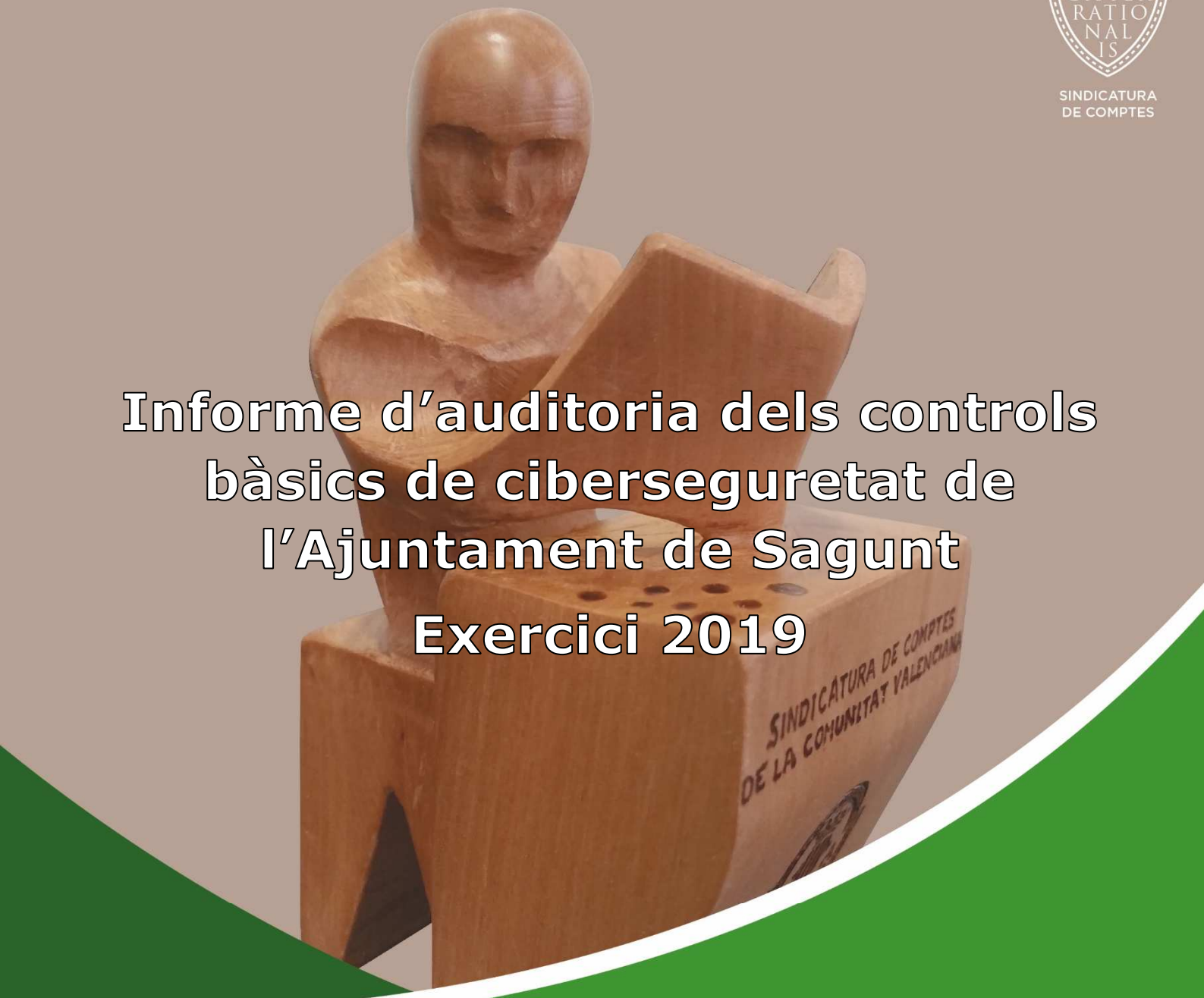
SINDICATURA DE COMPTES



Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de Sagunt

Exercici 2019

INFORME D'AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DE L'AJUNTAMENT DE SAGUNT

Exercici 2019

RESUM

L'auditoria realitzada per la Sindicatura de Comptes sobre els controls bàsics de ciberseguretat de l'Ajuntament de Sagunt en l'exercici 2019 ha donat com a resultat que, amb caràcter general, el grau de compliment existent en la gestió d'aquesta matèria és d'un 55,6% respecte al nivell establit com a objectiu. Això implica que, encara que hi ha un cert nivell d'efectivitat en els controls analitzats, és insuficient i hi ha possibilitats clares de millora.

D'altra banda, la valoració de l'auditoria sobre el compliment dels aspectes de legalitat representa un índex del 62,5% respecte del nivell establit com a objectiu, una xifra que l'òrgan fiscalitzador considera insatisfactòria.

