat un informe de síntesi que ofereix una visió de conjunt, en el qual es destaquen les principals conclusions i observacions realitzades en els informes individuals.

Conclusions

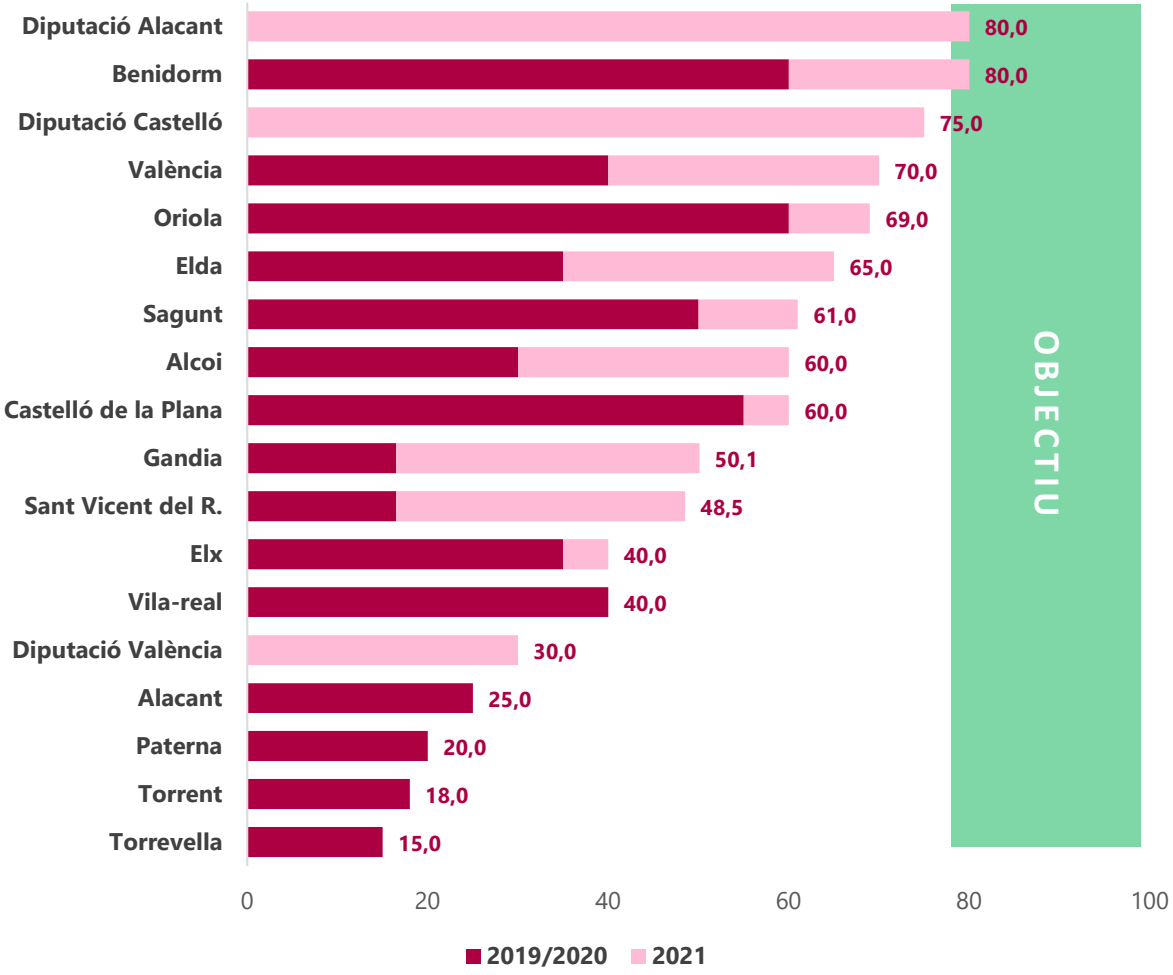
Encara que els ajuntaments han realitzat progressos des de la nostra auditoria anterior i han atés parcialment algunes de les nostres recomanacions, l'índex de maduresa mitjà dels CBCS només arriba al 52,4% (44,1% en 2019/2020), que continua sent insuficient i ha de millorar per a aconseguir el 80% exigit per l'ENS.

Respecte a les tres diputacions, l'índex de maduresa mitjà dels CBCS arriba al 61,6%, que tampoc compleix l'objectiu establit en l'ENS.

En el gràfic següent es pot observar de manera visual l'índex de maduresa mitjà dels CBCS de les diferents entitats i la seua evolució des de l'auditoria anterior en el cas dels ajuntaments.



En el gràfic següent es pot observar de manera visual la situació de l'índex de maduresa mitjà per a cada una de les diferents entitats auditades i la seua evolució des de l'auditoria anterior en el cas dels ajuntaments.



Encara que la majoria dels ajuntaments ha millorat el compliment de la normativa relacionada amb la seguretat de la informació, la nostra revisió ha posat de manifest que el grau de compliment és, en general, deficient, i que hi ha incompliments significatius generalitzats.

Hem avaluat, a més, l'estat de la seua governança de la ciberseguretat, entesa aquesta com el conjunt de responsabilitats i activitats dutes a terme pels òrgans de govern de les entitats per a proporcionar una direcció estratègica en matèria de ciberseguretat i garantir que s'aconseguisquen els objectius, que el risc es gestione adequadament i que els recursos de l'entitat s'utilitzen de manera responsable.

Els resultats del treball mostren que les entitats, en general, no tenen establida una adequada governança de la ciberseguretat, tal com exigeixen tant la normativa com un sistema de control intern ben establit. Les organitzacions requereixen el compromís i

implicació dels seus òrgans superiors. L'alta direcció té la responsabilitat d'establir una adequada governança de la ciberseguretat.

Aquest lideratge ha de fer-se efectiu per mitjà de la participació activa dels òrgans superiors en la gestió de les TIC i en la gestió de riscos, en l'aprovació de polítiques, normatives i procediments de seguretat de la informació, establint plans estratègics, vetlant pel correcte funcionament dels òrgans i rols designats en matèria de seguretat, dotant de recursos materials i humans i impulsant la implantació de controls sobre els sistemes d'informació i les comunicacions. Únicament d'aquesta manera podrà establir-se amb èxit un sistema eficaç de gestió continuada de seguretat de la informació.

El grau d'atenció a les nostres recomanacions ha sigut molt baix en alguns ajuntaments. Set dels quinze ajuntaments auditats no han atés completament cap de les nostres recomanacions. En contraposició, huit entitats han atés, almenys parcialment, la majoria de les recomanacions efectuades.

Hem reformulat les recomanacions d'acord amb la situació observada, amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió en les organitzacions. Entre les recomanacions realitzades amb major freqüència es troben: aprovar formalment procediments que descriguen les accions i controls implantats, l'establiment de solucions per a monitorar i detectar comportaments anòmals en les xarxes corporatives, el desplegament d'eines per a gestionar vulnerabilitats, restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa o actualitzar els sistemes obsolets.

NOTA

Aquest resum pretén ajudar a comprendre els resultats del nostre informe i facilitar la tasca als lectors i als mitjans de comunicació. Recomanem la lectura de l'informe complet per a conéixer el veritable abast del treball realitzat.

Informe de síntesi de les auditories de ciberseguretat dels quinze majors ajuntaments i de les tres diputacions de la Comunitat Valenciana

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 la ciberseguretat està 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, el **Pla Estratègic de la Sindicatura de Comptes per al període 2019-2022 assenyala la ciberseguretat com una de les àrees d'alt risc i prioritàries per a dur a terme la tasca fiscalitzadora**.

En 2019 i 2020 la Sindicatura de Comptes va realitzar auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants. Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 fer un treball de seguiment de la situació dels CBCS d'aquests 15 ajuntaments, dels quals ja s'han emés els informes corresponents. A més, es van emetre informes d'auditoria dels CBCS de l'exercici 2021 de les tres diputacions.

Després de publicar els díhuit informes individuals indicats (accessibles en la nostra pàgina web), la Sindicatura ha considerat convenient fer el treball de compilació i síntesi inclòs en aquest informe. D'aquesta manera s'ofereix una visió de conjunt en què es destaquen les principals conclusions i observacions realitzades en aquells.

L'entorn actual d'administració electrònica i els riscos tecnològics

Les lleis 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, i 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, representen la consolidació des del punt de vista jurídic de l'administració electrònica en les entitats públiques, i estableixen que la tramitació electrònica constituirà la seua actuació habitual, tant en les relacions amb tercers com entre administracions i intraadministracions, establint el principi de "digital per defecte".

A conseqüència de l'aplicació d'aquestes lleis, totes les entitats locals estan immerses en processos de transformació en la forma de prestació dels serveis als ciutadans i de la gestió pública, per a un desplegament ple de l'administració electrònica sustentada en sistemes d'informació cada vegada més complexos tecnològicament i interconnectats a través d'internet.

Els riscos per als sistemes d'informació que suporten els processos de l'administració electrònica augmenten a mesura que les amenaces a la seguretat provinents del ciberespai evolucionen contínuament i apareixen atacs nous cada vegada més sofisticats i destructius que obliguen els ens públics a fer-los front de manera proactiva i sistemàtica, establint mecanismes de defensa que en el seu fonament estan articulats per mitjà de l'**Esquema Nacional de Seguretat** (ENS), d'aplicació obligatòria per a tot el sector públic.

En el informe "Anàlisi i seguiment del Pla de Transformació Digital de la Generalitat 2016-2019" assenyalàvem que "la total dependència dels sistemes d'informació i de comunicacions existent en la gestió pública fa que les administracions públiques siguen més vulnerables davant dels ciberatacs, de manera que la transformació digital ha d'anar inseparablement unida a la ciberseguretat".[1]

La **total dependència dels SIC** que actualment existeix en la gestió pública fa que les nostres administracions siguen **molt vulnerables** davant dels ciberatacs i que **mantindre una adequada ciberhigiene i un sòlid sistema de protecció davant d'aquells siga més necessari que mai**. La generalització del treball en remot provocada per la pandèmia COVID-19, encara que actualment haja disminuït parcialment, té com a contrapartida de la seua eficiència un fort augment de la superfície d'exposició davant de les ciberamenaces, al qual les entitats públiques han de fer front amb la diligència deguda.

La governança de la ciberseguretat com a element articulador

A l'efecte d'aquest informe, s'entén per governança de la ciberseguretat el conjunt de responsabilitats i activitats que tenen com a objectiu proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una manera responsable. És el procés d'establir i mantindre un marc de referència, i donar suport a l'estructura i als processos de gestió per a garantir la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de les dades.

És més que una mera qüestió tècnica, per la qual cosa exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització. Considerem que una governança adequadament establida proporciona mecanismes que garanteixen que la

[1] En termes molt similars es manifesta el CCN en la seua publicació *Aproximación al marco de gobernanza de la ciberseguridad*, on s'afirma que l'èxit de la transformació digital depén, en gran manera, de garantir els requisits mínims de seguretat protegint la informació tractada i els serveis prestats, elements consubstancials al desenvolupament de la nostra societat.

seguretat és entesa com un sistema integrat i continuat, amb processos de gestió que vetlen per l'eficàcia de les mesures i processos de seguretat. La inexistència d'aquest marc de governança impedeix assegurar-ne l'eficàcia i idoneïtat.

2. OBJECTIUS, ABAST I METODOLOGIA DE LES AUDITORIES

Objectius

L'objectiu general de les auditories realitzades sobre la situació dels controls bàsics de ciberseguretat, en els quinze majors ajuntaments i en les tres diputacions de la Comunitat Valenciana, ha sigut proporcionar una avaluació sobre el seu disseny i eficàcia operativa, i sobre el compliment de la normativa bàsica relativa a la seguretat de la informació.

També hem analitzat l'evolució de la situació dels controls i l'atenció a les nostres recomanacions en els ajuntaments des de la nostra auditoria anterior.

Així mateix hem formulat recomanacions que contribuïsquen a esmenar les deficiències observades i a millorar els procediments de control.

Amb aquesta finalitat el treball d'auditoria ha consistit en:

- L'anàlisi del disseny i l'eficàcia operativa dels CBCS implantats en els ajuntaments i diputacions auditats.
- La identificació de deficiències de control que puguen afectar negativament la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de les dades, la informació i els actius dels sistemes d'informació d'aquestes entitats.
- La determinació del nivell de maduresa existent en cadascun dels CBCS i a nivell general en les diferents entitats auditades.
- La identificació d'incompliments significatius de la normativa sobre seguretat de la informació.
- L'avaluació de la governança de la ciberseguretat existent en cada entitat.

Atés el caràcter limitat de la revisió, l'objectiu no ha consistit a emetre una conclusió general sobre la confiança que mereixen els controls de ciberseguretat existents en el conjunt dels sistemes d'informació dels ens auditats. No obstant això, l'auditoria proporciona informació rellevant sobre el grau de ciberseguretat i ciberresiliència de les entitats i sobre les possibles accions de millora, mesures de ciberhigiene, que haurien d'escometre per a esmenar les deficiències observades i aconseguir els nivells de maduresa establits com a objectiu en l'ENS.

Àmbit subjectiu

Hem auditat els quinze municipis de la Comunitat Valenciana amb població superior a 50.000 habitants. En el quadre 1 es poden veure els ajuntaments auditats amb les dades de població i les obligacions reconegudes netes (ORN) de 2021, en milions d'euros.

Quadre 1. Ajuntaments auditats

Ajuntament	Població 2021	ORN 2021
València	789.744	956,5
Alacant	337.304	263,8
Elx	234.205	202,9
Castelló de la Plana	172.589	178,7
Torrent	84.025	63,0
Torrevella	82.842	108,7
Oriola	78.940	81,1
Gandia	75.970	95,8
Paterna	71.361	63,6
Benidorm	69.118	103,5
Sagunt	67.043	75,3
Alcoi	59.128	58,5
Sant Vicent del Raspeig	58.912	41,1
Elda	52.551	42,7
Vila-real	51.130	53,8
Ajuntaments auditats	**2.284.862**	**2.389,0**
Població de la Comunitat Valenciana	**5.058.138**	**5.288,4**
Cobertura de l'auditoria	**45,2%**	**45,2%**

Font: Ministeri d'Hisenda. Liquidacions dels pressupostos de l'exercici 2018. Dades actualitzades 31/07/2019 (<https://serviciostelematicosext.minhap.gob.es/sgcal/conprel>).

Les ORN són informació consolidada obtinguda de la liquidació de cada entitat local.

També auditem les tres diputacions provincials, les obligacions reconegudes netes (ORN) de les quals de 2021, en milions d'euros, es mostren en el quadre 2.

Quadre 2. Diputacions provincials

Diputació	ORN 2021
València	518,0
Alacant	274,1
Castelló de la Plana	178,1

En total s'han aprovat **díhuit informes** d'auditoria dels controls bàsics de ciberseguretat que estan publicats en el web de la Sindicatura. Aquest és un informe de síntesi que recull les conclusions de caràcter general que s'han pogut extraure després de realitzar aquestes auditories.

Àmbit objectiu

L'auditoria s'ha centrat en l'anàlisi de la situació dels huit CBCS definits en la GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat":

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

En l'apèndix 3 es proporciona un major detall sobre aquests controls, els seus objectius de control i els subcontrols que els formen.

Ha sigut necessari delimitar i concretar quins sistemes s'anaven a analitzar, a causa de la naturalesa de l'objecte material a revisar, que comprén els sistemes d'informació i comunicacions d'un ens local de grans dimensions, amb la seua gran amplitud, complexitat i diversitat. En aquest sentit, de cada entitat hem analitzat les aplicacions informàtiques que suporten dos dels processos de gestió més rellevants a l'efecte de la Sindicatura, com són la gestió comptable i pressupostària i la gestió tributària i recaptadora.

A més, per la seua importància per al bon funcionament dels sistemes d'informació i la ciberseguretat, en cada ens hem analitzat també una selecció dels tipus d'elements següents:

- controlador de domini

- programari de virtualització
- equips d'usuari
- elements de la xarxa de comunicacions (encaminador, *switches*, punts d'accés wifi, etc.)
- elements de seguretat (tallafoc, IPS, *proxy* de correu, *proxy* de navegació, servidors d'autenticació, infraestructura de generació de certificats, etc.)

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions sobre els ajuntaments es refereixen a la situació dels controls a 31 de desembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe. En el cas de les diputacions els indicadors s'han calculat amb referència al 30 de setembre de 2021.

Metodologia

Hem dut a terme les auditories de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques d'auditoria 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.

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

Els procediments realitzats en una auditoria de seguretat limitada són reduïts en comparació amb els que es requereixen per a obtindre una seguretat raonable, però s'espera que el nivell de seguretat siga, d'acord amb el judici professional de l'auditor, significatiu per als destinataris de l'informe. La seguretat limitada no garanteix que una auditoria realitzada de conformitat amb els principis i normes tècniques mencionades sempre detecte un incompliment significatiu quan existisca.

Les auditories dels controls bàsics de ciberseguretat (CBCS) han sigut realitzades 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", i en la resta de les seccions aplicables del *Manual de fiscalització* de la Sindicatura de Comptes.

Hem avaluat la situació dels CBCS en les diferents entitats utilitzant el model de nivell de maduresa dels processos, ja que és el sistema previst en l'ENS i permet establir objectius i

realitzar comparacions de manera homogènia entre diferents entitats i també veure l'evolució al llarg del temps en una entitat.

Els sistemes d'informació revisats estan classificats com de categoria de seguretat MITJANA. Així, d'acord amb aquesta categoria, el nivell de maduresa requerit per l'ENS i que també hem aplicat per als CBCS en les auditories realitzades és *N3, procés definit* i un índex de maduresa del 80%. Aquest nivell exigeix que els processos estiguen estandarditzats, documentats i comunicats amb accions formatives. Això implica que s'ha de disposar d'un catàleg de processos que es manté actualitzat; que aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general; que hi ha normativa establida i procediments per a garantir la reacció professional davant els incidents, i que s'exerceix un manteniment regular; que les oportunitats de sobreviure a un ciberatac són altes, encara que sempre queda el factor d'allò desconegut (o no planificat).

Com s'ha assenyalat abans, els resultats obtinguts en aplicar aquesta metodologia permeten formar una idea general de la situació dels controls de ciberseguretat en els ens auditats, de la seua ciberresiliència i del grau de compliment d'una sèrie de disposicions legals molt importants en matèria de seguretat dels sistemes d'informació.

Les constatacions de l'auditoria, les conclusions i els esborranys d'informe individuals es van discutir amb els responsables de les diferents entitats, d'acord amb el que s'estableix en el nostre *Manual de fiscalització*. Els informes individuals es van sotmetre al procediment contradictori per mitjà del corresponent tràmit d'al·legacions tal com es recull en aquells. En aquest informe es mostren els resultats comparatius de totes les entitats de manera sintètica.

En l'apèndix 1 es proporciona un major detall de la metodologia utilitzada.

Confidencialitat

Atés que la informació utilitzada en l'auditoria i els resultats detallats d'aquesta tenen un caràcter sensible i poden afectar la seguretat dels sistemes d'informació de les entitats revisades, les comunicacions d'informació sensible entre la Sindicatura i les entitats s'han realitzat per mitjà de canals xifrats, a fi de garantir la integritat i confidencialitat de les dades. Addicionalment, la Sindicatura disposa de les polítiques, procediments i mecanismes necessaris per a garantir que aquesta informació únicament és accessible pel personal encarregat de l'execució d'aquest treball.

3. CONCLUSIONS GENERALS

PRIMERA CONCLUSIÓ

Encara que, en general, els ajuntaments han realitzat progressos des de la nostra auditoria anterior i han atés parcialment algunes de les nostres recomanacions, l'índex de maduresa mitjà dels controls bàsics de ciberseguretat (52,4%) continua sent insuficient i ha de millorar per a aconseguir els nivells exigits per l'ENS. Només un ajuntament (Benidorm) aconsegueix el 80% requerit per l'ENS.

La situació de les diputacions és lleugerament millor i aconsegueix un índex de maduresa mitjà del 61,6%, però també està per davall de l'objectiu establit en l'ENS.

En el quadre 3 es mostra la situació detallada en les diferents entitats auditades.