Aquest treball s'emmarca dins de les auditories realitzades als controls bàsics de ciberseguretat dels quinze ajuntaments més grans de la Comunitat Valenciana, incloses en el Programa Anual d'Actuació de 2019 de la Sindicatura i posteriorment ampliades a tots els municipis amb població superior a 50.000 habitants. Amb les seues valoracions, l'òrgan fiscalitzador verifica si el marc de ciberseguretat aplicat sobre els sistemes d'informació garanteix un nivell de control adequat, inclou la protecció de la informació que gestionen i la continuïtat dels serveis públics oferits.

En aquest sentit, la crisi sanitària i socioeconòmica mundial causada per la pandèmia de COVID-19 que marca la nostra realitat en el moment de publicar aquest informe, ha posat de manifest la total dependència que té la gestió pública dels sistemes d'informació i les comunicacions (SIC). Això fa que administracions públiques i ajuntaments siguen més vulnerables enfront dels ciberatacs i que, per tant, mantindre un sòlid sistema de protecció davant d'ells i una adequada ciberhigiene siga més necessari que mai.

Amb el propòsit de millorar la gestió de la ciberseguretat en l'ens auditat, a més de l'informe amb els resultats obtinguts en el treball, la Sindicatura ha traslladat a l'Ajuntament de Sagunt l'anàlisi detallada de les deficiències identificades i les recomanacions orientades a esmenar-les. La millora dels controls de ciberseguretat requerirà actuacions i inversions, tant en mitjans materials com personals, que cal planificar adequadament. En aquest sentit, l'òrgan fiscalitzador preveu la realització del seguiment de les recomanacions com a part del Programa Anual d'Actuació de 2020.

La Sindicatura considera que és necessari que els màxims òrgans responsables de l'Ajuntament (Ple, alcalde i la regidoria responsable de les TIC) prenguen consciència de la necessitat d'aconseguir els nivells exigits per la normativa per a la protecció dels sistemes d'informació davant de la multiplicitat d'amenaces existents, a fi de garantir la consecució dels objectius de l'entitat, la prestació adequada de serveis als ciutadans i la protecció de la informació i de la resta dels actius dels sistemes d'informació.

NOTA

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

ÍNDEX **Pàgina**

1. INTRODUCCIÓ

En virtut de les disposicions de l'article 8.3 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i segons el que es preveu en el Programa Anual d'Actuació de 2019 (PAA2019), s'ha efectuat una auditoria sobre la situació en 2019 dels controls bàsics de ciberseguretat (CBCS) dels ajuntaments de la Comunitat Valenciana amb una població superior a 60.000 habitants, entre els quals es troba l'Ajuntament de Sagunt.

La realitat del nostre entorn pròxim i de la resta de la societat espanyola i mundial en el moment de publicar aquest informe és la d'una crisi sanitària i socioeconòmica sense precedents provocada per l'epidèmia de la COVID-19. Entre moltes qüestions més, aquesta crisi ha posat de manifest que gran part de les administracions públiques i ajuntaments han sigut capaços de continuar en marxa confiant en gran manera en el bon funcionament i l'eficàcia dels sistemes d'informació i les comunicacions (SIC).

Al mateix temps, aquesta circumstància ha mostrat amb claredat absoluta la dependència total dels SIC que existeix actualment en la gestió pública, la qual cosa fa que les nostres administracions siguen més vulnerables als ciberatacs i que, per tant, mantindre una ciberhigiene adequada i un sistema sòlid de protecció davant d'aquells siga més necessari que mai.

2. RESPONSABILITATS DELS ÒRGANS MUNICIPALS EN RELACIÓ AMB ELS CONTROLS DE CIBERSEGURETAT

Els òrgans municipals (el Ple, l'alcalde, la Junta de Govern i la Secretaria General) són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions. D'acord amb les seues competències, han de garantir que el funcionament de l'entitat és conforme amb les normes aplicables i que els controls interns proporcionen una garantia raonable que les dades, la informació i els actius dels sistemes d'informació compleixen les propietats següents, que coincideixen amb les cinc dimensions de la seguretat de la informació que estableix l'Esquema Nacional de Seguretat (ENS):[1]

- Confidencialitat. És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.

- Integritat. És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades i que assegura que no se n'ha produït l'alteració, la pèrdua o la destrucció,

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

tant de manera accidental com 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 segons la qual una entitat és la que diu ser o bé que garanteix la font de la qual procedeixen les dades.

- Traçabilitat. És la propietat o característica segons la qual les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

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

Àmbit objectiu

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

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

Atesa la naturalesa de l'objecte material que cal revisar –la gran amplitud, complexitat i diversitat dels sistemes d'informació d'un ens local de grans dimensions–, ha sigut necessari delimitar i concretar quins sistemes s'havien d'analitzar. En aquest sentit, hem analitzat les aplicacions que suporten dos dels processos de gestió més rellevants per a la Sindicatura, com ara la gestió comptable i pressupostària i la gestió tributària i recaptadora. La revisió ha inclòs els controls relacionats amb:

- les aplicacions informàtiques que els suporten,
- les bases de dades subjacents,
- els sistemes operatius instal·lats en cada un dels sistemes que integren l'aplicació de gestió (per exemple, servidor web, servidor d'aplicació, servidor de base de dades).