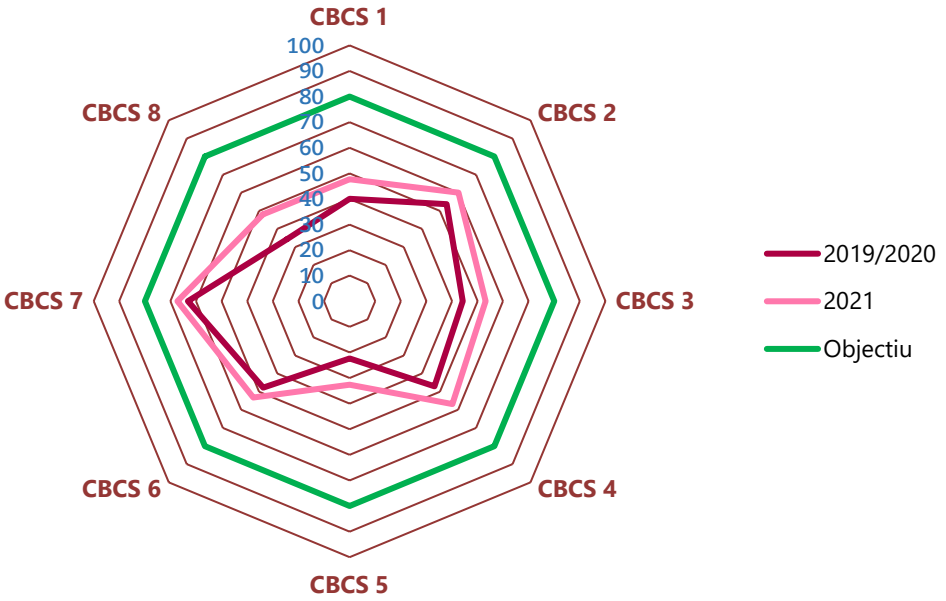
Quadre 3. Índex de maduresa mitjà dels controls bàsics de ciberseguretat dels 15 ajuntaments i de les tres diputacions

		AJUNTAMENTS						DIPUTACIONS		
		2019/2020			31/12/2021			30/09/2021		
	Control	*Índex de maduresa*	*Nivell de maduresa*	*Índex de compliment*	Índex de maduresa	Nivell de maduresa	Índex de compliment	Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1	Inventari i control de dispositius físics	*40,1%*	***N1***	*50,1%*	47,7%	**N1**	59,6%	66,3%	N2	82,9%
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	*53,6%*	*N2*	*67,0%*	60,1%	N2	75,2%	63,3%	N2	79,2%
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	*44,2%*	***N1***	*55,3%*	53,2%	N2	66,5%	55,5%	N2	69,3%
CBCS 4	Ús controlat de privilegis administratius	*47,0%*	***N1***	*58,7%*	56,8%	N2	71,0%	68,3%	N2	85,4%
CBCS 5	Configuracions segures del programari i maquinari	*22,3%*	***N1***	*27,9%*	32,6%	**N1**	40,7%	49,2%	**N1**	61,5%
CBCS 6	Registre de l'activitat dels usuaris	*47,7%*	***N1***	*59,6%*	53,2%	N2	66,5%	65,6%	N2	82,0%
CBCS 7	Còpies de seguretat de dades i sistemes	*63,2%*	*N2*	*79,0%*	67,3%	N2	84,1%	62,9%	N2	78,6%
CBCS 8	Compliment normatiu i governança de ciberseguretat	*34,4%*	***N1***	*43,0%*	48,0%	**N1**	60,0%	61,7%	N2	77,1%
	General	***44,1%***	***N1***	***55,1%***	**52,4%**	***N2***	**65,4%**	**61,6%**	***N2***	**77,0%**

La comparació dels resultats detallats obtinguts en l'auditoria de 2021 amb els obtinguts en les auditories de 2019/2020 mostra una millora en tots els controls. No obstant això, el nivell d'efectivitat mitjà en els controls analitzats continua sent insuficient, ja que cap aconsegueix l'objectiu i hi ha possibilitats clares de millora per a aconseguir els nivells exigits per l'ENS, particularment sobre els controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 1, 5 i 8).

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

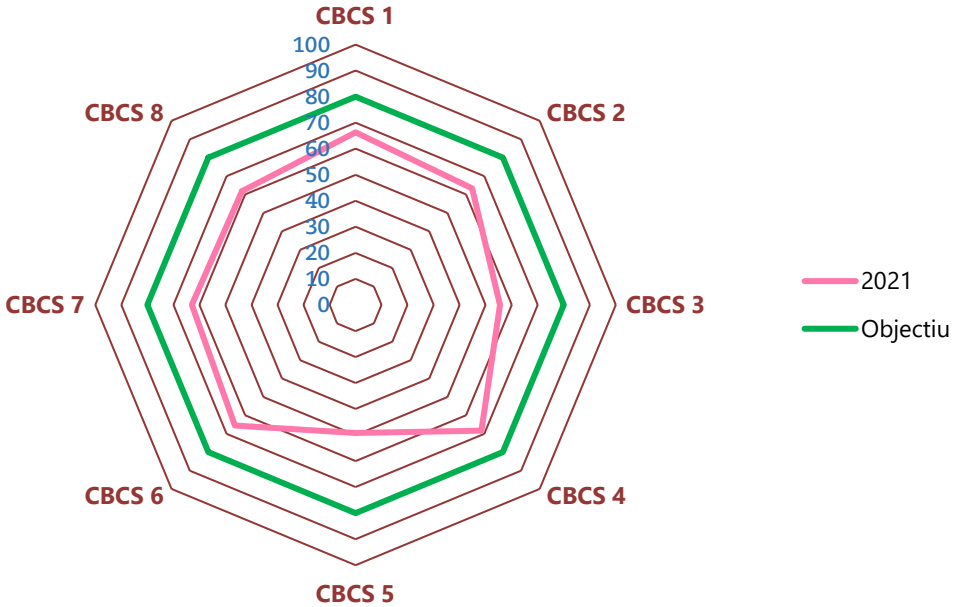
Gràfic 1. Índex de maduresa mitjà dels CBCS dels quinze ajuntaments



En general, els ajuntaments han realitzat accions encaminades a millorar els seus sistemes, però aquestes accions no són suficients per a complir els requisits de l'ENS.

D'altra banda, el gràfic 2 reflecteix el mateix indicador (índex de maduresa mitjà de cada control) en les tres diputacions provincials.

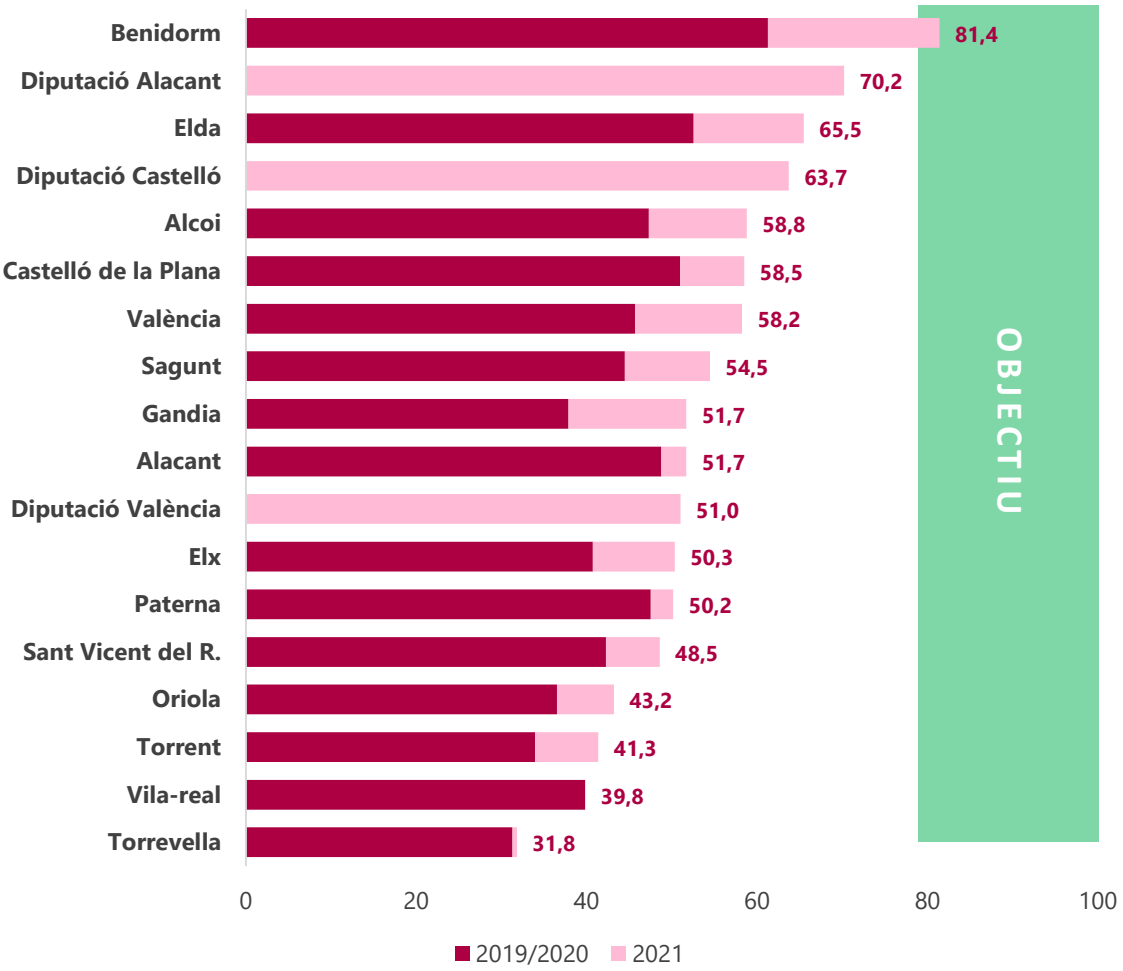
Gràfic 2. Índex de maduresa mitjà dels CBCS de les diputacions



Encara que els resultats s'aproximen a l'objectiu en alguns dels controls revisats, cap arriba, de mitjana, al valor objectiu.

El gràfic 3 mostra l'evolució de l'índex de maduresa mitjà de cada una de les díhuit entitats auditades.

Gràfic 3. Situació de l'índex de maduresa mitjà dels CBCS



Tal com s'observa en el gràfic anterior, **únicament l'índex de maduresa mitjà de l'Ajuntament de Benidorm aconsegueix l'objectiu establit per l'ENS.**

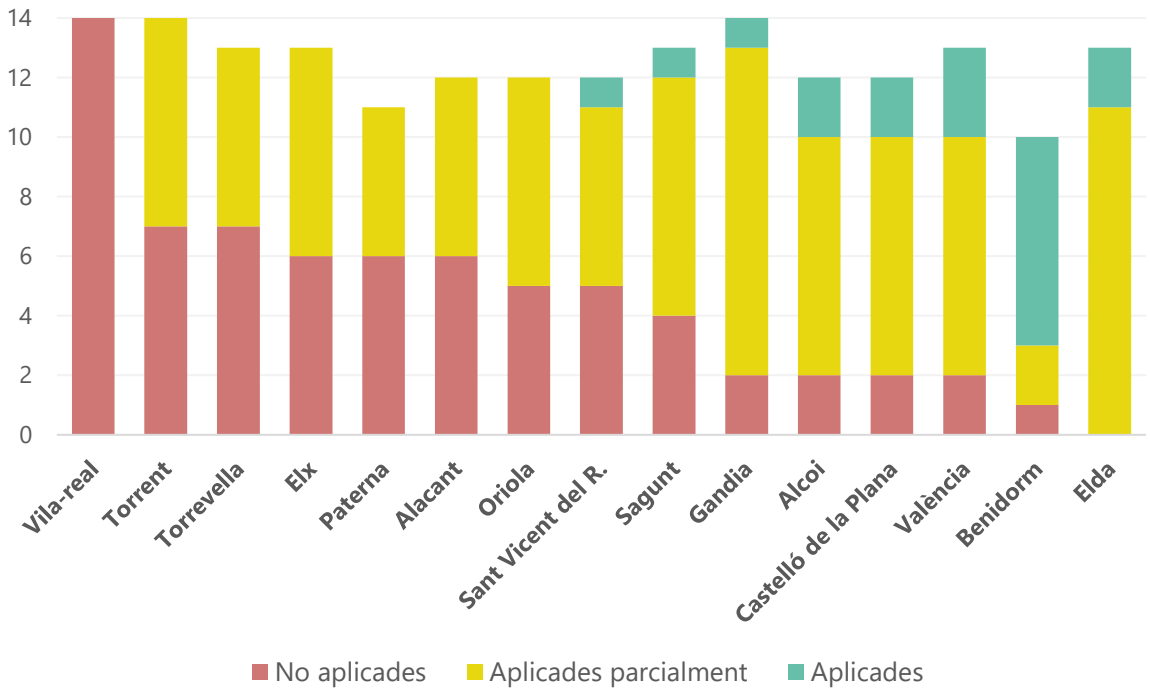
En l'apèndix 3 es detallen les deficiències observades i s'afig més informació sobre com millorar el funcionament dels controls.

SEGONA CONCLUSIÓ

El grau d'atenció a les nostres recomanacions per part dels ajuntaments ha sigut desigual. Cal que aquests dediquen els esforços i recursos necessaris per a esmenar les deficiències identificades i aconseguir un nivell raonable de ciberseguretat.

En els 15 informes emesos en 2019/2020 es van efectuar 188 recomanacions, de les quals únicament 19 s'han atés per complet, 100 s'han atés parcialment i 69 no han sigut ateses. El gràfic següent mostra el nivell d'atenció a les nostres recomanacions per part de cada una de les entitats auditades.

Gràfic 4. Recomanacions ateses per entitat



Del gràfic anterior és destacable que set entitats no han atés completament cap de les recomanacions que vam realitzar en 2019/2020, una de les quals (Vila-real) no ha atés cap de les recomanacions realitzades ni tan sols parcialment.

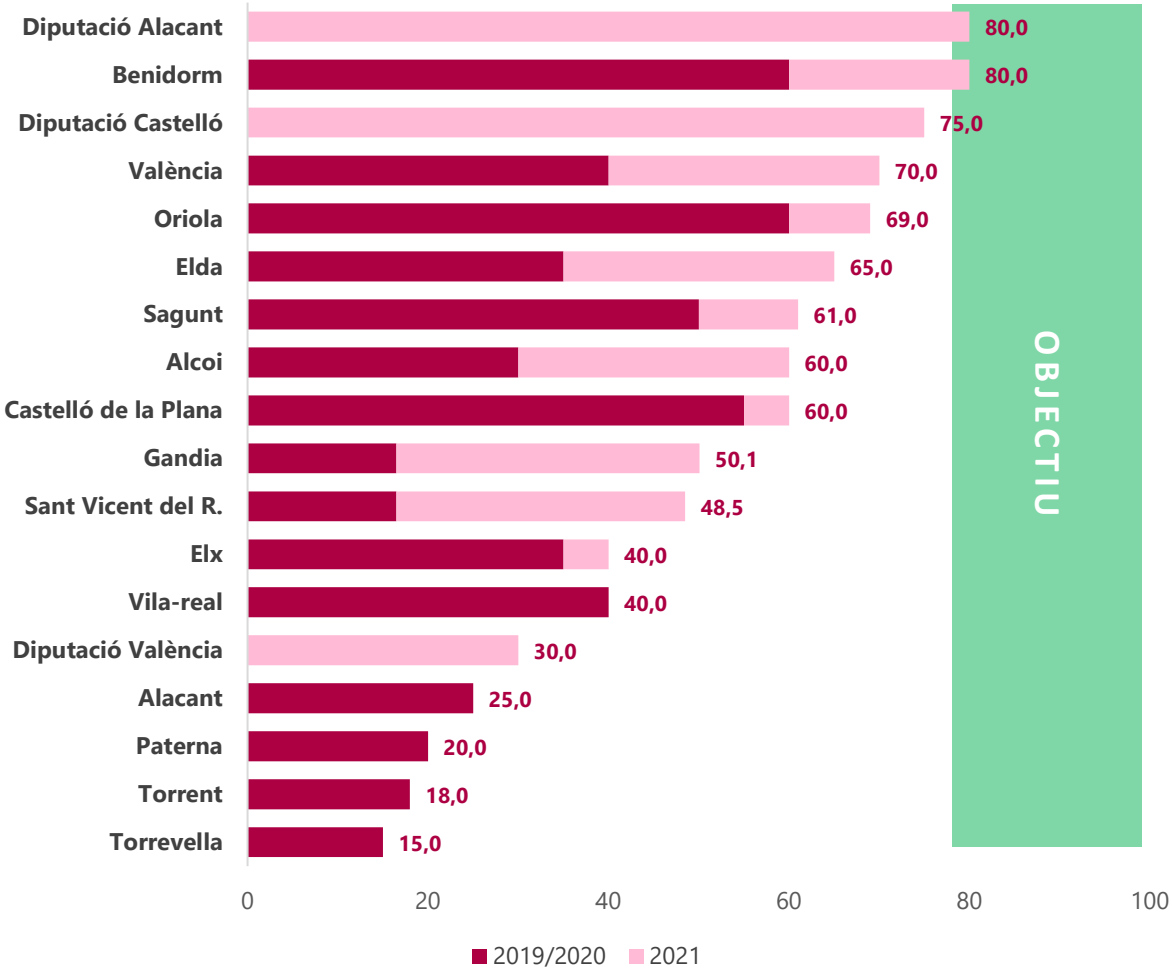
En contraposició a això, hi ha huit entitats que han atés completament almenys una recomanació i de manera parcial la majoria de les recomanacions realitzades en 2019/2020.

TERCERA CONCLUSIÓ

El grau de compliment de la normativa relativa a la seguretat de la informació és, en general, deficient i hi ha incompliments de la normativa significatius generalitzats.

El gràfic següent mostra l'índex de compliment normatiu obtingut per les entitats durant el nostre treball de revisió.

Gràfic 5. Índex de maduresa del compliment de la normativa (CBCS 8)



Com pot observar-se en el gràfic, la majoria dels ajuntaments ha millorat el seu grau de compliment de la normativa des de la nostra auditoria anterior.

QUARTA CONCLUSIÓ

Les entitats auditades, en general, no tenen establida una adequada governança de la ciberseguretat, tal com exigeixen tant la normativa com un sistema de control intern ben establit.

Els òrgans superiors de les entitats (alcalde o alcaldessa en el cas dels ajuntaments; president o presidenta en el cas de les diputacions) són els **responsables** que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació que garantisca la ciberresiliència de l'entitat. S'ha d'actuar de manera urgent per a solucionar les mancances identificades en aquesta matèria en cada una de les entitats, ja que afecten de manera negativa l'estat de la seua ciberseguretat.

Una adequada governança de ciberseguretat ha de reflectir-se, principalment, en:

- Ha d'existir un clar **compromís dels òrgans de govern de l'entitat amb la ciberseguretat**. En aquest sentit, els òrgans de govern tenen responsabilitat no sols en la formalització i adequació legal, sinó que han de ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat.

- L'aprovació pel president de l'ens local de les **polítiques de seguretat de la informació**.

- Ha d'existir una **planificació estratègica en matèria de ciberseguretat**, que proporcione un marc d'actuació a mitjà termini que assegure l'atenció a les necessitats prioritàries respecte a la seguretat, i es trobe alineada amb l'estratègia corporativa. La planificació estratègica de la seguretat evita una gestió reactiva basada principalment en necessitats sobrevingudes.

- La constitució, i funcionament efectiu, d'un **comité de seguretat de la informació**, òrgan especialitzat i permanent per a la ciberseguretat integrat per aquelles persones de l'organització amb responsabilitat en la presa de decisió en matèria de seguretat i privacitat de la informació, així com per aquelles designades en representació d'altres òrgans o comités.

- El nomenament de **rols de gestió de seguretat**, a fi de concretar i personalitzar les responsabilitats en matèria de seguretat de la informació.

- L'elaboració d'uns **pressupostos i la dotació d'equips humans adequats** a les exigències d'una ciberdefensa eficaç en els actuals entorns d'administració electrònica avançats i interconnectats.

- Las normes i els procediments de seguretat **han d'estar formalment aprovats** per l'òrgan que s'establisca en el document de polítiques de seguretat de la informació i **han de ser d'aplicació obligatòria en tots els sistemes d'informació de**

l'ajuntament o diputació, que han d'estar governats per les mateixes polítiques i normes de seguretat.

Aquesta **normativa interna ha de dissenyar-se per a ser aplicada, no per a complir una formalitat**. El contingut del conjunt de polítiques, normes i procediments aprovats ha de ser una representació fidedigna i precisa del sistema de seguretat implantat per l'ens local. L'aprovació d'un marc normatiu que no represente la realitat de l'ens esdevé un ús estèril de recursos per la seua falta d'efectivitat i una falsa percepció de compliment que pot comportar l'abandó d'altres mesures més adequades.

L'apèndix 2 detalla les deficiències observades i s'afig més informació sobre com ha d'establir-se una governança adequada en les entitats per a garantir el funcionament eficaç d'un sistema integral de gestió continuada de la seguretat de la informació.

4. RECOMANACIONS

S'inclou en aquest apartat un resum de les recomanacions realitzades en els 18 informes individuals dels controls bàsics de ciberseguretat d'ajuntaments i diputacions.

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

a) L'inventari de dispositius físics s'ha de mantindre sistemàticament actualitzat, utilitzant un procediment d'autorització per a l'alta de nou maquinari i un altre per a actualitzar les baixes.

Si bé moltes de les entitats auditades compten amb un inventari de maquinari actualitzat, la principal recomanació ha sigut que s'ha d'aprovar un procediment que descriga les accions dutes a terme per a inventariar els elements i actualitzar aquest inventari.