A més, per la seua importància per al bon funcionament dels sistemes d'informació i la ciberseguretat, 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 (encaminadors, *switches*, punt d'accés a xarxa wifi, etc.)
- elements de seguretat (tallafocs, IPS, *proxy* de correu, *proxy* de navegació, servidors d'autenticació, infraestructura de generació de certificats, etc.)

Metodologia

La Unitat d'Auditoria de Sistemes d'Informació de la Sindicatura de Comptes (UASI) ha realitzat aquesta auditoria dels controls bàsics de ciberseguretat seguint la metodologia establida en la guia *GPF-OCEX 5313 Revisió dels controls bàsics de ciberseguretat* (integrada en el *Manual de fiscalització* de la Sindicatura de Comptes).

Hem avaluat la situació dels CBCS utilitzant el model de nivell de maduresa dels processos ja que, a més de ser un sistema àmpliament acceptat, permet establir objectius i realitzar comparacions entre entitats diferents i veure l'evolució al llarg del temps. La metodologia utilitzada està plenament alineada amb el que estableix l'ENS, que és d'aplicació obligatòria en tots els ens públics.

En l'apèndix 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, els resultats detallats de cada un dels controls només es comuniquen amb caràcter confidencial als responsables de l'Ajuntament perquè puguen adoptar les mesures correctores que consideren necessàries. En aquest informe els resultats es mostren de manera sintètica.

4. CONCLUSIONS

Com a resultat del treball realitzat cal concloure que, amb caràcter general, el grau de control existent en la gestió dels controls bàsics de ciberseguretat assenyalats en l'apartat 3, arriba a un índex de maduresa del 44,5%, que correspon amb un nivell de maduresa *N1, inicial / ad hoc*; és a dir, els processos de control existeixen, però la gestió no està correctament organitzada.

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 apliquem als CBCS en aquesta auditoria és *N3, procés definit* i un índex de maduresa del 80%.

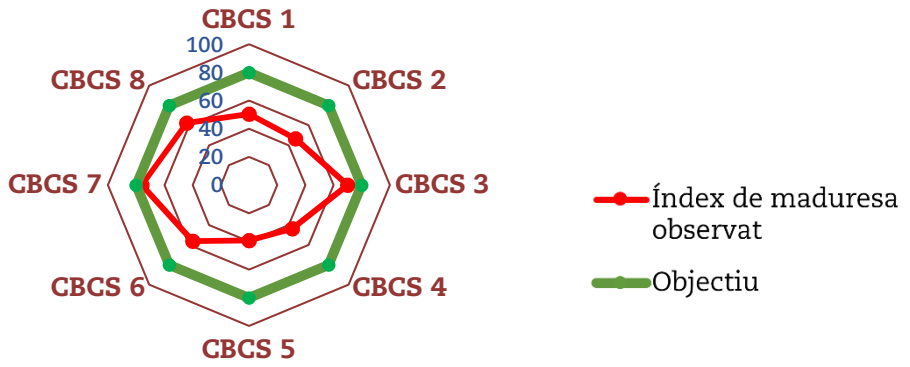
En conseqüència, l'índex de compliment dels CBCS és del 55,6%, que resulta de comparar l'indicador de maduresa observat amb el nivell requerit o objectiu que ha de tenir el sistema segons l'ENS.

En el quadre següent es mostren de manera detallada els resultats de l'avaluació realitzada per a cada un dels CBCS.

Quadre 1. Índex i nivell de maduresa dels CBCS de l'Ajuntament

Control		Índex de maduresa	Nivell de maduresa	Índex de compliment
CBCS 1	Inventari i control de dispositius físics	40,4%	N1	50,5%
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	37,4%	N1	46,8%
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	56,0%	N2	70,0%
CBCS 4	Ús controlat de privilegis administratius	34,8%	N1	43,5%
CBCS 5	Configuracions segures del programari i maquinari	31,4%	N1	39,2%
CBCS 6	Registre de l'activitat dels usuaris	45,0%	N1	56,3%
CBCS 7	Còpies de seguretat de dades i sistemes	60,8%	N2	76,0%
CBCS 8	Compliment normatiu	50,0%	N2	62,5%
Índex / Nivell global de l'Ajuntament		**44,5%**	**N1**	**55,6%**
Índex / Nivell requerit o objectiu		**80,0%**	**N3**	**100,0%**

Gràfic 1. Índex de maduresa dels CBCS



A la vista dels resultats obtinguts en la revisió, es conclou que, encara que existeix cert nivell d'efectivitat en els controls analitzats, hi ha possibilitats clares de millora. Per tant, és necessari que els màxims òrgans responsables de l'Ajuntament (Ple, alcalde i la regidoria responsable de les TIC) prenguen consciència de la necessitat d'aconseguir els nivells exigits per la normativa per a la protecció dels sistemes d'informació davant de la multiplicitat d'amenaces existents, a fi de garantir la consecució dels objectius de l'entitat, la prestació

adequada de serveis als ciutadans i la protecció de la informació i de la resta dels actius dels sistemes d'informació. Aquesta cultura de ciberseguretat s'ha de traslladar a tots els nivells i departaments de l'Ajuntament.