D'altra banda, la principal mancança en aquest apartat ha sigut la falta de controls de connexió de dispositius físics no autoritzats a la xarxa corporativa. Aquesta mancança ha sigut identificada com de risc i cost alts, la qual cosa implica que les entitats han de realitzar inversions per a implantar de manera efectiva aquest control.

Sobre l'inventari i control de programari autoritzat i no autoritzat (CBCS 2)

b) De manera similar a l'apartat anterior, s'ha evidenciat l'existència d'inventaris de programari actualitzat en moltes de les entitats auditades. La principal recomanació relacionada amb aquest control ha sigut que ha d'aprovar-se formalment un pla de manteniment per al programari llicenciat.

Una altra de les recomanacions generalitzades ha sigut que s'ha d'identificar i actualitzar tot el programari que està fora del període de suport, que s'ha considerat com a deficiència greu en quasi totes les entitats auditades.

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

c) Una de les principals recomanacions relatives a aquest CBCS ha sigut que les entitats han de dotar-se d'eines que faciliten la detecció i aplicació d'actualitzacions i pedaços de seguretat. S'ha recomanat a aquest efecte l'ús d'eines centralitzades de gestió de pedaços.

La no utilització d'aquestes eines implica un risc alt per a l'organització per falta del control necessari sobre els dispositius i sistemes. Establir-les pot suposar un cost moderat, però el risc disminueix considerablement.

Addicionalment, per a aconseguir un control efectiu sobre les vulnerabilitats, es recomana l'ús d'eines d'escaneig i la realització de proves de *hacking* ètic o de penetració.

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

d) En aquest apartat les entitats tenen un ampli marge de millora per mitjà de la implantació de certes mesures que suposen un cost baix per a l'organització, però que impliquen la disminució significativa del risc.

Entre les recomanacions realitzades destaquem la necessitat d'eliminar l'ús d'usuaris genèrics, la utilització de permisos basats en la regla de mínims privilegis, canvi d'usuaris i contrasenyes per defecte i la implantació d'una política robusta de contrasenyes que s'aplique a tots els sistemes de l'entitat.

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

e) La recomanació més freqüent ha sigut que s'ha d'establir i aprovar un procediment per a l'ús de guies de fortificació basades en les recomanacions dels fabricants i del Centre Criptològic Nacional.

Si bé la pràctica totalitat d'entitats revisades disposa de guies informals de configuració de certs sistemes, la seua elaboració no considera com a objecte la consecució d'un determinat nivell de seguretat i la inclusió de mesures de seguretat en aquestes no es troba formalitzada. A més, en cas d'incloure configuracions específiques de seguretat, aquestes en general es basen únicament en l'experiència i coneixements dels administradors i implantadors dels sistemes i no en les recomanacions de fabricants i organismes de referència.

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

f) Les principals recomanacions han sigut la formalització i aprovació d'un procediment de gestió de registres d'activitat i la seua centralització en sistemes específics per al seu tractament.

La configuració per defecte dels sistemes inclou en general l'habilitació dels registres d'activitat d'usuaris i administradors. No obstant això, la falta d'organització de la seua gestió i la dispersió en múltiples sistemes dificulten l'explotació de la informació i el seu aprofitament per a la identificació d'esdeveniments i vulneracions de seguretat.

Sobre les còpies de seguretat de dades i sistemes (CBCS 7)

g) Hem recomanat quasi en la totalitat d'auditories la realització de proves planificades de recuperació de les còpies de seguretat de dades i sistemes, ja que la seua absència impedeix garantir la completa eficàcia del procés de gestió de còpies de seguretat. En general només es realitzen recuperacions de dades d'usuaris a demanda.

Sobre el compliment normatiu (CBCS 8)

h) Han d'adoptar-se les mesures necessàries per a donar compliment als diferents requeriments legals en matèria de seguretat de la informació.

APÈNDIX 1
Metodologia aplicada

1. 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 classe provinents del ciberespai, majors riscos de ciberseguretat i s'han multiplicat els incidents de seguretat dels quals són víctimes les entitats públiques, amb greus repercussions potencials –i en molts casos, reals– tant econòmiques com en la prestació dels serveis públics.

Les entitats locals no són alienes a aquesta problemàtica de la ciberseguretat, 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'ENS, que és **de compliment obligat**.

Per aquestes raons, és imperatiu que els responsables de les entitats gestionen aquest tipus de riscos i establisquen els controls de ciberseguretat necessaris per a mantindre els sistemes d'informació protegits davant de les amenaces de seguretat i evitar la interrupció en els serveis prestats als ciutadans.

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

Tot i que l'adopció de mesures de seguretat adequades fa més resilients les organitzacions davant dels ciberatacs, l'anàlisi dels incidents produïts que es realitza en els informes INES[2] del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs es mantinguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan correctament implementades.

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

2. LA GUIA PRÀCTICA DE FISCALITZACIÓ DELS OCEX 5313

La guia 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.

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

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), 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 el màxim possible.

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

3. ALINEACIÓ DELS CBCS AMB L'ESQUEMA NACIONAL DE SEGURETAT

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

Quadre 4. 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 i op.exp.2
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	mp.sw.2 i op.exp.4
CBCS 4	Ús controlat de privilegis administratius	op.acc.4 i op.acc.5
CBCS 5	Configuracions segures del programari i maquinari	op.exp.2 i op.exp.3
CBCS 6	Registre de l'activitat dels usuaris	op.exp.8 i 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 de 2010 (vigent en el moment de les auditories).

4. ELS CBCS COM A MESURES DE CIBERHIGIENE

L'European Union Agency for Cybersecurity (ENISA) assenyala[3] 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. Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.[4]

En aquesta direcció, ENISA estableix deu punts d'acció per a una ciberhigiene adequada. Com s'observa en el quadre 5, 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.

Quadre 5. Punts d'acció d'ENISA

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

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

5. CRITERIS D'AUDITORIA: ELS CBCS 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.

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

[4] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices*, 2017.

Quadre 6. Els CBCS i els seus subcontrols

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

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

6. 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 6 anterior), dels quals hem revisat tant el disseny com l'eficàcia operativa.

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

Quadre 7. Avaluació dels subcontrols

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

Controls

Per a determinar la situació global de cada control de ciberseguretat hem utilitzat el **model de nivell de maduresa** dels processos de control d'acord amb el que s'estableix en la GPF-OCEX 5313, que al seu torn està basada en la *Guía de seguridad CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 8. Nivells de maduresa

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

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

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

7. NIVELL DE MADURESA MÍNIM REQUERIT EN FUNCIÓ DE LA CATEGORIA DELS SISTEMES D'INFORMACIÓ AUDITATS

Als sistemes d'informació i comunicacions 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 ciberincident amb repercussió en la capacitat organitzativa per a:

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

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

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

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

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

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

b) Un sistema d'informació és 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 és 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:[5]

Quadre 9. Categories de seguretat

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%.

[5] *Guía de seguridad de las TIC. CCN-STIC 824. Informe Nacional del Estado de Seguridad de los Sistemas TIC*.

8. INDICADORS GLOBALS

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

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

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

9. SEGUIMENT DE LES RECOMANACIONS

En les auditories dels ajuntaments s'ha realitzat el seguiment de les recomanacions efectuades en els informes d'auditoria de 2019/2020.

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

Quadre 10. Situació de les recomanacions

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

10. NOU ESQUEMA NACIONAL DE SEGURETAT (RD 311/2022)

Durant els últims anys, el creixement de les TIC ha suposat l'aparició de nombroses i noves tecnologies relacionades amb el ciberespai (intel·ligències artificials, *blockchain*, descentralització de serveis, *edge computing*, etc.), i com ha conseqüència han aparegut riscos i amenaces nous i s'ha incrementat el nombre de ciberatacs, cada vegada més sofisticats.

En aquest escenari tan complex, per a abordar els riscos i garantir un ús segur de les xarxes, comunicacions i sistemes d'informació, han d'adoptar-se estratègies i mesures per a previndre, detectar i respondre a ciberatacs de manera proactiva, fomentant així l'ús d'un ciberespai segur i fiable. Al mateix temps, han d'adaptar-se a les regulacions europees i nacionals en matèria de seguretat.

El Reial Decret 3/2010, de 8 de gener, pel qual es regulava l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, fixava una sèrie de principis bàsics, requisits mínims i mesures de seguretat per a garantir la seguretat de la informació i els serveis prestats pels organismes públics. Totes les nostres auditories dels CBCS de les entitats locals, fins a 2022 inclusivament, s'han realitzat prenent com a base aquest ENS.

Les tecnologies emergents i els nous riscos que aquestes comporten, al costat de l'experiència i coneixement adquirits pel Centre Criptològic Nacional durant els últims anys, necessitaven que l'ENS fora actualitzat. Així, el nou Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, substitueix l'anterior i inclou algunes novetats:

- Incorporació de la figura del perfil de compliment, per a ajustar els requisits de l'ENS a necessitats específiques, com ara determinats col·lectius (entitats locals, universitats, etc.) o determinats àmbits tecnològics (serveis *cloud*, per exemple).
- Establiment d'un protocol d'actuació davant ciberincidents.
- Nou sistema de codificació dels requisits de les mesures de seguretat que afegeix reforços als requisits bàsics de seguretat.
- S'actualitzen les mesures de seguretat respecte al Reial Decret 3/2010.

APÈNDIX 2
La governança de la ciberseguretat

1. QUÈ ÉS LA GOVERNANÇA DE LA CIBERSEGURETAT

A l'efecte d'aquest informe, s'enten per governança de la seguretat de la informació i les comunicacions o de ciberseguretat (termes que utilitzem de manera indistinta) el conjunt de responsabilitats i activitats que tenen com a objectiu proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una manera responsable.[6]

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.[7] Aquest lideratge ha de ser exercit per l'alta direcció/òrgans superiors de l'entitat. El seu compromís amb la seguretat és el factor clau que habilita l'establiment d'un marc de governança efectiu en les organitzacions.

2. PER QUÈ ÉS IMPORTANT LA GOVERNANÇA DE LA CIBERSEGURETAT

La importància de la governança en la gestió de la ciberseguretat ha sigut objecte de diversos documents i guies del Centre Criptològic Nacional (CCN), entre els quals destaquen l'*Aproximación al marco de gobernanza de la ciberseguridad. Año 2022*, la *Guía de seguridad de las TIC CCN-STIC 201. Organización y gestión para la seguridad de las TIC* i la *Guía de seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad, responsabilidades y funciones*.

L'existència d'un conjunt eficaç de processos de gestió de la ciberseguretat i de responsabilitats definides proporciona a les entitats múltiples avantatges respecte a les entitats sense un marc de governança adequadament definit, independentment de l'existència de recursos tècnics i de les mesures de seguretat aplicades.

Alguns dels avantatges que l'existència d'un marc efectiu de governança proporciona a les entitats són:

- Possibilita l'alineació de les activitats relatives a la seguretat de la informació amb els objectius estratègics de l'entitat.
- Facilita la coordinació entre diferents àrees de l'organització i els implicats en matèria de seguretat de la informació.

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

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

- Possibilita que el conjunt d'activitats realitzades i mesures de seguretat aplicades constituïsquen un sistema de gestió de la seguretat de la informació que transcendeix les iniciatives individuals.

- Estableix les responsabilitats del personal implicat, necessàries per a garantir que es compleixen els objectius i s'aconsegueix el nivell de seguretat requerit.

- Estableix processos que impedeixen que l'eficàcia de les activitats de seguretat depenga de rols concrets de l'organització o només d'iniciatives personals, sinó d'un sistema ben establit.

- Ajuda a fomentar una cultura en matèria de ciberseguretat en les organitzacions.

Per contra, aquelles entitats que no disposen d'un marc de governança adequadament definit i implantat tenen una alta probabilitat d'experimentar les mancances següents:

- El principal risc consisteix en el fet que l'entitat siga vulnerable davant de ciberatacs per no disposar d'un sistema de controls coherent i acceptat per tota l'organització.

- Probable ús ineficient dels recursos, atés que, independentment de la idoneïtat d'aquests recursos respecte a les necessitats identificades, no hi ha mecanismes que asseguren que aquests s'utilitzen de manera adequada per a respondre a necessitats alineades amb els objectius estratègics.

- No assegura l'existència de mecanismes de coordinació interna entre les diferents àrees de l'organització i els responsables de la seguretat, la qual cosa impedeix garantir que les necessitats siguen adequadament identificades dins del termini i en la forma escaient. A més, possibilita que hi haja àrees que, de manera inadequada, realitzen una gestió no coordinada de la seguretat al marge de les polítiques i normes de seguretat de l'organització.

- No s'assegura que el conjunt de mesures i processos de seguretat implantats constituïsquen un sistema de gestió de la seguretat de la informació, integrat i coherent, la qual cosa implica un risc que no hi haja mecanismes de control que vetlen per l'eficàcia d'aquestes mesures i processos.

- En cas de no haver-se definit responsabilitats al nivell directiu adequat, existeix un risc que les necessitats, respecte a la seguretat de la informació identificades pels seus responsables, no siguen degudament ateses per l'organització.

- No s'assegura que hi haja mecanismes que independitzen les mesures i processos de seguretat de les persones encarregades de gestionar-les, de manera que existeix un risc que, davant determinades absències, les mesures de seguretat no siguen aplicades.

Per tant, podem concloure que una governança adequadament establida proporciona a les entitats mecanismes que garanteixen que la seguretat és entesa com un sistema integrat i continuat, amb processos de gestió que vetlen per l'eficàcia de les mesures i

processos de seguretat. La inexistència d'aquest marc de governança, independentment dels esforços i recursos dedicats a la seguretat, impedeix assegurar la seua eficàcia i idoneïtat.

3. RESPONSABLES DE L'ESTABLIMENT D'UNA ADEQUADA GOVERNANÇA DE CIBERSEGURETAT

L'estructura organitzativa i les responsabilitats que habiliten l'existència d'una adequada governança han sigut descrites, a més dels documents citats en l'apartat anterior, en el *Prontuario de ciberseguridad para entidades locales*, elaborat de manera conjunta pel CCN i la Federació Espanyola de Municipis i Províncies.

Encara que les responsabilitats relacionades amb la governança es troben distribuïdes entre diferents agents implicats, amb diferents nivells de responsabilitat i atribucions, **la responsabilitat d'establir una adequada governança de la ciberseguretat** per mitjà de l'aprovació de les polítiques de seguretat de la informació, d'acord amb l'article 11 del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS-2010), **és del titular de l'òrgan superior corresponent**.

En les entitats locals, aquesta responsabilitat principal recau en el president o presidenta. Són els responsables de garantir que el funcionament de l'organització resulta conforme amb les normes aplicables i que hi ha uns controls adequats sobre els sistemes d'informació i les comunicacions. Són els màxims responsables de la implantació de l'ENS.

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.[8]

No obstant això, en la pràctica, de manera general, les administracions locals han assumit de manera errònia que la responsabilitat de la seguretat de la informació i els serveis, materialitzada en el compliment de l'Esquema Nacional de Seguretat, recau en exclusiva sobre els responsables de les àrees informàtiques i tecnològiques, incorrent en **un greu error de criteri** que menyscaba la ciberresiliència de les institucions.

Els responsables de les àrees informàtiques ja assumeixen la responsabilitat de la gestió dels sistemes, que és **incompatible** amb la responsabilitat sobre la seguretat de la informació (article 10 de l'ENS-2010 i article 11 de l'ENS-2022).

La responsabilitat de l'execució de les activitats establides per l'alta direcció correspon a la direcció executiva. En aquest grup, a l'efecte d'aquest informe, s'inclou el regidor responsable dels sistemes d'informació i les comunicacions, el secretari general, l'interventor general, el tresorer, els funcionaris directors del departament TIC i els caps d'àrea o servei.

[8] *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.

4. ELEMENTS DE LA GOVERNANÇA DE LA CIBERSEGURETAT

Per a aconseguir implantar un sistema de prevenció proactiva de ciberseguretat, les organitzacions han d'establir un marc de governança, en el qual es designe els responsables en la matèria i les seues funcions, i descriure els processos de gestió relacionats amb la ciberseguretat.[9]

D'acord amb aquest marc i l'experiència de la Sindicatura en les auditories de ciberseguretat, hi ha una sèrie d'elements que o bé són components essencials de la governança o són condicions imprescindibles per al seu bon funcionament.

La relació d'aquests elements essencials és la següent:

- **Els òrgans superiors de l'entitat han d'exercir lideratge i compromís** respecte a la seguretat de la informació i han de vetlar perquè se satisfacen totes les necessitats i condicions necessàries per a l'establiment d'una governança adequada.

- 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 corresponent**, és a dir, pel president de l'entitat. Aquesta PSI ha de ser difosa entre la totalitat dels membres de l'organització.

- Ha d'existir una **planificació estratègica en matèria de ciberseguretat**, que proporcione un marc d'actuació a mitjà termini que assegure l'atenció a les necessitats prioritàries respecte a la seguretat, i es trobe alineada amb l'estratègia corporativa. La planificació estratègica de la seguretat evita una gestió reactiva basada principalment en necessitats sobrevingudes.

- Ha d'existir un **comité de seguretat TIC** amb un funcionament efectiu.

- Les entitats han d'assignar **rols i responsabilitats en matèria de seguretat de la informació**.

- L'entitat ha de **disposar dels recursos materials i humans** adequats per a atendre les necessitats identificades i implementar les mesures de seguretat necessàries.

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

- Han d'existir **normes i procediments de seguretat formalitzats i degudament aprovats**.

- El conjunt de processos implantats per a la gestió de la seguretat ha de constituir un **sistema de gestió de la seguretat de la informació (SGSI)**, que tracte la seguretat

[9] *Aproximación al marco de gobernanza de la ciberseguridad*, CCN 2022.

de manera continuada i proactiva, i que abaste totes les fases del procés de seguretat: conéixer, avaluar i tractar els riscos i establir les mesures de seguretat necessàries.

- S'ha d'establir una **cultura en matèria de ciberseguretat** que afecte tots els nivells de l'organització.

  Aquesta cultura de ciberseguretat ha de ser impulsada per la direcció en forma de plans estratègics que definisquen objectius i mesures concretes, a més d'incloure **plans periòdics de formació i conscienciació** dels treballadors.

Encara que l'absència d'algun d'aquests elements no implica necessàriament la falta d'efectivitat de les mesures de seguretat que es troben implantades en les entitats, la falta d'una correcta organització de la ciberseguretat impedirà assegurar que l'efectivitat es mantindrà al llarg del temps, independentment de les circumstàncies i condicionants existents. En els apartats següents es desenvolupen amb major detall aquests aspectes.

5. EL COMITÉ DE SEGURETAT TIC

Què és el comité de seguretat TIC o comité de seguretat de la informació

La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC[10] o comité de seguretat de la informació (CSI), que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat. 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 estructura i composició ha de constar en la PSI.

El CSI és l'òrgan especialitzat i permanent d'una organització per a la ciberseguretat i està integrat per aquelles persones de l'organització amb responsabilitat en la presa de decisions en matèria de seguretat i privacitat de la informació, així com per aquelles designades en representació d'altres òrgans o comités. Pot integrar vocals d'altres àrees de l'entitat que siguen rellevants per a la finalitat del comité, com ara la persona designada com a delegat de protecció de dades o del departament jurídic o de recursos humans, entre altres.[11]

Consideracions generals

D'acord amb el que es disposa en l'ENS, amb els criteris generals exposats en les guies del CCN i amb les diferents situacions observades en les nostres auditories, considerem que s'han de tindre en compte les consideracions següents, tant en definir la composició del CSI com en el seu funcionament:

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

[11] Apartat 5.1 d'*Aproximación al marco de gobernanza de la ciberseguridad. Año 2022*, CCN.

- **No és un comité merament tècnic**, sinó que ha d'integrar vocals de qualsevol àrea significativa necessària per a dur a terme els seus objectius.

- Ha de ser un **òrgan amb poder de decisió, àgil en la presa de decisions**.

  Un comité sense poder de decisió pot resultar inefectiu. Per aquest motiu es requereix que l'òrgan compte amb integrants del nivell més alt de les organitzacions, a més de comptar amb el suport necessari per a implantar totes les decisions i acords que es prenguen en les reunions.

- Ha de **reunir-se periòdicament** a fi de conéixer l'estat de la seguretat de la informació de l'entitat i prendre les decisions pertinents de manera oportuna.

  En algunes de les entitats auditades hem observat una baixa o nul·la activitat del comité, a pesar d'estar constituït formalment, la qual cosa és equivalent a la seua no existència. En entitats de grans dimensions i atesa la complexitat que presenten els seus sistemes d'informació, el comité hauria de reunir-se normalment una vegada al mes.

- **El personal amb rols assignats en matèria de seguretat de la informació o protecció de dades ha de disposar del temps suficient de dedicació a la seguretat** per a exercir les seues funcions de manera efectiva.

- **Ha de comprendre tots els sistemes d'informació de l'entitat.**

  En el curs de les nostres auditories als ajuntaments hem constatat que, en general, els **departaments de policia municipal** gestionen de forma quasi totalment independent els seus propis sistemes d'informació, sense integrar-se en molts casos en el marc general de ciberseguretat de l'ajuntament. A més, resulta habitual que, per a determinats **sistemes crítics** de l'entitat, la contractació, el desenvolupament i el manteniment d'aquests siga efectuat pels **departaments o serveis responsables de la seua explotació** i no pel departament TIC.

  No és la nostra tasca definir com han d'estar organitzats en un ajuntament els seus sistemes d'informació, ni si els sistemes policials i altres sistemes crítics han d'estar totalment integrats amb els sistemes corporatius o és millor que estiguen totalment separats. Aquesta és una decisió organitzativa de la corporació.

  Qualsevol que siga la fórmula triada, el marc de ciberseguretat ha de ser únic. Això vol dir que pot haver-hi un únic responsable de seguretat de la informació amb responsabilitats en el conjunt de sistemes d'informació de l'ajuntament. O pot haver-hi un responsable de la seguretat de la informació dels sistemes d'informació policials i/o sistemes crítics, però en aquest cas hauran d'estar integrats també en el CSI perquè siguen copartícips i corresponsables de les decisions que s'adopten.

  El comité de seguretat de la informació ha d'exercir les seues competències sobre tots els sistemes de l'entitat sense excepcions, inclosos aquells que per la seua naturalesa són gestionats directament pels serveis que exploten aquests sistemes.

Components

La guia CCN-STIC 201 indica que serà cada administració la que establisca la composició del seu CSI en funció de les seues competències, estructura i circumstàncies, deixant a les administracions la decisió d'establir els components d'aquest òrgan. No obstant això, les guies del CCN estableixen una sèrie d'orientacions sobre la seua composició i les responsabilitats dels seus membres.

Atenent el que estableix el CCN i l'experiència obtinguda en les nostres auditories, considerem que els integrants del CSI haurien de ser, almenys, els següents:

- **El president** del comité ha de ser el **regidor o diputat responsable** en matèria TIC.
- Responsable de seguretat de la informació, que exercirà de secretari del CSI.
- Responsable de la informació.
- Responsable del sistema.
- Responsable de seguretat física (RSF).
- Delegat de protecció de dades (DPD).
- Responsable del compliment legal.

Considerem imprescindible la participació en el comité de seguretat dels **secretaris generals**, atés que sobre ells recau la responsabilitat sobre l'execució de moltes decisions del comité. Pot exercir el rol de responsable de seguretat.

El comité pot constituir-se amb membres fixos i altres opcionals, per la qual cosa, a més dels exposats, podrà convidar-se a intervindre en les reunions totes les persones que siguen necessàries d'acord amb els assumptes a tractar.

La composició del CSI ha de constar en la PSI i els seus membres designats per l'òrgan superior de l'entitat.

6. ROLS EN MATÈRIA DE SEGURETAT DE LA INFORMACIÓ

L'ENS estableix que la PSI ha d'identificar de manera inequívoca els responsables de vetlar pel seu compliment, els quals tenen les funcions següents:

a) El **responsable de la informació** determina els requisits de la informació tractada.

b) El **responsable del servei** determina els requisits dels serveis prestats.

c) El **responsable de la seguretat** determina les decisions per a satisfer els requisits de seguretat de la informació i dels serveis, supervisa la implantació de les mesures necessàries per a garantir que se satisfan els requisits i reporta sobre aquestes qüestions.

d) El **responsable del sistema**, que s'encarrega de desenvolupar la forma concreta d'implementar la seguretat en el sistema i de la supervisió de l'operació diària d'aquest.

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

Les característiques dels rols i les seues responsabilitats en matèria de ciberseguretat es detallen en la *Guía de seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad. Responsabilidades y funciones*, a més de ser una qüestió abordada per diversos documents i guies del Centre Criptològic Nacional. L'objecte d'aquest apartat no és definir aquests rols i responsabilitats, sinó exposar les bones pràctiques i errors que hem vist durant les nostres auditories.

Consideracions generals

Per a una correcta organització de la seguretat de la informació, les entitats, tal com estableix la normativa i s'ha assenyalat anteriorment, han de nomenar determinats rols i aquests han d'assumir certes responsabilitats. Sobre aquest tema i segons el nostre criteri, són importants les consideracions següents:

- **Que els rols en matèria de seguretat siguen formalment establits.**

  Els rols en matèria de ciberseguretat han de ser formalment assumits per persones o òrgans segons s'establisca en la política de seguretat de la informació.

- **Que els rols establits exercisquen les seues funcions de manera efectiva.**

  La mera designació de rols per a complir la normativa no és suficient. Les organitzacions han de garantir que les persones amb rols establits en matèria de seguretat de la informació i protecció de dades de caràcter personal **tinguen la disponibilitat de temps necessària per a fer les seues tasques** de manera efectiva.

  La dedicació compartida entre múltiples tasques i competències o l'existència de múltiples tasques assignades a una mateixa persona poden originar riscos com la falta de dedicació a la matèria en qüestió o el conflicte entre prioritats de les seues diferents responsabilitats.

- **Que els rols estiguen correctament assignats, sense existir incompatibilitats amb altres competències.**

  Els documents i guies del CCN ens descriuen algunes incompatibilitats legals per a evitar conflictes d'interessos. Addicionalment, hi ha rols que han de realitzar les seues funcions amb independència, de manera transversal a tota l'organització.

Responsable de seguretat de la informació

El responsable de seguretat de la informació pot ser un càrrec unipersonal del nivell directiu de l'organització o un òrgan col·legiat. **No requereix desenvolupar funcions de**

caràcter tècnic, la seua funció és bàsicament supervisora del compliment efectiu de les decisions del CSI i de la normativa de seguretat.

En una entitat local, la màxima figura que coneix els serveis que presta l'entitat és el secretari o secretària general i, en conseqüència, està en millors condicions per a assumir el rol de responsable de la informació o nomenar algú que depenga directament d'aquest. És qui coneix millor tots els serveis oferits per l'organització i la seua importància i, amb això el nivell de seguretat requerit. Pot recolzar-se en totes les persones de la institució que considere oportú.

La *Guía de seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad Responsabilidades y funciones* estableix "que la figura del responsable de la seguretat ha d'estar situada en una posició que li permeta tindre un accés directe als nivells directius de l'organització". I a més indica que, "en el cas d'entitats locals (diputacions, consells insulars o ajuntaments), hauria de dependre del secretari general".

D'acord amb la guia CCN-STIC 201, el responsable de seguretat **ha de ser el secretari del Comité de Seguretat de la Informació**, i conseqüentment:

- Convoca les reunions del Comité de Seguretat de la Informació.
- Prepara els temes a tractar en les reunions del Comité, aportant informació puntual per a la presa de decisions.
- Elabora l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comité.

Responsable de seguretat física

Aquest rol assumeix la responsabilitat sobre la seguretat física de l'organització i seria l'enllaç amb el Comité de Seguretat Corporativa. Tant aquest comité com el CSI han d'estar degudament coordinats.

7. NORMATIVA INTERNA DE CIBERSEGURETAT

Un sistema de gestió continuada de la seguretat de la informació requereix que la PSI es complete amb normativa interna, desenvolupada en documents més precisos que materialitzen els requisits de la PSI (ús correcte d'equips, serveis, instal·lacions, usos indeguts, responsabilitats del personal); i un conjunt de procediments de seguretat que descriguen, pas a pas, com han de realitzar-se tasques concretes (documents que detallen com es fan les tasques habituals, responsables, report de comportaments anòmals).

És important diferenciar entre norma i procediment. Una norma o política (de l'anglés *policies)* indica "què ha de fer-se". Els procediments detallen les accions a realitzar, és a dir, el "com ha de fer-se" i, quan és el cas, qui ha de fer-ho.

Aquesta normativa interna ha de dissenyar-se per a ser aplicada, no per a complir una mera formalitat. El contingut del conjunt de polítiques, normes i procediments aprovats ha de ser

una representació fidedigna i precisa del sistema de seguretat implantat per l'ens local. L'aprovació d'un marc normatiu que no represente la realitat de l'ens esdevé un ús estèril de recursos per la seua falta d'efectivitat i una falsa percepció de compliment que pot comportar l'abandó d'altres mesures més adequades.

Cada entitat ha d'establir i aprovar la seua pròpia organització de seguretat, d'acord amb la seua naturalesa, estructura, dimensió i recursos disponibles, que haurà d'estar recollida en la seua política de seguretat de la informació.[12]

És important tindre en compte que, independentment del model organitzatiu existent en una entitat, tota la normativa de ciberseguretat afecta, sense excepció, tots els departaments i sistemes d'informació. L'organització de la seguretat, siga la que siga, ha d'estar definida en la PSI aprovada per l'òrgan superior i ha d'incloure tots els sistemes d'informació sense cap excepció.

Política de seguretat de la informació

La política de seguretat de la informació (PSI) és un document d'alt nivell que defineix, d'acord amb l'article 12 de l'ENS (2022), el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta. Constitueix l'expressió formal del compromís i lideratge de l'alta direcció amb la seguretat.

L'ENS indica els principis bàsics i els requisits mínims de la PSI. A més, hi ha alguns aspectes que les organitzacions han de tindre en compte, com ara:

- Ha de ser elaborada pel CSI i aprovada pel president de l'ens local.
- Que siga un document breu, que deixe detalls tècnics per a les normes que la despleguen.
- Ha de ser revisada i actualitzada periòdicament.
- Ha de ser accessible (publicada i donada a conéixer) als empleats i col·laboradors de l'organització.

Normativa de seguretat

Es disposarà d'una sèrie de documents que descriguen:

- L'ús correcte d'equips, serveis i instal·lacions, així com el que es considerarà ús indegut.
- La responsabilitat del personal respecte al compliment o violació de la normativa: drets, deures i mesures disciplinàries d'acord amb la legislació vigent.

[12] *CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones.*

Aquesta normativa haurà de ser aprovada per qui es dispose en la PSI. És de caràcter obligatori i haurà d'estar a la disposició de tots els membres de l'organització (publicada en la intranet corporativa).

Procediments de seguretat

Les entitats han de disposar d'un conjunt de procediments aprovats que detallen de manera clara i precisa com operar els elements del sistema d'informació:

- Com dur a terme les tasques habituals.
- Qui ha de fer cada tasca.
- Com identificar i reportar comportaments anòmals.
- La forma en què s'ha de tractar la informació en consideració al nivell de seguretat que requereix,

Els procediments hauran de ser aprovats per qui es dispose en la PSI.

8. ALTRES ÒRGANS DE GOVERN RELACIONATS AMB LA GESTIÓ DE LA CIBERSEGURETAT

Les organitzacions, depenent de la seua grandària i complexitat, poden disposar, a més del CSI, de diversos òrgans de govern relacionats amb la gestió de la ciberseguretat, que poden administrar funcions a diferents nivells, incloent-hi l'operatiu, l'executiu/supervisió o el de govern. Alguns d'aquests òrgans poden ser:

- El comité de seguretat corporativa.
- El comité de governança TIC
- El comité de gestió de crisis.
- El comité de seguretat física.
- El comité de protecció de dades.
- El centre d'operacions de seguretat.
- L'oficina de governança i compliment normatiu.

L'existència d'aquests òrgans respon, en general, a les exigències de la normativa bàsica d'aplicació, l'Esquema Nacional de Seguretat i la Llei Orgànica de Protecció de Dades. No obstant això, pot ser també d'aplicació una altra legislació sectorial i específica, com la de la Llei de Protecció d'Infraestructures Crítiques (Llei PIC8/2011), que estableixen els seus propis requisits de seguretat addicionals, incloent-hi mesures organitzatives.

Encara que l'existència d'aquests òrgans pot no ser obligatòria en totes les circumstàncies, depenent de la legislació que siga aplicable en cada cas, sí que resulta **imprescindible que**, en cas d'existir, el **conjunt d'aquests òrgans coordine adequadament les seues activitats i que hi haja mecanismes de comunicació i col·laboració** entre aquests.

Encara que la revisió d'aquests òrgans no estava inclosa en l'abast de les auditories dels CBCS, per la seua important relació realitzem a continuació alguns comentaris sobre ells.

Comité de governança TIC

És l'òrgan col·legiat encarregat de la definició i supervisió de l'estratègia sobre les TIC en una entitat, que hauria d'aprovar la Junta de Govern. La definició de la composició i funcions d'aquest comité correspon a aquest òrgan superior; no obstant això, ha d'haver-hi algun membre comú amb el CSI (com per exemple el responsable del sistema) de manera que les seues activitats siguen coherents.

S'entén per govern o governança TIC el conjunt d'accions que realitza l'àrea de TI en coordinació amb l'alta direcció per a mobilitzar els seus recursos de la forma més eficient en resposta a requisits reguladors, operatius o del negoci. Constitueix una part essencial del govern de l'entitat en el seu conjunt i aglutina l'estructura organitzativa i directiva necessària per a assegurar que les TIC suporten i faciliten el desenvolupament dels objectius estratègics definits. Això garanteix que:

- Les TIC estan alineades amb l'estratègia del negoci.
- Els serveis i funcions de TI es proporcionen amb el màxim valor possible o de la forma més eficient.
- Tots els riscos relacionats amb TI són coneguts i administrats i els recursos de TI estan segurs, incloent-hi els relacionats amb la ciberseguretat per mitjà de la coordinació amb el CSI.

En les entitats de grandària xicoteta el comité de governança TIC i el de ciberseguretat poden confluir en un d'únic.

Comité de gestió de crisis

Un ciberincident greu provocarà una crisi i això implica la necessitat de prendre decisions sota molta pressió, en poc de temps i amb informació probablement incompleta.

Amb independència del tipus de ciberincident que cause la crisi, es fa patent la component de gestió que implica la seua resolució. Per a això, l'organització afectada necessita haver-se dotat de les capacitats i estructures de gestió (comités/equips) adequades que li han de permetre abordar-la amb garanties d'èxit.

En resum, la capacitat de gestionar una situació de crisi depén en gran manera de les estructures o comités que s'hagen establit abans que ocórrega el desastre causat per un ciberincident, succés de "baixa probabilitat i alt impacte".

El comité de crisis és l'òrgan encarregat de la gestió de la crisi a alt nivell dins de l'organització, amb una visió estratègica. S'encarregarà de prendre les decisions i coordinar les accions necessàries per a la resolució dels incidents que hagen sigut qualificats de crisis dins de l'entitat, determinant i/o validant les estratègies d'anàlisi, de contenció i mitigació que permeten recuperar les operacions en el menor temps possible, minimitzant els impactes sobre les parts interessades.

Encara que la revisió dels diversos aspectes relacionats amb la gestió i els comités de crisis han quedat fora de l'abast de les nostres auditories, recomanem que s'analitzen tots els aspectes relacionats amb la gestió de les crisis provocades per ciberincidents de manera coordinada amb el CSI.

Centres d'operacions de ciberseguretat

D'acord amb la guia CCN-STIC 201, la governança de la seguretat en una organització s'articula a través d'un comité de seguretat TIC i s'implementa per mitjà de centres d'operacions de ciberseguretat que vetlen per l'operació i correcta implementació de la seguretat, per mitjà d'una vigilància contínua dels sistemes d'informació

Sota la direcció del responsable de seguretat, el centre d'operacions de ciberseguretat presta serveis de ciberseguretat i desenvolupa la capacitat de vigilància i detecció d'amenaces en l'operació diària dels sistemes TIC, especialment els que manegen informació classificada, alhora que millora la capacitat de resposta del sistema davant qualsevol atac.

En definitiva, els centres d'operacions de ciberseguretat han d'articular la resposta als incidents de seguretat, sense perjudici de les capacitats de resposta a incidents de seguretat que puga tindre cada administració amb competències i de la funció de coordinació del CSIRT-CV de referència i del CCN-CERT, com a coordinador nacional.

Així mateix, en funció de la naturalesa i dimensions de l'organització, el centre d'operacions de ciberseguretat pot ser intern o estar externalitzat, i en aquest cas actuarà remotament a través de canals establits en coordinació amb el responsable de seguretat.

Equip de resposta a incidents de seguretat

Aquest equip s'encarrega de gestionar els incidents de seguretat sota les directrius marcades pel CSI i el responsable de seguretat i possibles alertes rebudes del centre d'operacions de ciberseguretat.

Està compost per un equip amb capacitats d'atenció immediata denominat "primer nivell d'atenció" i per un grup d'especialistes per a aquells incidents no resolts pel primer nivell que requerisquen un major grau d'especialització.

9. PRINCIPALS DEFICIÈNCIES EN MATÈRIA DE GOVERNANÇA OBSERVADES EN LES NOSTRES AUDITORIES

En cada un dels díhuit informes d'auditoria de ciberseguretat individuals realitzats hem indicat la situació quant a la governança i hem observat que les entitats, en general, no

tenen establida una adequada governança de la seguretat de la informació. A continuació, assenyalem les principals deficiències observades.

En matèria de normativa de seguretat

Una de les mancances generalitzades detectades és la falta d'un marc normatiu i procedimental de seguretat formalment aprovat. D'acord amb la definició dels nivells del model de maduresa establit pel CCN, per a aconseguir un nivell 3 de maduresa és requisit necessari l'existència de procediments formalment aprovats. Les deficiències en aquest aspecte impedeixen que els controls aconseguisquen nivells superiors al nivell 2, les més comunes de les quals són:

- Inexistència de PSI formalment aprovada per la corporació, o desactualitzada o no adaptada a la realitat de les entitats, la qual cosa impedeix que els principis que han de regir les actuacions en matèria de seguretat siguen coneguts per tota la corporació.

- Inexistència de normativa i procediments formalitzats, la qual cosa pot originar el risc de no realització de tasques importants per no estar assignades a responsables i que la seua execució depenga de la bona voluntat dels qui els duen a terme.

- El contingut dels procediments no detalla de manera clara i precisa les tasques que cal realitzar ni qui són els responsables d'executar-les, especificant únicament el deure de realitzar l'acció, aspecte que correspon a les normes de seguretat de rang superior, la qual cosa genera procediments ineficaços.

- Existència de procediments escrits que, encara que estan definits de manera correcta, han sigut realitzats per consultores externes i tenen poca o nul·la adaptació en l'entorn de l'entitat, atés que no reflectien la realitat de les accions dutes a terme en la pràctica.

- Els procediments existents, inclosos aquells formalment aprovats, no es troben actualitzats i no representen amb fidelitat els processos de seguretat que descriuen.

En relació amb el comité de seguretat de la informació

- Hi ha entitats que no disposen de comité de seguretat de la informació, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat.

- En altres casos, encara que el comité de seguretat de la informació està formalment constituït, no es reuneix o no ho fa amb la periodicitat necessària, la qual cosa impedeix fer un seguiment de l'estat de la seguretat de la informació i prendre les decisions pertinents de manera oportuna.

- El comité de seguretat no disposa dels membres adequats i està compost únicament de membres amb càrrecs relacionats amb els sistemes d'informació i la seguretat. La falta de membres amb el més alt poder de decisió en l'organització i de vocals de les àrees significatives converteix el comité en un òrgan merament tècnic i impedeix un govern eficient i la presa de decisions estratègiques d'àmbit corporatiu.

En relació amb els rols de seguretat

A més d'establir un marc normatiu i procedimental, les entitats han de nomenar els diferents rols en matèria de seguretat i assignar formalment responsabilitats a aquests rols. Les principals deficiències relacionades que hem advertit durant les auditories han sigut:

- Hi ha entitats que no han assignat els rols i responsabilitats en matèria de seguretat de la informació.

- Hi ha entitats que no disposen d'un delegat de protecció de dades formalment nomenat.

- Alguns dels rols de seguretat no exerceixen les seues funcions de manera que es garantisca la necessària independència i l'absència de conflicte d'interessos.

  - El responsable del departament TIC és el responsable de seguretat. D'acord amb l'ENS i la guia CCN-STIC 801, el responsable de la seguretat ha de ser una persona física, jeràrquicament independent del responsable del sistema. Si el responsable de seguretat està legitimat per a determinar, supervisar i pronunciar-se sobre la idoneïtat de les mesures de seguretat adoptades, aquest rol no pot recaure sobre la persona encarregada de la seua implantació i explotació diària.

  - Hem observat situacions en què els rols designats en matèria de seguretat de la informació (DPD i responsable de seguretat) estan assumits per personal extern que, encara que exerceixen les seues funcions de manera concorde a l'especificada en el contracte, aquests contractes són licitats pel departament TIC. Aquesta dependència en la contractació del departament TIC limita la capacitat operativa i de decisió dels serveis contractats, que haurien de ser promoguts des de secretaria general.

  - El DPD coincideix amb el responsable de seguretat. L'AEPD assenyala que "en aquelles organitzacions que, per la seua grandària i recursos, no pogueren observar aquesta separació, seria admissible [...] sempre que en aquesta concórreguen els requisits de formació i capacitació previstos en el RGPD. A més, resultaria imprescindible adoptar totes les mesures [...] que garantisquen la necessària independència i l'absència de conflicte d'interessos [...]".