La millora dels controls de ciberseguretat requerirà actuacions i inversions, tant en mitjans materials com personals, que s'han de planificar adequadament.

A més, la revisió del compliment de legalitat en matèria relacionada amb la ciberseguretat ha posat de manifest un nivell de compliment insatisfactori. Els màxims òrgans de direcció de l'Ajuntament tenen la responsabilitat de garantir un nivell adequat de compliment de les normes legals i han d'impulsar les mesures necessàries per a esmenar la situació.

5. SITUACIÓ DELS CONTROLS

A continuació, es detallen els principals aspectes que han sorgit en la revisió de cada un dels CBCS de l'Ajuntament.

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

Hem verificat que l'Ajuntament realitza accions per a l'inventari i control d'actius físics de l'entitat com a part d'un procés adequat que està implantat de manera general per a tots els sistemes, encara que aquest procés no es troba establit en un procediment formalment aprovat.

El procés d'elaboració de l'inventari es troba recolzat per l'ús d'una eina específica, que gestiona l'inventari de tots els actius de l'entitat, bé per mitjà d'un agent de xarxa o per detecció automàtica. S'ha evidenciat que l'inventari existent es troba completament actualitzat per a tots els seus elements.

D'altra banda, no s'han implantat mesures efectives orientades a impedir la connexió de dispositius físics no autoritzats al sistema d'informació, control que actualment només existeix de manera parcial en determinades ubicacions amb riscos particulars.

En conseqüència, considerem que hi ha un nivell de control insuficient sobre l'inventari de dispositius físics, i la valoració global del control arriba a un índex de maduresa del 40,4%, que es correspon amb un nivell de maduresa *N1, inicial / ad hoc;* és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un índex de compliment del CBCS 1 del 50,5%.

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

Quant al control que realitza l'Ajuntament del programari instal·lat i autoritzat en els equips, hem observat que es realitzen accions com a part d'un procés que es troba parcialment definit i no aprovat formalment.

L'inventari de programari es manté correctament actualitzat de manera automatitzada, mitjançant l'ús de l'eina que també gestiona l'inventari d'actius físics i que manté relacionats tots dos inventaris.

D'altra banda, s'ha evidenciat l'existència d'un determinat nombre d'equips amb programari fora del període de suport del fabricador, fet que representa un risc greu per al sistema d'informació. No obstant això, es troba en execució un projecte pluriennal que té com a objectius, entre altres, l'actualització tecnològica i l'adquisició de llicències de programari per a substitució dels sistemes fora de suport del fabricant.

Encara que l'entitat disposa de mesures orientades a impedir l'ús de programari no autoritzat, hi ha determinades carències que fan completament ineficaces aquestes mesures de control.

Hi ha, per tant, un nivell de control insuficient sobre l'inventari i programari autoritzat, per la qual cosa s'han de dedicar esforços i recursos a millorar-lo. La valoració global del control arriba a un índex de maduresa del 37,4%, que es correspon amb un nivell de maduresa *N1, inicial / ad hoc*; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un índex de compliment del CBCS 2 del 46,8%.

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

Hem analitzat la gestió de vulnerabilitats realitzada per l'Ajuntament i hem observat que aquestes accions formen part d'un procés adequadament implantat i que està establit en un procediment, però que no s'ha aprovat formalment en el moment de la revisió. No obstant això, no totes les accions descrites en el procediment es duen a terme, ni totes les accions que es realitzen (per exemple, la priorització i resolució de vulnerabilitats) s'hi han descrit.

La identificació i solució de vulnerabilitats es realitza, bé de manera manual per mitjà de la cerca i resolució per a determinats elements, o bé la realitzen tercers per mitjà de contractes de manteniment de determinats sistemes i serveis específics de gestió de riscos i vulnerabilitats.

Durant el treball d'auditoria s'ha evidenciat l'existència d'una eina per a la gestió centralitzada d'actualitzacions, però no es troba

implantada en l'actualitat, la qual cosa representa un risc greu per a la seguretat dels sistemes de l'entitat.

Això significa que existeix cert nivell de control en la identificació i solució de vulnerabilitats, però s'identifiquen possibilitats de millora i la valoració global arriba a un índex de maduresa del 56,0%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat degudament. Això representa un índex de compliment del CBCS 3 del 70,0%.

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

Hem verificat que les accions de l'Ajuntament per al control dels comptes d'usuaris administradors formen part d'un procés implantat de manera general per a tots els sistemes inclosos en l'abast del treball, però no es troba correctament definit ni s'ha establit formalment en un procediment aprovat.

S'ha detectat l'ús de comptes d'administració no nominatius, així com l'ús de comptes amb privilegis d'administració per usuaris que no compleixen la regla de mínima funcionalitat.

S'ha confirmat la inexistència d'identificadors diferenciats per a un mateix usuari, depenent de la mena de tasca que haja d'exercir en el sistema, la qual cosa implica un ús indegut d'identificadors amb privilegis administratius en les tasques que no el requereixen.