  És a dir, **amb caràcter general els dos rols són incompatibles**.

- Alguns rols en matèria de seguretat no disposen de la dedicació suficient per a les necessitats d'una entitat de la grandària de les auditades. Els responsables de seguretat de manera general no exerceixen les seues funcions de manera exclusiva, de manera que incorren en una acumulació de competències no directament relacionades amb la seguretat de la informació que impedeix que desenvolupen les seues funcions de manera efectiva.

En relació amb el lideratge i el compromís amb la ciberseguretat

A més de les qüestions anteriors, per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació es requereix el lideratge, implicació, compromís i impuls de mesures per part dels òrgans superiors de l'ens local (en particular, el president i la junta de govern). D'aquests depén l'existència d'uns controls adequats sobre els sistemes d'informació i les comunicacions. En aquest aspecte, les principals deficiències que hem observat han sigut:

- Inexistència d'implicació dels màxims responsables de l'organització.

  Tal com s'ha indicat anteriorment, els òrgans superiors de les entitats són els **responsables** de la seguretat dels sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen el factor més important per a la implantació reeixida d'un SGSI. Aquest compromís també s'ha d'estendre a la direcció, que són els responsables d'articular i facilitar l'execució de les activitats en matèria de ciberseguretat.

  L'absència d'aquest lideratge té un efecte generalitzat sobre l'organització i gestió de la seguretat en l'organització.

- L'absència de plans estratègics desenvolupats i impulsats pel més alt nivell de la corporació en els quals s'establisquen accions, objectius i mesures concretes per a aconseguir els nivells de seguretat exigits per la normativa.

- La falta de recursos, tant econòmics com de personal, en els departaments TIC, indispensable per a implantar les mesures de seguretat necessàries i dur a terme projectes transversals que afecten tota l'organització.

- La falta d'una cultura de ciberseguretat en l'entitat, materialitzada en accions formatives i campanyes de conscienciació dirigides als empleats.

10. COORDINACIÓ I INTEGRACIÓ AMB ORGANISMES DE REFERÈNCIA

La majoria de les entitats auditades han participat en les activitats incloses en el Pla de Xoc de Ciberseguretat per a les Entitats Locals de la Comunitat Valenciana, promogut per la Direcció General de Tecnologies de la Informació i les Comunicacions (DGTIC) de la GVA.

Entre les activitats d'aquest pla, es troba el desplegament de diverses de les eines oferides pel CSIRT-CV o el CCN. Aquesta és una de les millors pràctiques observades en les entitats auditades.

Adherir-se als serveis que proporcionen els organismes referents en matèria de seguretat aporta molts avantatges, entre els quals destaquem:

- La gestió d'incidents: vigilància, sistema d'alertes i suport per a la detecció i tractament de les amenaces detectades.

- Participació en aquelles accions proposades pel pla de xoc de ciberseguretat per a les entitats locals, que la Generalitat Valenciana ha posat a la disposició dels ajuntaments de més grandària, que comporten, entre altres, monitoratge i anàlisi d'esdeveniments, emissió d'informes, suport, etc.

- Assessorament tècnic en la implantació de mesures de seguretat, materialitzat en accions com les recomanacions rebudes de part del CSIRT-CV per a la maquetació de llocs de treball durant la pandèmia.

A més de les tasques de col·laboració amb els organismes de referència, aquests posen a la disposició de les entitats un conjunt d'eines en matèria de ciberseguretat que, d'acord amb el que s'ha observat, han tingut una acollida molt positiva entre les entitats.

La llista següent mostra les eines que hem observat desplegades en algunes de les organitzacions auditades:

- LUCIA (Llistat Unificat de Coordinació d'Incidents i Amenaces), eina per a la gestió de ciberincidents en les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat.

- CARMEN, solució desenvolupada amb l'objectiu d'identificar el compromís de la xarxa d'una organització per part d'amenaces persistents avançades. Eina en fase d'implantació a data 31 de desembre de 2021 però implantada íntegrament a data d'aquest informe.

- CLAUDIA, solució d'*endpoint* integrada amb l'eina CARMEN que permet tindre una visió més completa del que ocorre dins d'una xarxa.

- GLORIA, plataforma per a la gestió d'incidents i amenaces de ciberseguretat a través de tècniques de correlació complexa d'esdeveniments (SIEM).

- SAT-INET (Sistema d'Alerta Primerenca d'Internet), servei desenvolupat i implantat per l'Equip de Resposta davant Incidents de Seguretat de la Informació del Centre Criptològic Nacional (CCN-CERT) per a la detecció en temps real de les amenaces i incidents.

- microCLAUDIA, que proporciona protecció contra codi nociu de tipus *ransomware*.

- REYES, que permet realitzar investigació i anàlisi sobre ciberincidents de manera àgil i ràpida. Consisteix en un metacercador d'informació de diverses fonts especialitzades en ciberamenaces, que està integrat amb eines d'anàlisi del CCN-CERT. Les entitats reben informes periòdics del CSIRT-CV amb incidents de seguretat relacionats amb els dominis i correus corporatius (vigilància digital).

APÈNDIX 3

Situació dels controls bàsics de ciberseguretat

1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS (CBCS 1)

Objectiu del control

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

Per què és important aquest control de ciberseguretat

La finalitat del control és conéixer el que està connectat a la xarxa perquè puga ser defensat i, posteriorment, impedir que dispositius no autoritzats es connecten a la xarxa. Aquest control ajuda les organitzacions a definir la base del que cal defensar, ja que, si es desconeix quins dispositius estan connectats, no poden ser defensats.

L'òrgan competent ha d'aprovar formalment un procediment que especifique les accions a realitzar per a mantindre actualitzat l'inventari de tot el maquinari de l'entitat, que incloga també aspectes com la realització periòdica de revisions i la descripció de les mesures implantades per a impedir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

L'inventari ha de ser tan complet com siga possible. En organitzacions amb un nivell de maduresa bàsic l'inventari pot ser realitzat i mantingut amb procediments manuals i, en altres més madures, utilitzant eines d'escaneig que detecten els dispositius connectats a la xarxa corporativa.

Ha d'existir en tota la xarxa corporativa un control efectiu que impedisca accedir-hi a qualsevol dispositiu físic no autoritzat. És més probable que les màquines no controlades estiguen executant programari que no siga necessari per als fins de l'entitat (introduint possibles vulnerabilitats de seguretat), o executant *malware* introduït per un atacant després que un sistema ha sigut compromés.

Altres dispositius que es connecten a la xarxa corporativa (per exemple, sistemes per a demostracions, xarxes per a convidats, etc.) han de ser gestionats amb cura o aïllats per a previndre accessos no autoritzats que comprometen la seguretat.

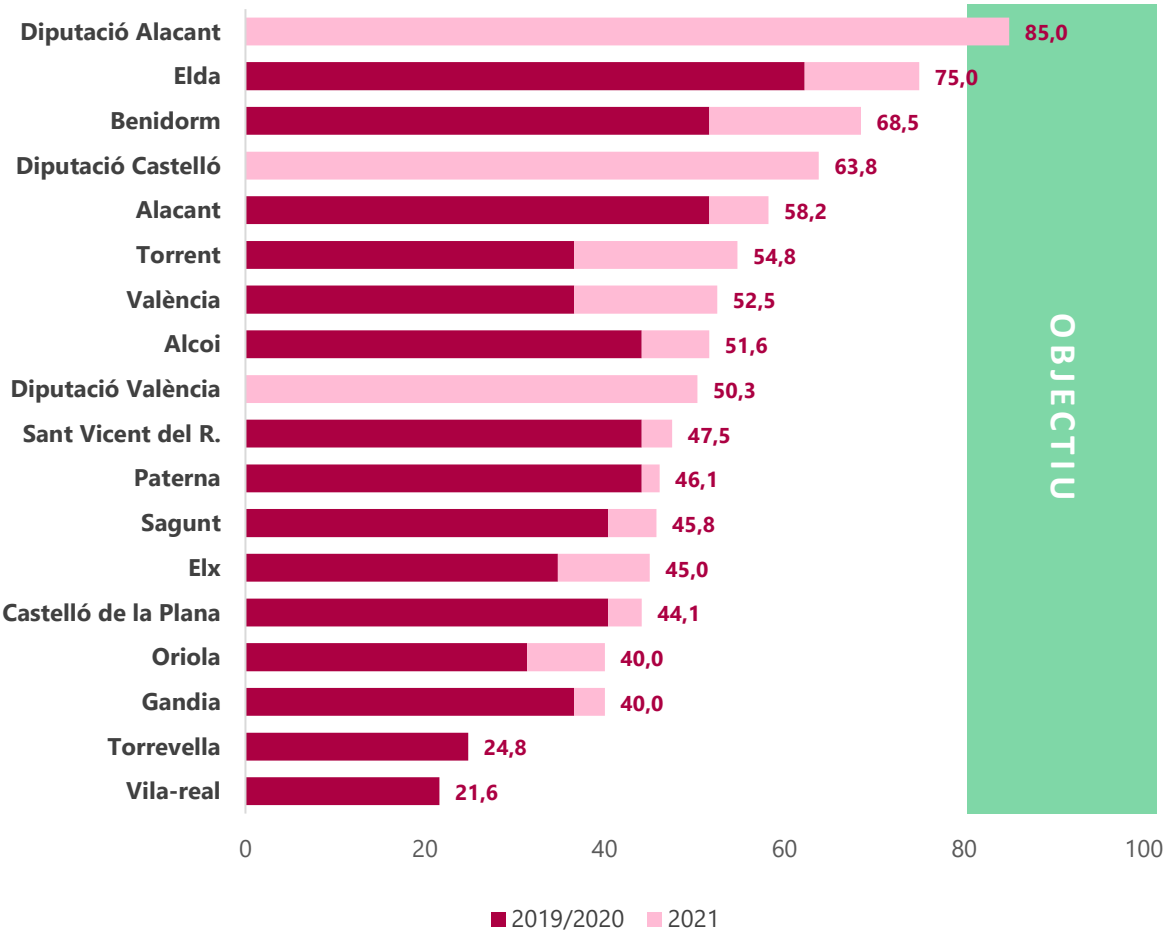
Els dispositius personals dels empleats (portàtils, tauletes, mòbils) que es connecten a la xarxa corporativa també es poden veure compromesos i ser usats per a infectar els recursos interns.

Situació de l'índex de maduresa del control

El gràfic 6 següent mostra l'índex de maduresa del CBCS 1 que els quinze ajuntaments van obtindre en les nostres auditories inicials en 2019/2020 i la millora que han experimentat fins al 31 de desembre de 2021 i que fa una mitjana del 47,7%.

També s'hi inclou la situació del control en les diputacions a 30 de setembre de 2021, que obtenen un índex de maduresa mitjà del 66,3%. Únicament la Diputació d'Alacant aconsegueix el nivell de maduresa exigit en l'ENS.

Gràfic 6. Índex de maduresa del CBCS 1 per entitat



S'observa que quasi totes les entitats, exceptuant dos ajuntaments, han realitzat accions que milloren els índexs de maduresa previs. No obstant això, la millora, en general, no és suficient per a aconseguir el nivell que exigeix l'ENS.

Situació dels subcontrols revisats

El CBCS 1 consta de dos subcontrols:

- CBCS 1.1: Inventari d'actius físics autoritzats
- CBCS 1.2: Control de dispositius físics no autoritzats.

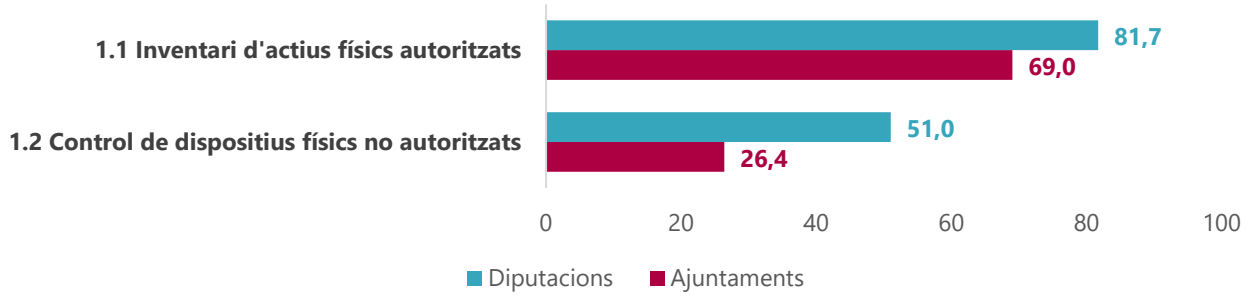
Si analitzem l'índex de maduresa mitjà per a cada un d'aquests subcontrols, s'observa:

- Els ajuntaments tenen cert control sobre els seus inventaris de maquinari (69,0%), però els mecanismes per a controlar l'accés de dispositius no autoritzats a les xarxes corporatives són, en general, inexistents o deficients.

- Les diputacions aconsegueixen, de mitjana, el nivell exigit per l'ENS per al control de l'inventari, però no l'aconsegueixen per al control de dispositius no autoritzats, encara que la Diputació d'Alacant sí que aconsegueix un índex de maduresa del 90% en aquest subcontrol.

De manera gràfica:

Gràfic 7. Índex mitjà de maduresa dels subcontrols del CBCS 1 en 2021



Per a esmenar les deficiències detectades i aconseguir un nivell acceptable d'efectivitat del control, les entitats han de mantindre l'inventari d'actius actualitzat, realitzar revisions periòdiques del maquinari i implantar solucions que permeten restringir l'accés de dispositius físics no autoritzats a les xarxes corporatives.

2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT (CBCS 2)

Objectiu del control

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

Per què és important aquest control bàsic de ciberseguretat

La finalitat d'aquest control és assegurar que només s'executa programari autoritzat en els sistemes de l'organització, impedint l'execució de programari no autoritzat o potencialment vulnerable.

Mantindre un inventari actualitzat de programari és important, ja que permet conéixer què cal protegir. Per exemple, el control de tot el programari existent exerceix un paper fonamental en la planificació i execució de còpies de seguretat i en la recuperació del sistema. Sense el coneixement o el control apropiats dels programes desplegats en una organització, els defensors no poden assegurar adequadament la seua protecció. Les organitzacions que no tenen inventaris complets de programari no poden trobar quin és el vulnerable o maliciós per a mitigar problemes o eliminar als atacants.

D'altra banda, disposar d'una llista blanca d'aplicacions autoritzades limita la capacitat d'executar únicament a aquelles que estan expressament autoritzades. Aquest control

sovint es considera un dels més eficaços per a la prevenció i detecció de ciberatacs. La implementació del control sovint requereix que les organitzacions reconsideren les seues polítiques i la seua cultura, ja que els usuaris ja no podran instal·lar el programari que desitgen.

L'aplicació de pedaços i actualitzacions en el programari inventariat i controlat permet a les entitats eliminar les vulnerabilitats o reduir els riscos derivats de la materialització de les amenaces. Perquè el procés d'actualització i pedaços siga possible, és necessari que l'entitat complisca els requisits següents: els programes utilitzats han de trobar-se en un estat del seu cicle de vida que permeta l'alliberament d'actualitzacions del fabricador, les llicències de programari comercial han de trobar-se actives, i aquell que ha sigut adaptat i implantat específicament per a l'entitat ha de trobar-se suportat per contractes de manteniment amb les empreses corresponents.

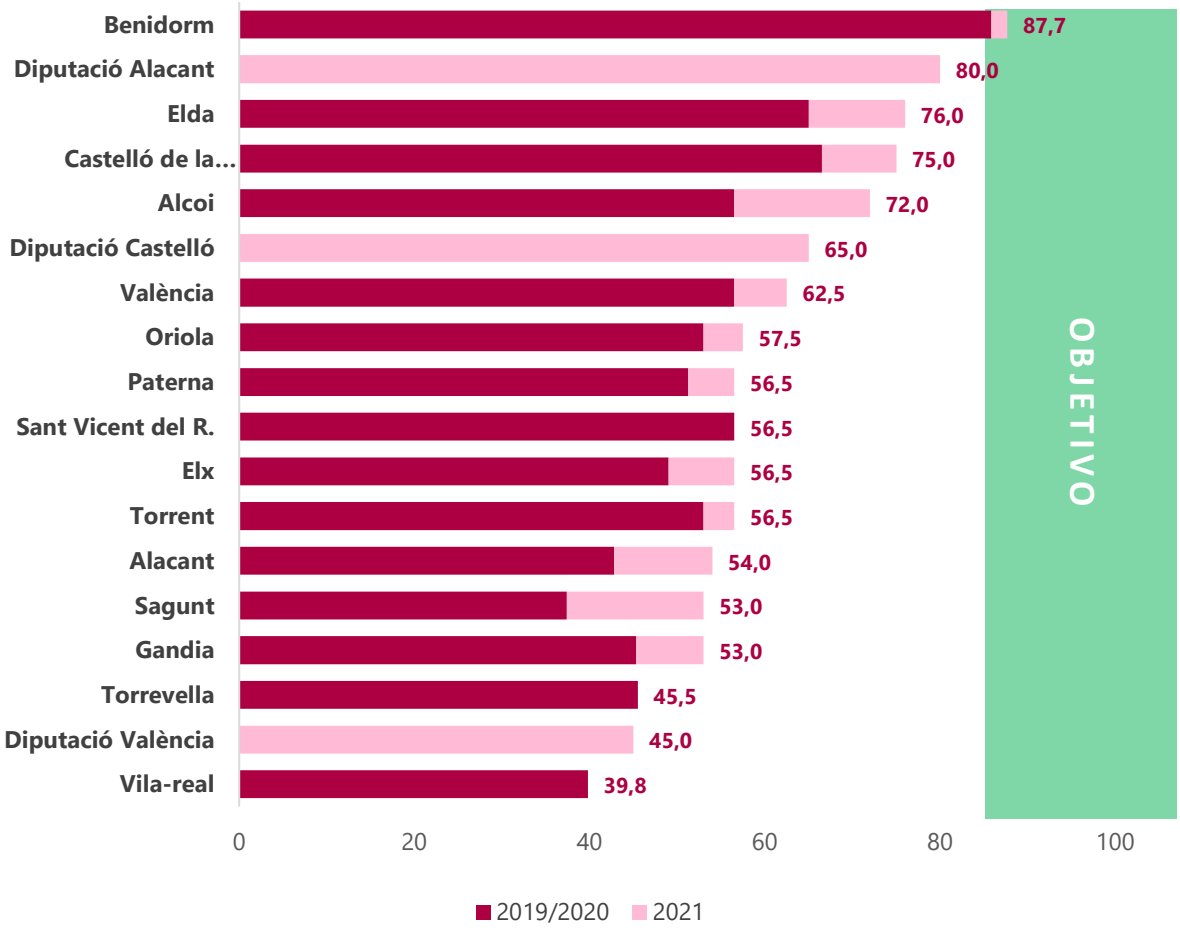
Les entitats han de disposar d'un procediment que descriga la gestió de l'inventari, que incloga totes les aplicacions i identifique els seus responsables. Addicionalment, es realitzaran revisions periòdiques dels programes, que hauran de ser documentades. L'efectivitat del control és producte d'un inventari de programari actualitzat, al costat d'una llista blanca d'aplicacions permeses i la implantació de les mesures necessàries per a bloquejar qualsevol aplicació no inclosa dins d'aquesta llista.

Situació de l'índex de maduresa del control

El gràfic següent mostra l'índex de maduresa del CBCS 2 que els quinze ajuntaments van obtindre en la nostra revisió inicial i la millora experimentada fins al 31 de desembre del 2021, que van obtindre un índex mitjà del 60,1%.

Les tres diputacions provincials van obtindre un índex de maduresa mitjà del 63,3%.

Gràfic 8. Índex de maduresa del CBCS 2 per entitat



S'observa que quasi tots els ajuntaments, exceptuant-ne dos, han realitzat accions que milloren els índexs de maduresa obtinguts en 2019/20. Únicament un dels ajuntaments auditats i una de les diputacions aconsegueixen el nivell que exigeix l'ENS.

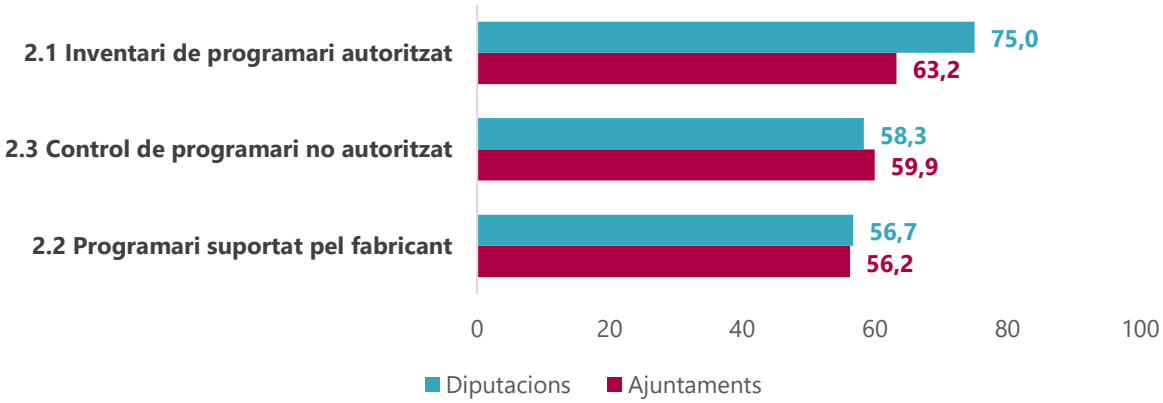
Situació dels subcontrols revisats

El CBCS 2 consta de tres subcontrols:

- CBCS 2.1: Inventari de programari autoritzat
- CBCS 2.2: Programari suportat pel fabricant
- CBCS 2.3: Control de programari no autoritzat

Si analitzem l'índex de maduresa mitjà per a cada un dels subcontrols s'observa que no n'hi ha cap que arribe, de mitjana, al nivell exigit per l'ENS, tal com es veu en el gràfic .