Després de la revisió, considerem que hi ha un nivell de control insuficient, per la qual cosa s'hauran de dedicar esforços i recursos a millorar-lo. La valoració global del control existent sobre l'ús de privilegis administratius arriba a un índex de maduresa del 34,8%, que es correspon amb un nivell de maduresa *N1, inicial / ad hoc*; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un índex de compliment del CBCS 4 del 43,5%.

5. *Sobre les configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors (CBCS 5)*

Hem analitzat les accions realitzades a l'Ajuntament per al control de configuracions segures en dispositius i aplicacions i hem verificat que el control és molt limitat, i no existeix un procediment formalment aprovat a aquest efecte.

Si bé s'ha evidenciat que es disposa de plantilles per a la configuració de determinats dispositius, aquestes plantilles no tenen caràcter de fortificació ni la configuració segura d'aquests dispositius es troba formalment establida.

S'apliquen configuracions de seguretat o es realitzen comprovacions únicament en la posada en operació de certs sistemes, amb la finalitat de proporcionar un cert nivell de seguretat.

Això significa que hi ha un nivell deficient de control en l'aplicació de configuracions segures en dispositius i programari, per la qual cosa s'hauran de dedicar esforços i recursos a millorar-lo. La valoració global del control arriba a un índex de maduresa del 31,4%, que es correspon amb un nivell de maduresa *N1, inicial / ad hoc*; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un índex de compliment del CBCS 5 del 39,2%.

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

Hem analitzat les accions de l'Ajuntament per al registre de l'activitat dels usuaris en els diferents sistemes i hem verificat que, encara que s'han aplicat certes mesures relacionades amb aquest control, aquestes no s'han establit formalment no s'han aprovat en un procediment.

També hem verificat que el registre d'activitat es troba activat en la majoria dels sistemes, si bé es manté la configuració per defecte que defineix el fabricant.

L'Ajuntament disposa d'una eina centralitzada per als registres d'activitat de determinats elements, la qual cosa representa una millora de la configuració bàsica per defecte dels *logs* d'auditoria. No obstant això, aquesta eina no integra tots els sistemes rellevants des del punt de vista de la ciberseguretat i la revisió d'aquests registres d'activitat es realitza de manera informal, no procedimentada.

Hi ha un nivell insuficient de control en el registre de l'activitat dels usuaris, per la qual cosa s'hauran de dedicar esforços i recursos a millorar-lo. La valoració del control arriba a un índex de maduresa del 45,0%, que es correspon amb nivell de maduresa *N1, inicial / ad hoc;* és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat degudament. Això representa un índex de compliment del CBCS 6 del 56,3%

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

Hem analitzat les accions de l'Ajuntament per a la realització de còpies de seguretat de dades i sistemes i hem observat que formen part d'un procés implantat que es troba correctament definit i executat i que es troba recollit en un procediment. No obstant això, aquest procediment no es troba formalment aprovat i no ha sigut actualitzat amb les modificacions més recents del procés.

Les polítiques de còpia aplicades s'han desenvolupat d'acord amb les necessitats identificades pel departament TIC i el resultat d'aquestes és revisat per mitjà d'un procés manual. Així mateix, les mesures implantades per a la protecció de les còpies poden considerar-se efectives. No obstant això, no es realitzen de manera sistemàtica proves de recuperació planificades.

Això significa que hi ha un cert nivell de control sobre les còpies de seguretat de dades i sistemes, però hi ha possibilitats de millora. La valoració global del control arriba a un índex de maduresa del 60,8%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però existeixen controls parcialment establits o els procediments no han sigut formalitzats degudament. Això representa un índex de compliment del CBCS 7 del 76,0%.

8. Sobre el compliment de la legalitat (CBCS 8)

L'Ajuntament ha incorregut en diversos incompliments legals, per la qual cosa la valoració global sobre el compliment dels aspectes de legalitat que hem verificat[2] és que arriba a un índex de maduresa del 50,0%. Això es correspon amb un nivell de maduresa *N2*, que indica que hi ha incompliments significatius de la normativa. Això representa un índex de compliment del CBCS 8 del 62,5%.

En relació amb l'ENS

L'Ajuntament disposa d'una política de seguretat aprovada per l'òrgan superior competent que precisa, com a mínim, els objectius i la missió de l'organització, el marc legal i normatiu, la definició de rols i funcions, l'estructura organitzativa i el seu procés d'aprovació i de revisió.

S'ha realitzat la designació de les persones per als rols definits en la política de seguretat i s'han constituït els òrgans que s'hi descriuen.

S'han elaborat la declaració d'aplicabilitat i el Pla d'Adequació, basats en la categorització d'actius i anàlisis de riscos, si bé aquests documents es troben pendents d'aprovació.

No obstant això:

- No s'ha formalitzat i enviat la informació de l'informe de l'estat de la seguretat (informe INES).

2 ENS, RGPD, Llei Orgànica 3/2018, de 5 de desembre, i Llei 25/2013, de 27 de desembre, d'Impuls de la Factura Electrònica.