Gràfic 9. Índex mitjà de maduresa dels subcontrols del CBCS 2 en 2021



A més d'elaborar i aprovar formalment procediments que descriguen la gestió integral del programari de l'entitat i les mesures implantades, s'han de definir llistes blanques de programari autoritzat, el procés d'autorització per a la instal·lació de programari, la implantació de les mesures tècniques que impedisquen l'execució del programari no autoritzat i realitzar revisions periòdiques. Addicionalment, s'han de definir plans de manteniment de programari que consideren la totalitat d'aplicacions i revisar i actualitzar tots els sistemes que es troben fora del seu període de suport.

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

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.

Per què és important aquest control bàsic de ciberseguretat

La finalitat d'aquest control és conéixer i eliminar debilitats tècniques que existeixen en els sistemes d'informació de l'organització, reduint la probabilitat que els sistemes continuen sent vulnerables.

Les entitats han de comptar amb un pla de manteniment de l'equipament físic i lògic, que detalle els components a revisar i els responsables. S'especificarà el seguiment continu d'anuncis de defectes publicats pels fabricants i es documentaran les accions dutes a terme per a analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pedaços, millores i noves versions, tenint en compte el risc que pot implicar aquest canvi.

S'han d'implementar eines que centralitzen i automatitzen el procés de gestió de vulnerabilitats, actualitzacions i pedaços, per a dotar-se de la capacitat de detectar i remeiar debilitats de programari explotable. Ha de perseguir-se la detecció de vulnerabilitats de seguretat en els diferents sistemes de manera automàtica, contínua i proactiva, i facilitar la instal·lació d'actualitzacions i pedaços per a solucionar les vulnerabilitats existents. Si això

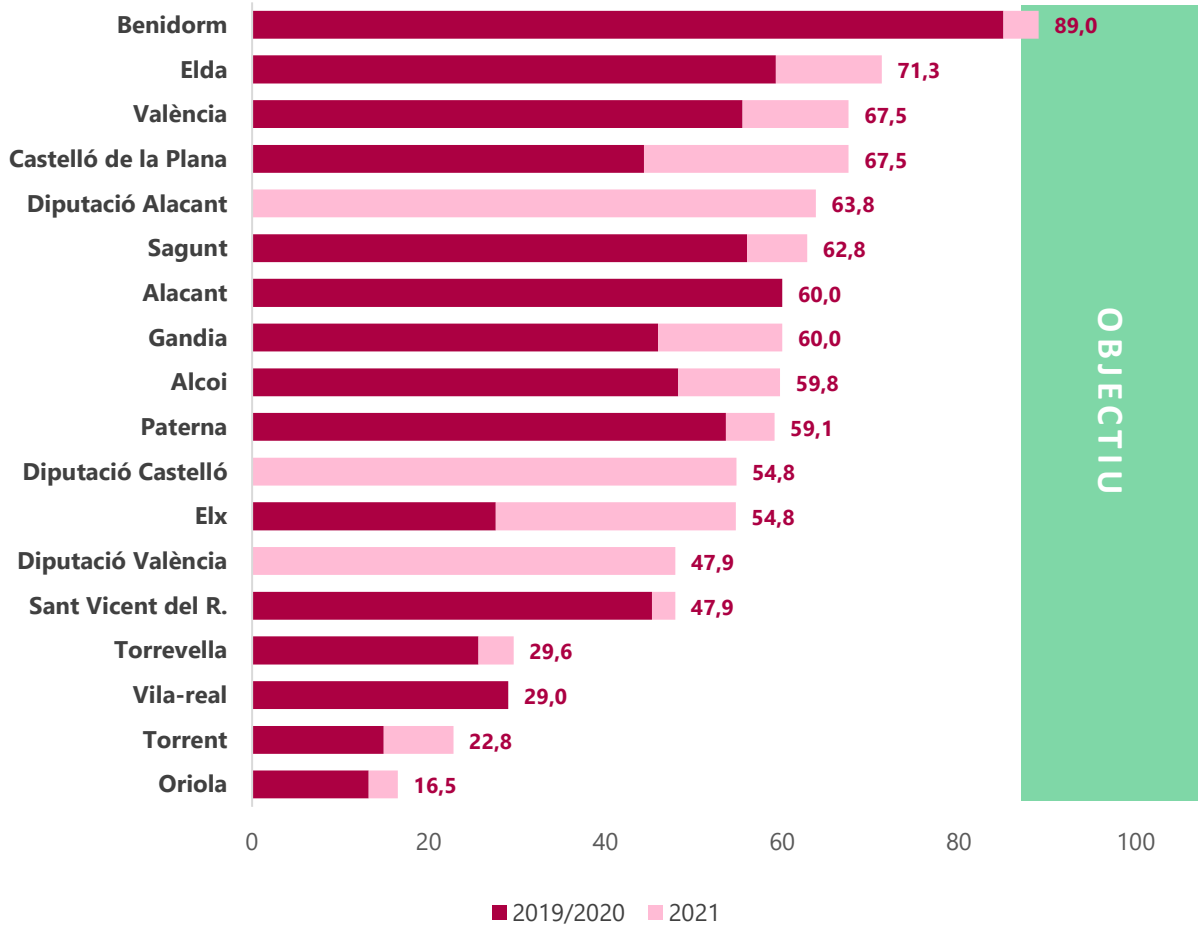
no es fa existirà una alta probabilitat que els seus sistemes informàtics siguen compromesos.

Els ciberdefensors han d'operar amb un flux constant d'informació: actualitzacions de programes, pedaços, avisos de seguretat, butlletins d'amenaces, etc. La comprensió i gestió de les vulnerabilitats és una activitat contínua, que requereix temps, atenció i recursos significatius. Els atacants tenen accés a la mateixa informació i poden aprofitar les bretxes entre l'aparició de nous coneixements i la seua solució. Per exemple, quan els investigadors reporten noves vulnerabilitats, comença una carrera entre totes les parts que inclou atacants (per a "armar-se", desplegar un atac i explotar-lo), proveïdors (per a desenvolupar, implementar pedaços o signatures i actualitzacions) i defensors (per a avaluar riscos, pedaços de prova i instal·lar-los).

Situació de l'índex de maduresa del control

El gràfic següent mostra l'índex de maduresa del CBCS 3 que les quinze entitats van obtindre en la nostra revisió inicial i la millora que han experimentat fins al 31 de desembre del 2021. S'hi afig també l'índex de maduresa de les tres diputacions.

Gràfic 10. Índex de maduresa del CBCS 3 per entitat



L'índex de maduresa mitjà ha sigut del 53,2% en els ajuntaments i del 55,5% en les diputacions.

Tots els ajuntaments han realitzat accions que milloren els índexs de maduresa obtinguts durant el nostre treball de 2019/20, però aquestes accions no són suficients per a aconseguir el nivell que s'exigeix en la normativa. Únicament Benidorm aconsegueix el nivell exigit sobre el control de vulnerabilitats.

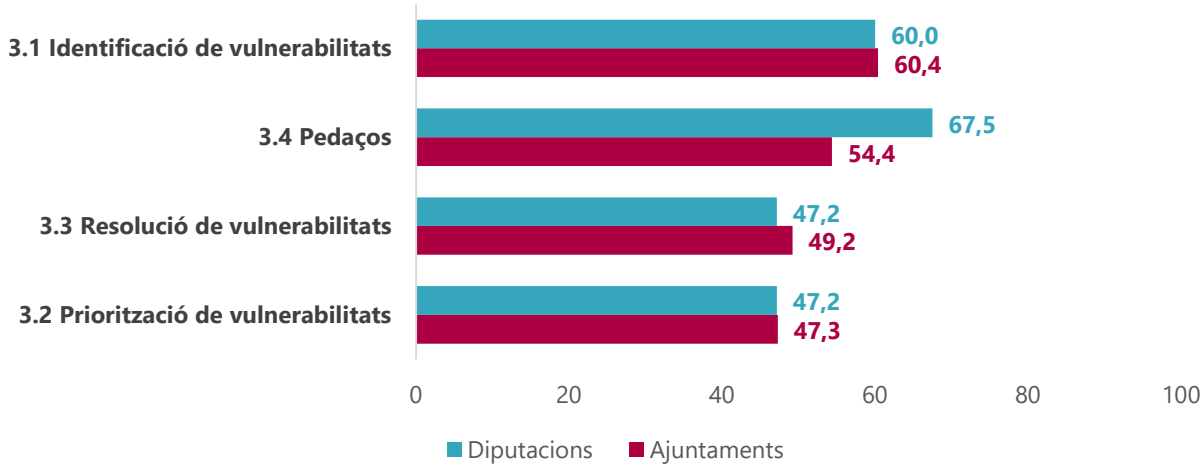
Situació dels subcontrols revisats

El CBCS 3 consta de quatre subcontrols:

- CBCS 3.1: Identificació de vulnerabilitats
- CBCS 3.2: Priorització de vulnerabilitats
- CBCS 3.3: Resolució de vulnerabilitats
- CBCS 3.4: Pedaços

Si analitzem l'índex de maduresa mitjà per a cada un dels subcontrols s'observa que, en general, els mecanismes de control implantats per a la gestió de vulnerabilitats no aconsegueixen el nivell d'eficàcia necessari.

Gràfic 11. Índex mitjà de maduresa dels subcontrols del CBCS 3 en 2021



Per a implantar un control efectiu d'identificació i solució de vulnerabilitats, les entitats han de definir els sistemes a revisar, la periodicitat de les revisions, l'anàlisi de sistemes prèvia a l'entrada en producció, el seguiment d'anuncis de fabricants i butlletins oficials en matèria de seguretat, la priorització de resolucions basada en l'anàlisi de riscos i la documentació de les vulnerabilitats tractades.

4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS (CBCS 4)

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.

Per què és important aquest control bàsic de ciberseguretat

Aquest control garanteix que els privilegis d'administració dels sistemes estiguen assignats únicament als empleats que els necessiten, sobre la base de les funcions que exerceixen (principi de mínim privilegi) i que l'entitat puga atribuir les accions administratives a usuaris identificables (traçabilitat).

Desafortunadament, per a facilitar l'agilitat i la comoditat, moltes organitzacions permeten que el seu personal tinga drets d'administrador tant a nivell d'una aplicació de gestió com en els sistemes que li donen suport (sistema operatiu, base de dades, etc.), així com en els seus equips. Aquesta situació deriva en l'existència del risc d'accés i de canvis no autoritzats als sistemes i dades, que pot materialitzar-se utilitzant els privilegis excessius d'un usuari com a porta d'entrada per a accedir des de fora a la xarxa interna de l'entitat.

Aquest control comporta que els comptes d'usuaris administradors d'aplicacions, bases de dades, sistemes operatius i equips d'usuari han d'estar identificats i el seu ús controlat, eliminant els que no s'utilitzen i canviant les contrasenyes que estan definides per defecte. Addicionalment, han de complir la política de fortalesa de contrasenyes.

L'ús inadequat de privilegis administratius és un mètode primari perquè els atacants es propaguen dins d'una entitat objectiu. Hi ha tècniques d'atac molt comunes que aprofiten els privilegis administratius incontrolats. Per exemple, un usuari administrador del seu equip obri un adjunt de correu electrònic maliciós, descarrega i obri un arxiu d'un lloc web maliciós, o simplement navega en un lloc web que allotja contingut de l'atacant que pot explotar automàticament navegadors. L'arxiu o *exploit* conté codi executable que s'activa en l'equip de la víctima, ja siga automàticament o enganyant l'usuari perquè execute el seu contingut. Si la víctima té privilegis administratius, l'atacant pot apoderar-se completament de la seua màquina i instal·lar els *keyloggers* (enregistradors de teclats), els *sniffers* i el programari de control remot per a trobar contrasenyes administratives i altres dades sensibles. A més, l'atacant és capaç d'accedir a tots els recursos compartits de la víctima.

Si els privilegis administratius es distribueixen de manera folgada, o les contrasenyes són idèntiques a les utilitzades en sistemes menys crítics, o a les que venen d'origen per defecte, a l'atacant li costa molt menys prendre el control total dels sistemes, perquè hi ha molts més comptes que poden actuar com a vectors de penetració.

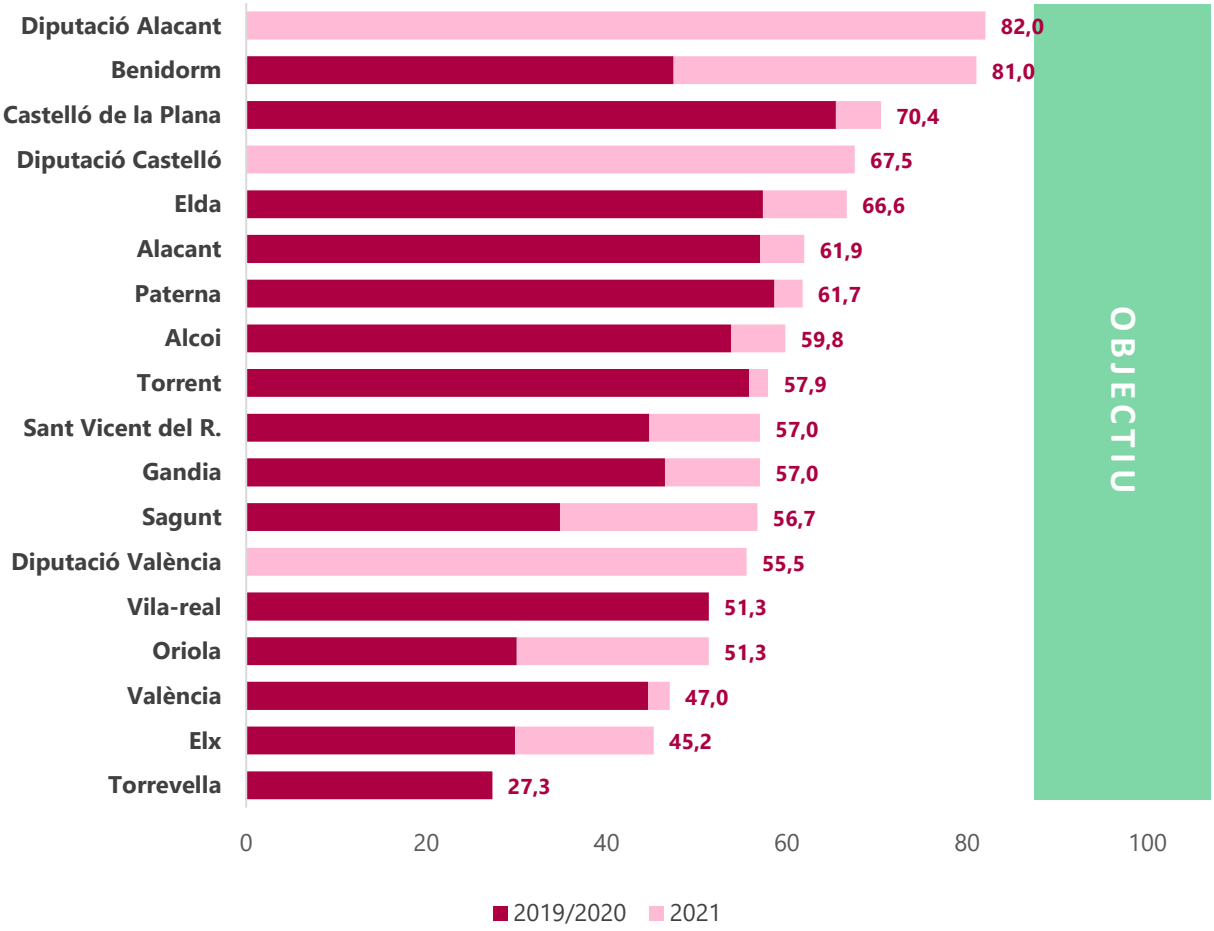
En conseqüència, les entitats han de disposar d'un procediment formalment aprovat que descriga les accions dutes a terme per a la gestió dels seus usuaris administradors, que complisca una sèrie de bones pràctiques per a garantir l'efectivitat del control. Entre aquestes cal destacar: assignació d'usuaris nominatius; permetre la traçabilitat de les accions; canvi de comptes i contrasenyes per defecte; i una política robusta de contrasenyes

que s'aplique de manera homogènia a tots els dispositius i sistemes que componen el sistema d'informació.

Situació de l'índex de maduresa del control

El gràfic següent mostra els resultats obtinguts. S'aprecia que quasi tots els ajuntaments, exceptuant-ne dos, han realitzat accions que milloren els índexs de maduresa obtinguts en l'auditoria anterior. No obstant això, la millora no és suficient per a aconseguir el nivell que s'exigeix en l'ENS. Únicament un ajuntament i una diputació aconsegueixen el nivell exigit per l'ENS.

Gràfic 12. Índex de maduresa del CBCS 4 per entitat



L'índex de maduresa mitjà ha sigut del 56,8% en els ajuntaments i del 68,3% en les diputacions.

Situació dels subcontrols revisats

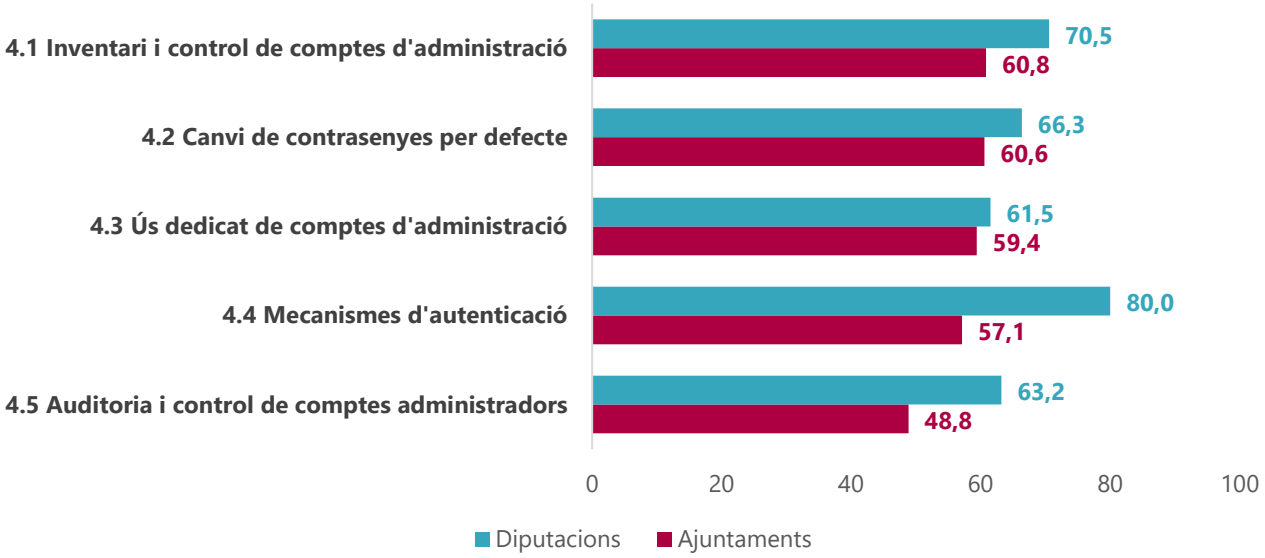
El CBCS 4 consta de cinc subcontrols:

- CBCS 4.1: Inventari i control de comptes d'administració

- CBCS 4.2: Canvi de contrasenyes per defecte
- CBCS 4.3: Ús dedicat de comptes d'administració
- CBCS 4.4: Mecanismes d'autenticació
- CBCS 4.5: Auditoria i control de comptes administratius

Si analitzem l'índex de maduresa mitjà de cada un dels subcontrols del CBCS 4 s'observa que, en general, les entitats no tenen implantades mesures que suposen un control efectiu sobre els seus usuaris administradors. No obstant això, s'observen millores que indiquen que, en general, les entitats són conscients de les seues mancances i realitzen accions encaminades a establir controls més eficaços.

Gràfic 13. Índex mitjà de maduresa dels subcontrols del CBCS 4 en 2021



Les entitats han d'aprovar procediments que descriguen la gestió dels usuaris administradors i incloguen les directrius que estableix la normativa, com l'eliminació de tots els usuaris no nominatius, la segregació de funcions en funció de la tasca a exercir, la política d'autenticació, el registre d'accions d'aquests usuaris, etc.

5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI (CBCS 5)

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.

Per què és important aquest control bàsic de ciberseguretat

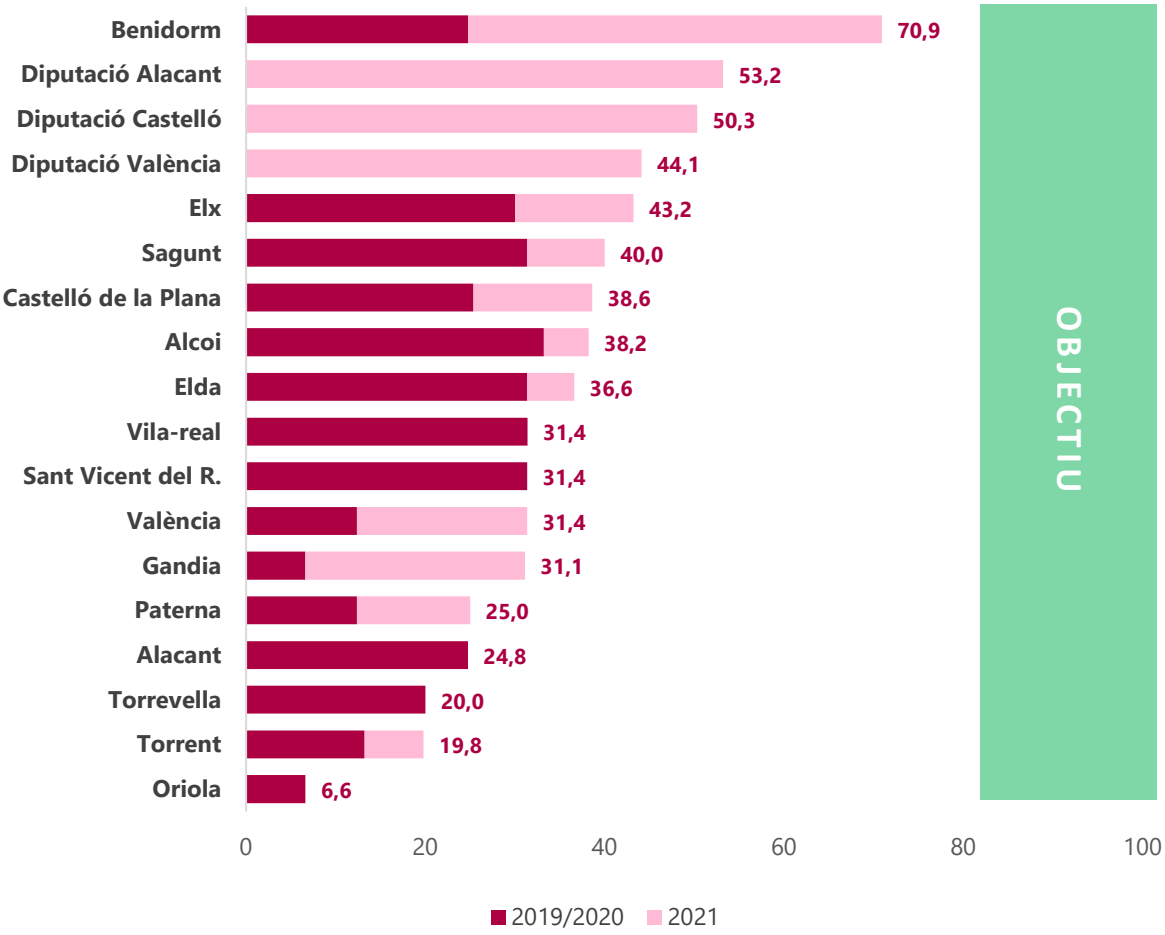
Per defecte, la majoria dels sistemes estan configurats per a facilitar-ne l'ús i no necessàriament pensant en la seguretat. Tal com els entreguen els fabricants i venedors, quan es rep un equip és habitual trobar-se controls poc robustos, serveis i ports oberts, comptes o contrasenyes predeterminades, protocols antics, programari preinstal·lat innecessari. Tots aquests aspectes són vulnerables en el seu estat predeterminat.

Per a implantar de manera efectiva aquest control, les organitzacions necessiten reconfigurar els sistemes d'acord amb estàndards de seguretat. El desenvolupament d'opcions de configuració amb bones propietats de seguretat no és una tasca senzilla i va més enllà de la capacitat dels usuaris individuals, perquè requereix anàlisis a vegades complexes i costoses per a prendre bones decisions. Per aquesta raó, és altament recomanable el seguiment i aplicació de bones pràctiques que alguns organismes publiquen en matèria de seguretat, aplicables a dispositius i sistemes.

Fins i tot si es desenvolupa i instal·la una configuració inicial forta, ha de ser revisada i actualitzada contínuament per a evitar la deterioració de la seguretat, en particular, quan el programari s'actualitza o posa pedaços es divulguen les noves vulnerabilitats de la seguretat, o les configuracions s'"ajusten" per a permetre la instal·lació de nous programes o per a donar suport a nous requeriments operacionals. Si no es revisa i actualitza de manera contínua, els atacants trobaran oportunitats per a explotar tant el programari com els serveis accessibles a la xarxa.

Situació de l'índex de maduresa del control

Gràfic 14. Índex de maduresa del CBCS 5 per entitat



Aquest gràfic mostra la situació de les entitats auditades. S'observa que cap aconsegueix el 80% exigit per l'ENS per a sistemes de categoria mitjana. No obstant això, hi ha entitats que, conscients de la inefectivitat del control, han dedicat esforços i mitjans per a millorar.

En la majoria de les entitats aquest índex és preocupantment baix, per la qual cosa han de destinar esforços per a millorar-lo.

L'índex de maduresa mitjà ha sigut del 32,6% en els ajuntaments i del 49,2% en les diputacions.

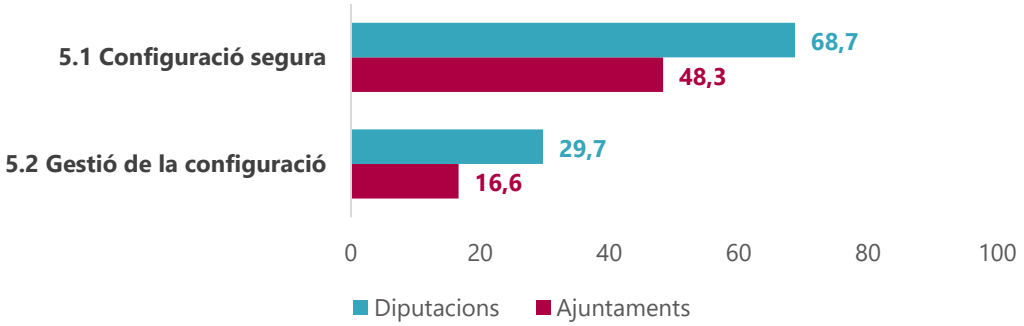
Situació dels subcontrols revisats

El CBCS 5 consta de dos subcontrols:

- CBCS 5.1: Configuració segura
- CBCS 5.2: Gestió de la configuració

Els resultats obtinguts per a aquests dos subcontrols són:

Gràfic 15. Índex mitjà de maduresa dels subcontrols del CBCS 5 en 2021



Les entitats han d'aprovar procediments que consideren la seguretat per defecte i el criteri de mínima funcionalitat, seguint les recomanacions dels fabricants en matèria de seguretat o les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN.

A més, s'ha aconsellat en tots els informes desenvolupar procediments de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics. Aquests han d'incloure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració.

6. REGISTRE DE L'ACTIVITAT DELS USUARIS (CBCS 6)

Objectiu del control

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

Per què és important aquest control bàsic de ciberseguretat

Implica que tots els sistemes i aplicacions haurien de tindre habilitades les traces d'auditoria, incloent-hi respostes a des d'on, qui i quan s'ha realitzat una determinada acció, així com tindre definides actuacions d'alerta.

En organitzacions amb pressupost i personal suficient se sol disposar d'un SIEM (*security information and event management*), sistema que, a més de centralitzar registres d'auditoria i disposar en temps real d'alertes de seguretat, és capaç de relacionar esdeveniments de seguretat dels diferents dispositius.

En l'actualitat, tots els sistemes operatius, serveis i dispositius de xarxa ofereixen capacitats de *log*, però aquests registres han de ser correctament configurats per a emmagatzemar tota la informació disponible i permetre fer-ne l'anàlisi posterior. Un exemple són els servidors, que han d'estar configurats per a crear registres de control d'accés quan un usuari intenta accedir a recursos sense els privilegis adequats. Per a avaluar si aquest registre està operatiu, l'organització ha d'escanejar periòdicament els seus *logs* i comparar-los amb

l'inventari d'actius instal·lat com a part dels CBCS 1 i 2 per a assegurar que els elements crítics de la xarxa estiguen generant periòdicament *logs*.

Els programes analítics per a revisar registres poden ser valuosos, però els mitjans utilitzats per a analitzar els *logs* d'auditoria són bastant diversos, fins i tot un examen ràpid realitzat per una persona és important per a aquesta finalitat. Les eines de correlació poden fer molt més útils els registres d'auditoria per a una inspecció posterior, i poden ser de gran ajuda en la identificació d'atacs subtils. No obstant això, aquestes eines no són un reemplaçament dels administradors de sistemes i personal experimentat de seguretat de la informació.

Deficiències en els registres de seguretat i en la seua anàlisi permeten als atacants ocultar la seua ubicació, el programari maliciós introduït i les activitats il·lícites que realitzen en les màquines víctimes. Fins i tot si els ens atacats saben que els seus sistemes han sigut compromesos, sense registres de *logs* complets i protegits romanen cecs als detalls de l'atac i a les accions posteriors dels atacants.

Sense uns *logs* d'auditoria sòlids, un atac pot passar desapercebut per temps indefinit i els danys infligits poden ser irreversibles. A causa de processos deficients o inexistents d'anàlisi de registres, a vegades els atacants controlen les màquines víctima durant mesos o anys sense que ningú se n'adone en l'organització de destinació, a pesar que l'evidència de l'atac consta en aquests registres no examinats.

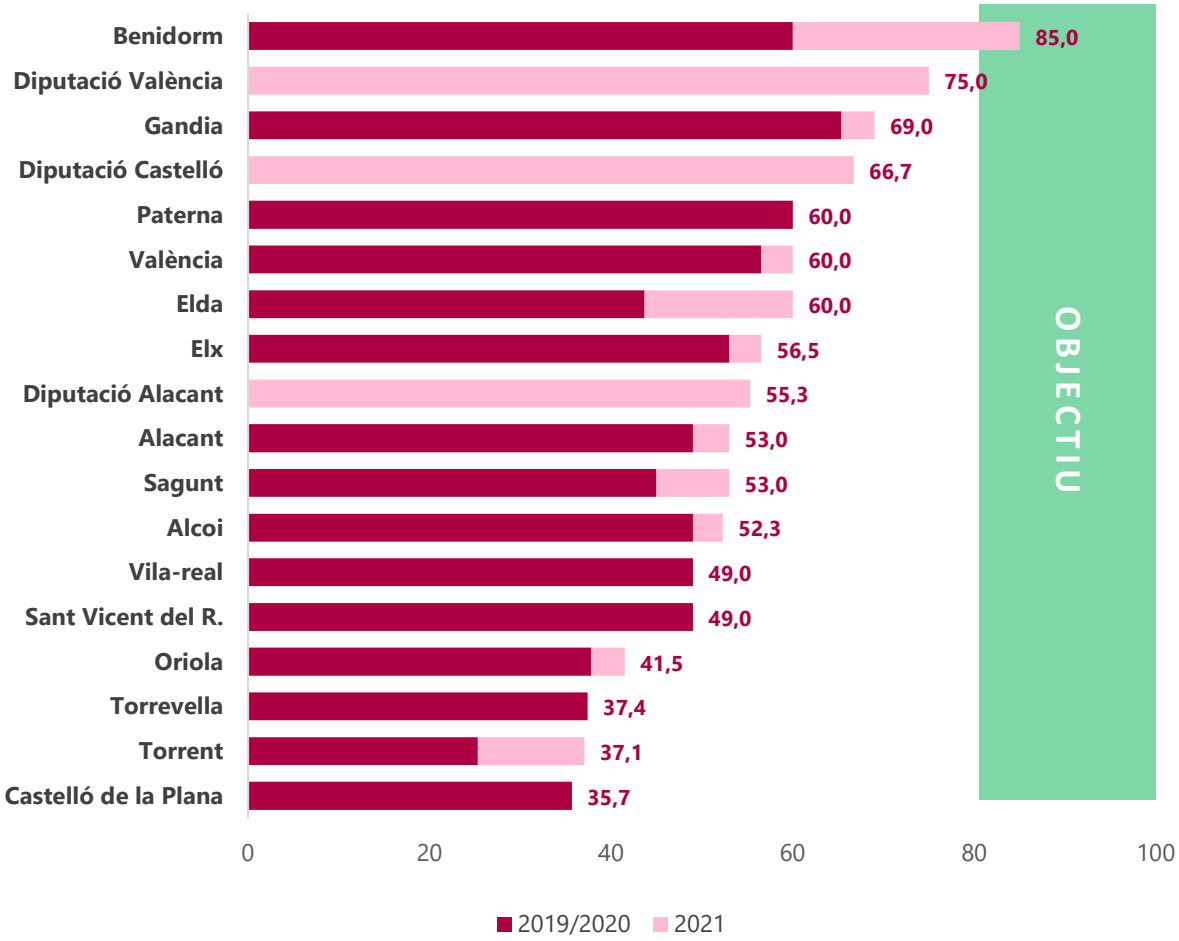
Per tot això, les organitzacions han d'incloure entre els seus procediments de seguretat la gestió dels registres d'auditoria, en els quals es definisquen els sistemes afectats, els tipus d'esdeveniments a registrar, el període de retenció, els responsables i els mecanismes de protecció que s'hi han aplicat.

Addicionalment, i atés l'ampli volum de registres generats pels diferents dispositius d'un sistema d'informació actual, és convenient l'ús d'eines per a la centralització o correlació d'esdeveniments per a gestionar-los de manera eficient.

Situació de l'índex de maduresa del control

El gràfic mostra l'índex de maduresa del CBCS 6 que els ajuntaments van obtindre en les auditories precedents i la millora que han experimentat fins al 31 de desembre del 2021, i incorpora la revisió realitzada a les tres diputacions.

Gràfic 16. Índex de maduresa del CBCS 6 per entitat



En general, els controls implantats per les entitats són insuficients per a aconseguir el nivell que s'exigeix en l'ENS, i l'índex de maduresa mitjà és del 53,2% en els ajuntaments i del 65,6% en les diputacions.

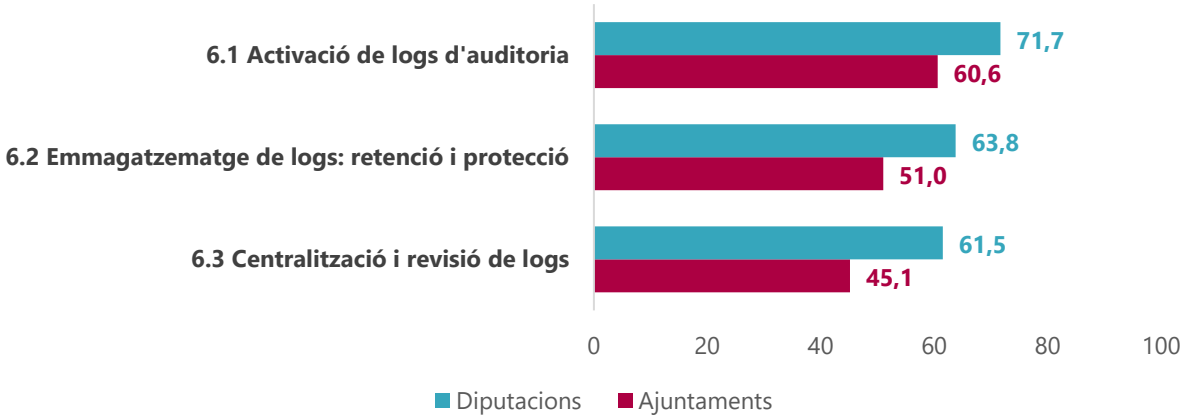
Situació dels subcontrols revisats

El CBCS 6 consta de tres subcontrols:

- CBCS 6.1: Activació de *logs* d'auditoria
- CBCS 6.2: Emmagatzematge de *logs*: retenció i protecció
- CBCS 6.3: Centralització i revisió de *logs*

Els índexs de maduresa mitjans per a cada un dels subcontrols es mostren en el gràfic següent.

Gràfic 17. Índex mitjà de maduresa dels subcontrols del CBCS 6 en 2021



Les entitats han d'aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat dels usuaris, que especifique els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre, procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.

7. CÒPIA DE SEGURETAT DE DADES I SISTEMES (CBCS 7)

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.

Per què és important aquest control bàsic de ciberseguretat

Quan els atacants comprometen els sistemes, sovint fan canvis significatius de les configuracions i el programari. A vegades, els atacants també realitzen alteracions subtils de les dades emmagatzemades en els sistemes compromesos, la qual cosa pot posar en perill l'eficàcia de l'organització amb informació contaminada. Altres vegades simplement destrueixen o invaliden totes o part de les dades i programari d'una entitat.

Quan es descobreix els atacants, pot ser extremadament difícil per a les organitzacions eliminar tots els aspectes de la presència de l'atacant en els sistemes. Els danys de ciberatacs poden ser mitigats si es disposa de còpia de seguretat de les dades afectades.

Els ciberdelinqüents han evolucionat amb el pas del temps, millorant els mètodes de xifratge o l'accés als recursos del sistema. Aquest tipus d'atacs "millorats" ha tingut efectes devastadors en les últimes onades de *ransomware*. Per això, disposar d'una còpia de seguretat no accessible a nivell de xarxa, és a dir, que es trobe aïllada o desconnectada, és una bona mesura de protecció addicional a les de xifratge i seguretat física.

Les còpies de seguretat han de ser verificades. Per a això, periòdicament, un equip de proves ha d'avaluar una mostra aleatòria de les còpies de seguretat realitzades planificant restauracions en entorns de proves. Les proves de restauració de sistemes han d'incloure

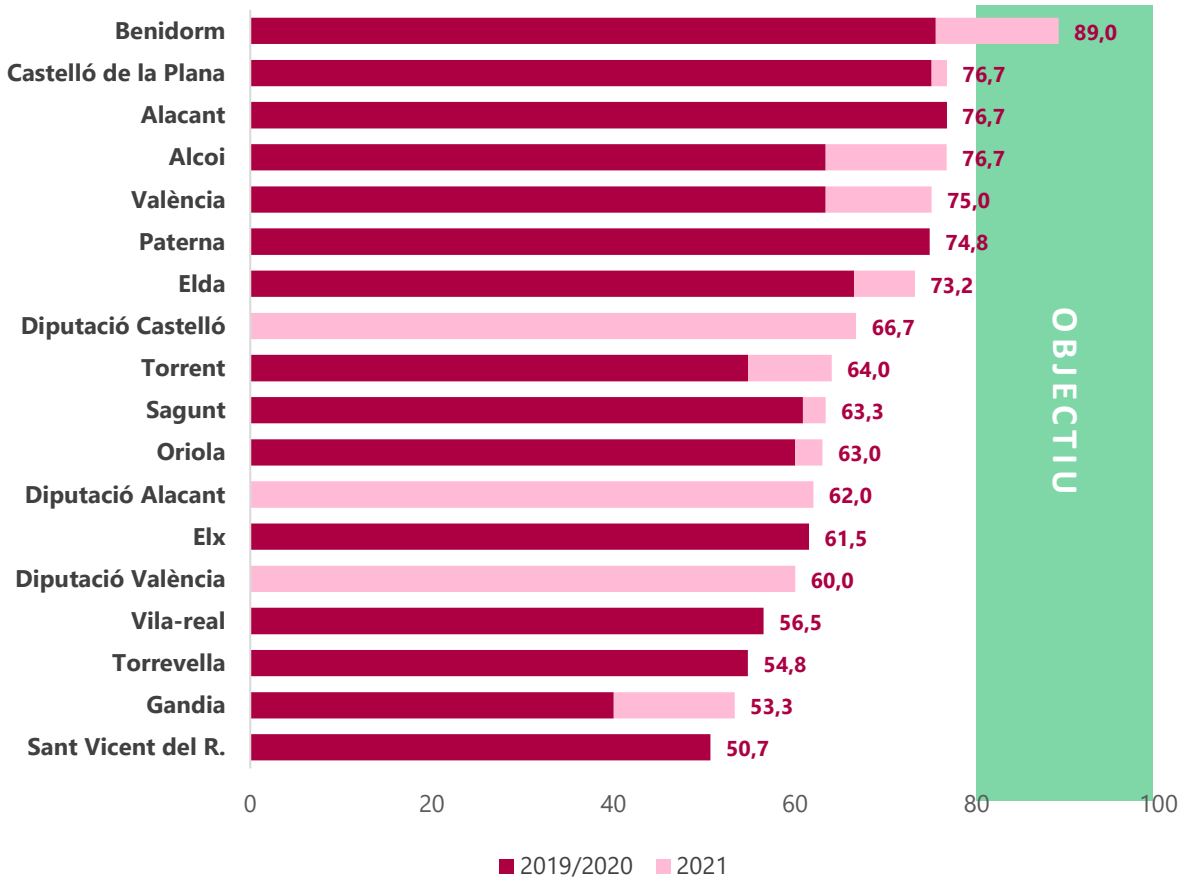
la verificació no sols del procés de recuperació, sinó també del seu contingut, és a dir, que el sistema operatiu, l'aplicació i les dades de la còpia de seguretat estiguen intactes i siguen funcionals.