- No es realitzen les auditories de compliment previstes en l'article 34 del Reial Decret 3/2010.

- No s'han publicat en la seu electrònica les declaracions de conformitat i els distintius corresponents previstos en l'ENS.

En matèria de protecció de dades personals

S'ha nomenat un delegat de protecció de dades (DPD) d'acord amb el que es preveu en l'article 37.1.*a* de l'RGPD.

S'ha elaborat el registre d'activitats de tractament de la informació requerida per l'RGPD i publicat aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.

S'ha realitzat una anàlisi de riscos sobre els tractaments de dades personals d'acord amb l'article 32.2 de l'RGPD.

No obstant això:

- No s'han aplicat les mesures organitzatives i tècniques necessàries per a protegir les dades personals, requerides per l'article 24.1 de l'RGPD.

- No s'han executat auditories de compliment en matèria de protecció de dades.

En relació amb la Llei de Factura Electrònica

No s'han dut a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.

6. RECOMANACIONS I MESURES PER AL COMPLIMENT DE LA LEGALITAT

Com a resultat de l'auditoria realitzada és procedent efectuar les recomanacions que s'assenyalen a continuació, per a l'atenció de les quals l'Ajuntament haurà de dedicar els esforços i recursos necessaris. També s'assenyalen les mesures per al compliment de la legalitat que han d'adoptar-se.

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

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

2) Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

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

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

   - L'elaboració de llistes de programari autoritzat (llistes blanques) i la realització de revisions periòdiques de programari.

   - La implantació de les mesures tècniques que impedisquen la instal·lació i execució del programari no autoritzat.

   - La definició d'un pla de manteniment de la totalitat del programari utilitzat, incloent-hi tant el gestionat per mitjà de licitacions i clàusules contractuals, com la resta de programari utilitzat a l'Ajuntament.

4) Revisar i actualitzar tots els sistemes que es troben fora del període de suport.

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

5) Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents:

   - La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, l'anàlisi prèvia a l'entrada en producció dels sistemes i les accions actualment establides de seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat.

   - La priorització actualment implantada basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.

6) Utilitzar eines que permeten la gestió unificada i automatitzada de pedaços de seguretat i altres actualitzacions.

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

7) Aprovar un únic procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga:

   - L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis

administratius de tots els sistemes. Totes les activitats de gestió han de realitzar-se amb usuaris nominatius.

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

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

- La política d'autenticació que cal aplicar a aquesta mena de comptes.

Sobre les configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors (CBCS 5)

8) Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN.[3]

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

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

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

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

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

10) Actualitzar i aprovar formalment el procediment existent per a la gestió de còpies de seguretat de dades i sistemes i que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, les ubicacions, els responsables, les proves de restauració i els requisits de protecció de les còpies.

Sobre el compliment de la legalitat (CBCS 8)

11) Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament:

    - Ha de formalitzar la Instrucció Tècnica de Seguretat de l'informe de l'estat de la seguretat, de la Secretaria d'Estat d'Administracions Públiques (informe INES).

    - Realitzar les auditories previstes en l'article 34 del Reial Decret 3/2010.

    - Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.

12) En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que estableixen l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular:

    - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.

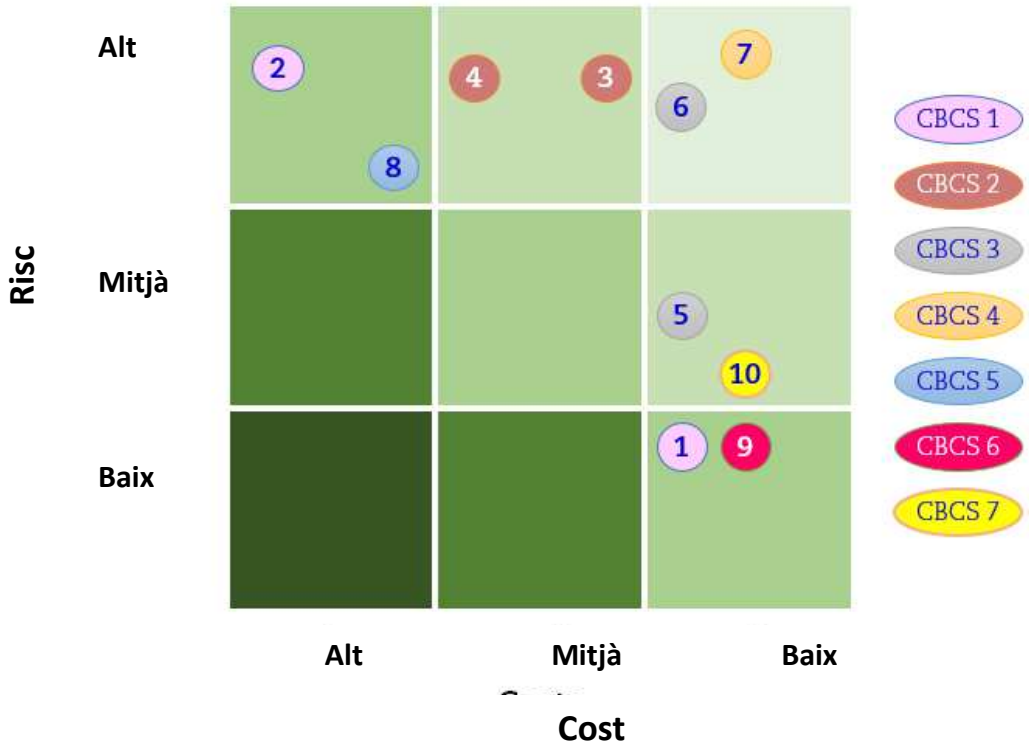
    - Planificar i executar auditories en matèria de protecció de dades.

13) Dur a terme l'auditoria del registre de factures exigida per la Llei 25/2013, de 27 de desembre.

Priorització de les recomanacions

A fi de que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic següent es mostra la classificació de les recomanacions segons els criteris combinats de risc potencial que cal mitigar i cost de la implantació. No s'hi inclouen les mesures que cal implantar 11) a 13) perquè són exigències legals.

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



A més de les recomanacions anteriors, juntament amb el detall al màxim nivell de les deficiències de seguretat observades, s'ha comunicat als responsables de l'Ajuntament altres recomanacions amb una relació de risc potencial a mitigar i cost de la implantació menys favorable que les anteriors.

APÈNDIX. Metodologia aplicada

1. La GPF-OCEX 5313 i l'Esquema Nacional de Seguretat

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

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS, que és de compliment obligat per a tots els ens públics. Aquesta alineació facilita la realització de les auditories de ciberseguretat per 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 estan exigits per 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 seleccionar els més rellevants es va atendre el marc conceptual establit per la prestigiosa organització Center for Internet Security (CIS),[4] que prioritza i classifica els controls segons la seua importància per a fer front a les ciberamenaces.

Els 20 controls de seguretat crítics del CIS són un conjunt concís i prioritzat d'accions de ciberdefensa orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. La versió 7 dels controls CIS classifica els sis primers controls com a bàsics i són els que s'han utilitzat com a referència en la GPF-OCEX 5313 per a establir els controls bàsics de ciberseguretat (CBCS) dels OCEX, als quals es va afegir el relatiu a les còpies de seguretat de dades i sistemes, per la seua importància per a la recuperació davant d'un desastre o atac reeixit i, per tant, per a garantir una raonable ciberresiliència, i un vuité CBCS relacionat amb el compliment normatiu, per la seua importància en una Administració pública.

Els vuit controls bàsics de ciberseguretat degudament referenciats amb l'ENS són:

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

Quadre 2. Els CBCS i l'ENS

Control		Mesura de seguretat de l'ENS
CBCS 1	Inventari i control de dispositius físics	op.exp.1
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	op.exp.1 op.exp.2
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	mp.sw.2 op.exp.4
CBCS 4	Ús controlat de privilegis administratius	op.acc.4 op.acc.5
CBCS 5	Configuracions segures del programari i maquinari, dispositius mòbils, portàtils, equips de taula i servidors	op.exp.2 op.exp.3
CBCS 6	Registre de l'activitat dels usuaris	op.exp.8 op.exp.10
CBCS 7	Còpies de seguretat de dades i sistemes	mp.info.9
CBCS 8	Compliment de la legalitat	ENS RGPD/LOPD Llei 25/2013

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

Els CBCS són controls globals formats per diversos subcontrols detallats que es mostren en la taula següent. Totes les nostres comprovacions tenen per finalitat contrastar la seua situació real en l'entitat amb les bones pràctiques recollides en la GPF-OCEX 5313, que es resumeixen en el quadre següent.

Els aspectes que es comproven en cada CBCS s'especifiquen amb el màxim detall en la GPF-OCEX 5313.

Quant als índexs o nivells objectiu que han d'aconseguir-se en cada CBCS i subcontrol, vegeu l'apartat 4 següent.

Quadre 3. Els CBCS i els seus subcontrols

Control	Objectiu de control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots el dispositiu 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 l'execució de programari no autoritzat.
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per a obtenir informació sobre noves vulnerabilitats, identificar-les, solucionar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats	Existeix 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 resoldre-les atenent el risc que suposen per a la seguretat del sistema.
		CBCS 3-3: Resolució de vulnerabilitats	Es realitza un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que 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, prevenir i corregir l'ús i la 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 control correcte.
		CBCS 4-2: Canvi de contrasenyes per defecte	Les contrasenyes per defecte dels comptes que no s'utilitzen, o bé que són estàndard, es canvien abans de l'entrada en producció del sistema.
		CBCS 4-3: Ús dedicat de comptes d'administració	Els comptes d'administració només es realitzen per a les tasques que són estrictament necessàries.
		CBCS 4-4: Mecanismes d'autenticació	Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes.
		CBCS 4-5: Auditoria i control	L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades.