Amb l'evolució de la ciberdelinqüència i els mètodes d'atac cada vegada més sofisticats, és necessari que les organitzacions estiguen preparades no sols per a defensar-se, sinó també per a refer-se davant atacs reeixits, és un element clau de la ciberresiliència d'una entitat.

Les organitzacions han de decidir quina informació protegir d'acord amb els responsables funcionals dels sistemes, i han de documentar el procés de còpies de seguretat en un procediment formalment aprovat que definisca la seua ubicació, el període de retenció, el tipus de còpies i la periodicitat. Addicionalment, les còpies han de ser proveïdes de les mesures de seguretat necessàries per a protegir-les i han de realitzar-se proves de restauració planificades, que garantisquen que els sistemes poden ser restaurats de manera efectiva.

Situació de l'índex de maduresa del control

Gràfic 18. Índex de maduresa del CBCS 7 per entitat



D'acord amb els resultats obtinguts en les auditories, el control sobre les còpies és un dels controls l'índex de maduresa del qual és, de mitjana, més alt, encara que sense aconseguir

l'objectiu. S'observa que sis entitats tenen un índex pròxim a l'objectiu, i únicament una hi arriba. Els índexs de maduresa de les altres entitats, encara que no són particularment baixos, no arriben al nivell exigit.

L'índex de maduresa mitjà ha sigut del 67,3% en els ajuntaments i del 62,9% en les diputacions.

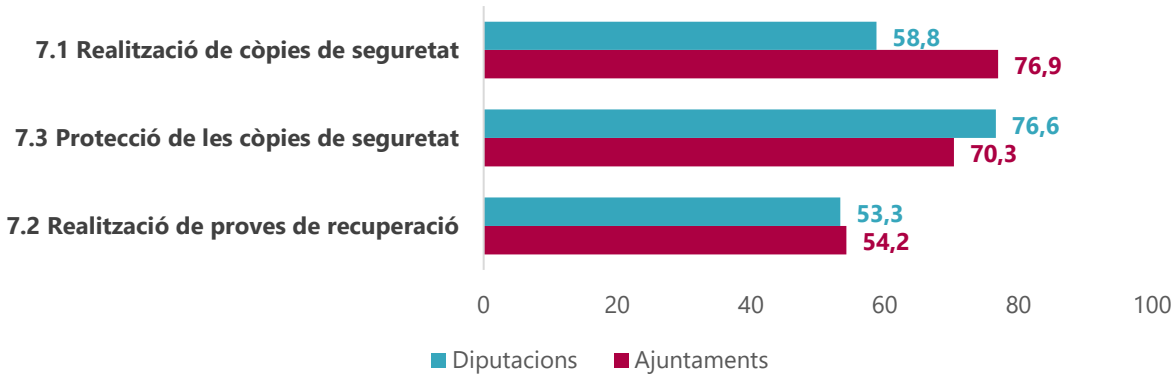
Situació dels subcontrols revisats

El CBCS 7 consta de tres subcontrols:

- CBCS 7.1: Realització de còpies de seguretat
- CBCS 7.2: Realització de proves de recuperació
- CBCS 7.3: Protecció de les còpies de seguretat

Si analitzem els resultats per subcontrol, s'observa que:

Gràfic 19. Índex mitjà de maduresa dels subcontrols del CBCS 7 en 2021



Les entitats han d'aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, les proves de restauració a realitzar i els requisits de protecció de les còpies.

8. COMPLIMENT NORMATIU (CBCS 8)

Objectiu del control

Assegurar el compliment de la normativa bàsica en matèria de seguretat de la informació.

Per què és important aquest control bàsic de ciberseguretat

Amb la inclusió d'aquest control es pretén assegurar que es compleixen diverses normes relacionades amb la seguretat de la informació que considerem rellevants per a mantindre un control adequat sobre la seguretat dels sistemes d'informació i les comunicacions i la privacitat de la informació.

Considerem molt important donar el degut compliment al que es disposa en l'Esquema Nacional de Seguretat, ja que la seua finalitat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeta als ciutadans i a les administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans. L'ENS estableix una sèrie de mesures de seguretat que han d'implantar les entitats públiques amb caràcter obligatori amb la finalitat de fonamentar la confiança que els sistemes d'informació prestaran els seus serveis i custodiaran la informació d'acord amb les seues especificacions funcionals, sense interrupcions o modificacions fora de control, i sense que la informació puga arribar al coneixement de persones no autoritzades.

D'altra banda, les administracions públiques, en el desenvolupament de les seues activitats, actuen com a responsables de tractar dades personals i han de garantir el dret de les persones a la protecció de les seues dades. Per tant, han d'adoptar les mesures necessàries per a garantir el nivell de seguretat requerit per la normativa vigent en matèria de protecció de dades personals.

Finalment considerem que, dins de l'àmbit de la gestió econòmica, és important disposar de l'informe d'auditoria de sistemes anual del Registre Comptable de Factures en compliment del que exigeix la Llei 25/2013, de 27 de desembre, d'Impuls de la Factura Electrònica i Creació del Registre Comptable de Factures, ja que un dels objectius d'aquestes auditories és la "revisió de la gestió de la seguretat en aspectes relacionats amb la confidencialitat, autenticitat, integritat, traçabilitat i disponibilitat de les dades i serveis de gestió".

Situació de l'índex de maduresa del control

El gràfic 5, "Índex de maduresa del compliment de la normativa (CBCS 8)", mostra, a l'inici d'aquest informe, que, encara que la majoria d'entitats es troben realitzant accions encaminades a esmenar els incompliments en aquesta matèria, el grau de compliment de la normativa relativa a la seguretat de la informació és, en general, deficient, i que hi ha incompliments significatius generalitzats.

Únicament un dels ajuntaments aconsegueix el nivell de maduresa exigit per l'ENS. Sis dels catorze restants aconsegueixen un nivell de compliment pròxim al que exigeix la normativa i hi ha cinc ajuntaments que no han millorat l'índex de compliment des del nostre treball d'auditoria de 2019.

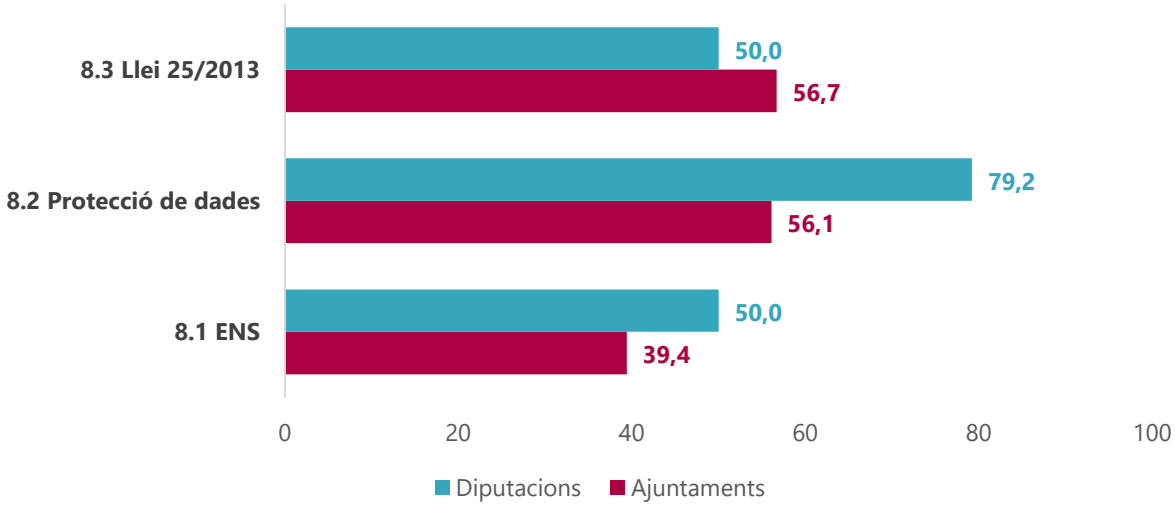
Subcontrols revisats i indicadors de la situació del control

El CBCS 8 consta de tres subcontrols:

- CBCS 8.1: Esquema Nacional de Seguretat
- CBCS 8.2: LOPD/RGPD
- CBCS 8.3: Llei 25/2013, d'Impuls de la Factura Electrònica

El gràfic següent mostra l'índex mitjà de maduresa dels tres aspectes normatius avaluats (compliment de l'ENS, matèria de protecció de dades de caràcter personal i factura electrònica).

Gràfic 20. Índex mitjà de maduresa per matèria revisada



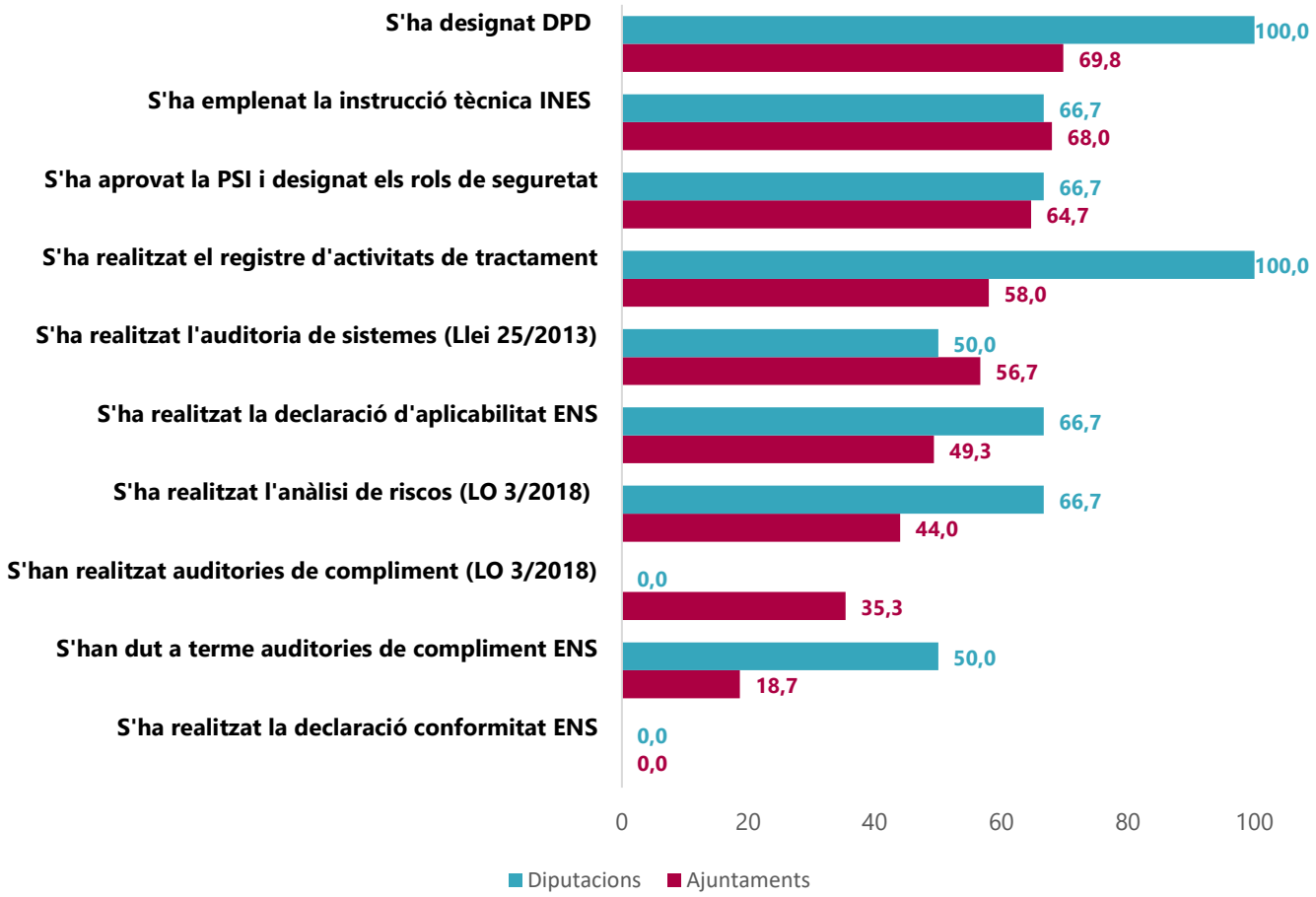
El gràfic 21 mostra l'índex de maduresa mitjà obtingut per les entitats per a cada un dels aspectes revisats en aquest CBCS. Aquests aspectes són:

- Respecte al compliment de l'ENS:
  - S'ha aprovat la PSI i s'han designat els rols de seguretat.
  - S'ha emplenat la instrucció tècnica INES.
  - S'ha realitzat la declaració d'aplicabilitat.
  - S'han dut a terme auditories de compliment.
  - S'ha realitzat la declaració de conformitat i s'han publicat els distintius en seu.
- Respecte al compliment de la normativa en matèria de protecció de dades de caràcter personal (LO 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals, i RGPD):
  - S'ha designat DPD.
  - S'ha realitzat el registre d'activitats de tractament de dades de caràcter personal.
  - S'ha dut a terme l'anàlisi de riscos dels tractaments de dades personals.
  - S'han dut a terme auditories de compliment en aquesta matèria.

- Respecte al compliment de la Llei 25/2013, de 27 de desembre, d'Impuls de la Factura Electrònica i Creació del Registre Comptable de Factures:

  – S'ha dut a terme l'auditoria de sistemes exigida per la llei esmentada.

Gràfic 21. Índex mitjà de maduresa de cada un dels aspectes avaluats en el CBCS8

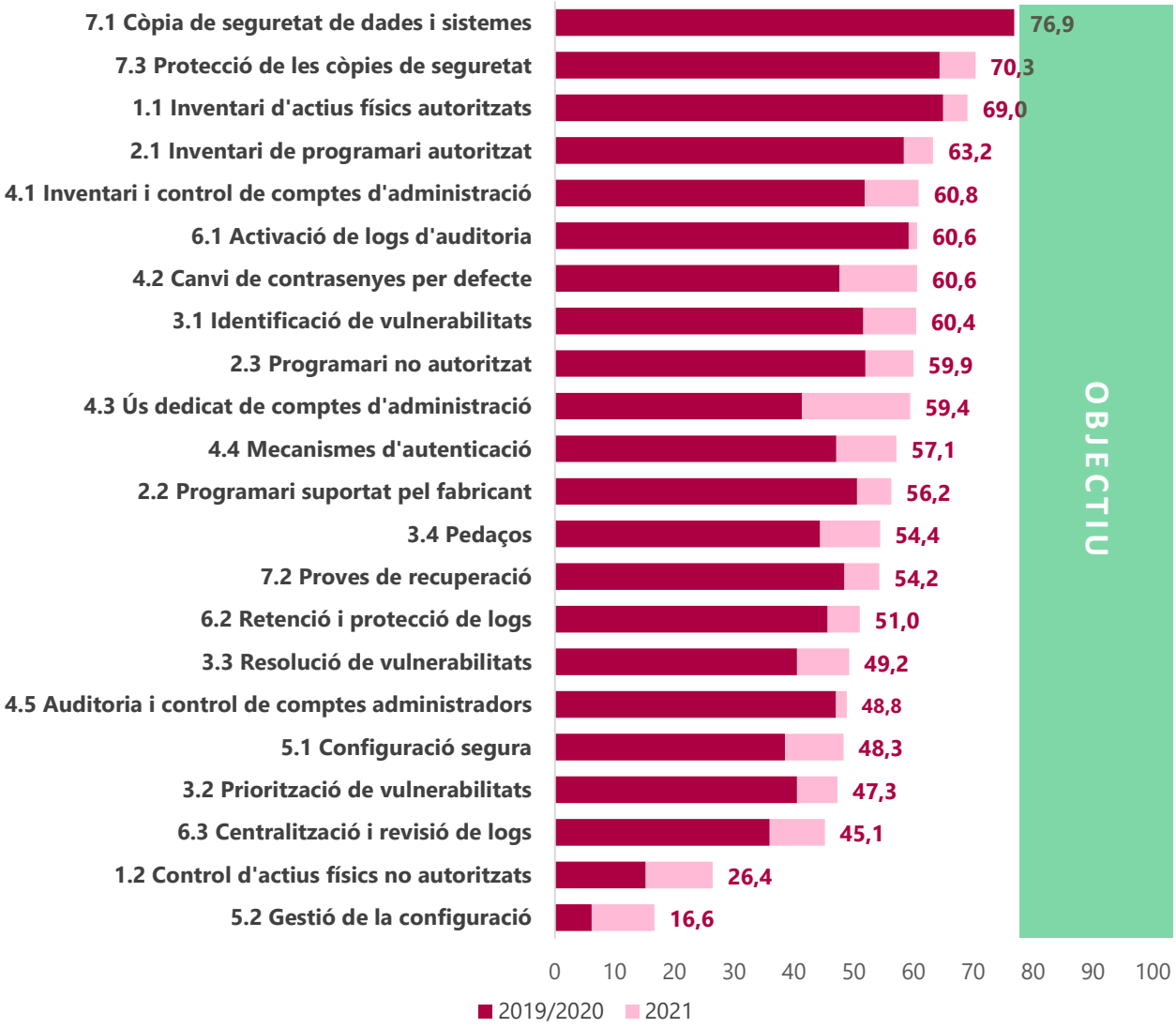


S'observa que la majoria d'entitats han designat un DPD o emés l'informe INES. No obstant això, cap de les entitats compleix l'ENS ni ha publicat en seu els distintius corresponents.

9. EVOLUCIÓ DE L'ÍNDEX DE MADURESA DELS SUBCONTROLS EN ELS AJUNTAMENTS AUDITATS

El gràfic 22 representa el conjunt dels subcontrols analitzats ordenats de major a menor índex de maduresa i la seua evolució des de l'auditoria anterior.

Gràfic 22. Índex de maduresa mitjà per subcontrol



Dels resultats observats en la gràfica extraiem les reflexions següents:

- Cap dels subcontrols aconsegueix, en mitjana, el nivell exigit per l'ENS.
- Els subcontrols relacionats amb les còpies de seguretat i els inventaris, tant maquinari com programari, continuen sent els controls amb major índex de maduresa obtingut.
- Hi ha controls l'índex de millora dels quals s'ha vist incrementat en major mesura que en altres, com en els subcontrols relacionats amb la gestió de perfils d'administració sobre els sistemes, contrasenyes, dispositius no autoritzats o configuracions per defecte.

- Hi ha subcontrols l'índex de maduresa dels quals continua sent molt deficient, encara que aquest s'haja incrementat des del nostre treball de revisió anterior. Entre aquests subcontrols hi ha la gestió de les configuracions segures, el control d'actius físics no autoritzats o l'ús d'eines per a la revisió de registres d'auditoria.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

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

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

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

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

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

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

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

EDR:[13] Un sistema EDR, sigla en anglés d'*endpoint detection and response*, és un sistema de protecció dels equips i infraestructures de l'empresa. Combina l'antivirus tradicional juntament amb eines de monitoratge i intel·ligència artificial per a oferir una resposta ràpida i eficient davant els riscos i les amenaces més complexes.

Governança corporativa: Es el sistema pel qual es dirigeixen i controlen les organitzacions (UNE-ISO/IEC 38500).

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

Governança sobre les TI: És un component clau de la governança corporativa en general. És el sistema per mitjà del qual es dirigeix i controla l'ús actual i futur de les tecnologies de la informació i les comunicacions. Implica avaluar i dirigir la utilització de les TI per a donar suport a l'organització i al monitoratge d'aquest ús per a aconseguir la consecució dels plans. Inclou l'estratègia i polítiques per a la utilització de les TI en l'organització (UNE-ISO/IEC 38500).

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

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

deriva i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desenvolupament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

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

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

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

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*h* del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 19 d'abril de 2023, va aprovar aquest informe d'auditoria.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe de síntesi CBCS_exercici 2021_val - SEFYCU 4095150

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

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

Codi Segur de Verificació (CSV): KUAA 93QL EFX2 2WNM RLUT

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

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

Empremta del document per a la persona firmant	Text de la firma	Dades addicionals de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrònica - ACCV - 09/05/23 10:02 VICENT CUCARELLA TORMO