Control	Objectiu de 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 dels dispositius mòbils, portàtils, servidors i de taula per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de prevenir 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 fer-ne la 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 l'anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de *logs*	Els *logs* de tots els sistemes es revisen periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels *logs* d'auditoria, de manera que se'n facilite la revisió.
		CBCS 6-4: Monitoratge i correlació	L'entitat disposa d'un SIEM (*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 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 efectuant 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 de legalitat	L'entitat compleix els requisits legals i reglamentaris que hi són aplicables.	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.

3. Confiança en les auditories de l'ENS

Atés que els CBCS estan alineats amb l'ENS, quan la seua revisió es realitze en entitats que hagen passat l'auditoria de seguretat obligatòria establida en l'article 34 del Reial Decret 3/2010, pel qual s'aprova l'ENS, la revisió podrà basar-se, en la mesura que siga possible, en els resultats d'aquesta auditoria i determinades comprovacions podran donar-se per acomplides.

Per a depositar confiança en aquestes auditories externes de seguretat, hauran de complir els requisits legalment establits com són, entre altres, que les entitats certificadores estiguen acreditades i constar en la secció "Entitats de certificació acreditades" del web del CCN (és necessària la seua acreditació si es pretén certificar el compliment de l'ENS). Quan s'haja depositat confiança en aquestes auditories s'assenyalarà expressament en l'informe.

4. Avaluació dels resultats del treball

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

Subcontrols

Els CBCS són controls globals compostos per diversos controls detallats o subcontrols (tal com es pot veure en l'apartat 2 anterior), dels quals hem revisat el disseny i l'eficàcia operativa.

El treball d'auditoria consisteix bàsicament a avaluar cada subcontrol en funció dels resultats de les proves realitzades i les evidències obtingudes, o bé de la informació proporcionada en l'informe d'auditoria de l'ENS, si existeix i si hi confiem. Cada subcontrol s'avalua segons l'escala mostrada en el quadre següent:

Quadre 4. 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 l'eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	A grans trets, compleix l'objectiu de control, si bé hi poden haver 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 pot no estar formalitzat. - El resultat de les proves d'implementació i d'eficàcia no és satisfactori. Cobreix a grans trets 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).

Nivell de maduresa dels CBCS

Per a determinar la situació global de cada CBCS 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 guia de seguretat CCN-STIC 804 del Centre Criptològic Nacional, usant una escala, tal com es resumeix en el quadre següent.

Quadre 5. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El CBCS no s'està aplicant en aquest moment.
N1 Inicial / *ad hoc*	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tenir personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan els 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. Hi ha 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 es gestiona en el nivell 3.*
N4 Gestionat i mesurable	90	La direcció controla i mesura l'acompliment 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, es revisen contínuament per a reflectir els canvis en els objectius de negoci i s'utilitzen com a indicadors en la gestió de la millora dels processos.* *En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes sobre la base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.*

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

Per a avaluar el nivell de maduresa de cada CBCS s'han tingut en compte els resultats obtinguts en la revisió dels subcontrols que el formen i considerant la ponderació o importància relativa que els assignem per al compliment de l'objectiu de control del CBCS.

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

La categoria d'un sistema és aplicable a tots els sistemes utilitzats per a la prestació dels serveis de l'administració electrònica i suport del procediment administratiu general.

A fi de poder determinar l'impacte que tindria sobre l'organització un incident que afectara la seguretat de la informació o dels sistemes, i de poder establir la categoria del sistema, cal tenir en compte les cinc dimensions de la seguretat:

- Confidencialitat. És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.

- Integritat. És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, i s'assegura que no se n'ha produït l'alteració, pèrdua o destrucció, tant de de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.

- Disponibilitat. És tracta de la capacitat d'un servei, un sistema o una informació de ser accessible i utilitzable pels usuaris o processos autoritzats quan ho requerisquen.

- Autenticitat. És la propietat o característica consistent en el fet que una entitat és la que 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'adscriu a un dels nivells següents: baix, mitjà o alt.

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

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

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

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

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

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[5]

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 estan classificats com de categoria mitjana.

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%.

6. Indicadors globals

Als efectes de l'ENS, la guia CCN-STIC-824 preveu una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics. Aquests indicadors s'han adaptat per a aplicar-los als CBCS, ja que permeten dur a terme tant un resum de l'estat de les mesures de seguretat de cada ajuntament als efectes de l'ENS com dels CBCS:

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

- 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.

[5] Informe nacional de l'estat de seguretat dels sistemes de les tecnologies de la informació i la comunicació de 2018, apartat 3.1. En els diferents perfils s'avaluen els controls per mitjà d'un nivell d'exigència, també conegut com a *nivell de maduresa*, i es fixa el nivell mínim d'exigència requerit.

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* d'aquesta Sindicatura, l'esborrany previ de l'Informe d'auditoria es va discutir amb els tècnics responsables de l'àrea de sistemes d'informació de l'Ajuntament de Sagunt per al seu coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*c* del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'Acord del Consell d'aquesta institució pel qual va tenir coneixement de l'esborrany de l'Informe d'auditoria corresponent a l'exercici 2019, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*h* del seu Reglament de Règim Interior i del Programa Anual d'Actuació de 2019 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 5 de març de 2020, va aprovar aquest informe d'auditoria.