SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME D'AUDITORIA DE CIBERSEGURETAT DE L'EMPRESA MUNICIPAL DE TRANSPORTS DE VALÈNCIA, SAU

Exercici 2020

RESUM

Per què realitzem aquesta auditoria

L'article 11 de la Llei de Sindicatura de Comptes estableix que, en el desenvolupament de la seua funció fiscalitzadora, la Sindicatura està facultada per a verificar la seguretat i fiabilitat dels sistemes informàtics que suporten la informació economicofinancera, comptable i de gestió. Cada vegada un major nombre d'aspectes de la gestió pública es realitza amb el suport de complexos sistemes i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de tota mena provinents del ciberespai, i s'han multiplicat els incidents de seguretat de què són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials tant econòmiques com en la prestació dels serveis públics. Addicionalment, en el Pla Estratègic de la Sindicatura de Comptes per al període 2019-2022 s'assenyala la ciberseguretat com una de les àrees d'alt risc i prioritàries per a dur a terme la tasca fiscalitzadora. Per aquesta raó s'ha realitzat una **auditoria de ciberseguretat** de l'Empresa Municipal de Transports de València, SAU, focalitzada en les àrees d'ingressos per transport de viatgers, de comptabilitat i de tresoreria, referida a la situació dels controls durant 2020.

Conclusions

Hem constatat un baix índex de maduresa dels controls de ciberseguretat, quantificat en un 51,5%, quan l'objectiu és del 80,0%.

Davant de la multiplicitat d'amenaces existents es requereix major conscienciació en relació amb la ciberseguretat per part dels òrgans superiors de l'EMT i més recursos dedicats a la seguretat de la informació, ja que l'esmena de les deficiències que s'assenyalen al llarg de l'informe requereix actuacions i inversions, tant en mitjans materials com personals.

És necessari actualitzar i reforçar la governança de la seguretat de la informació i alinear-la amb el que s'estableix en l'Esquema Nacional de Seguretat.

En l'auditoria hem observat que la situació dels controls d'accés privilegiat als sistemes s'ha de millorar, ja que hi ha greus deficiències en els controls relacionats amb els usuaris administradors d'alguns sistemes que proporcionen suport a processos crítics de negoci.

Recomanacions

A més de les deficiències de control significatives, que cal esmenar amb urgència, com a resultat de l'auditoria realitzada s'han efectuat 16 recomanacions per a l'atenció de les quals l'EMT ha de dedicar els esforços i recursos necessaris.

Resposta de l'entitat

Durant la fase d'al·legacions, la Direcció de l'EMT ha emfatitzat el procés de millora del sistema de seguretat de la informació emprés per l'entitat durant els dos exercicis anteriors i la seua intenció d'atendre les recomanacions realitzades.

Tant durant el transcurs del treball de camp de l'auditoria com en la fase d'al·legacions, l'EMT ens ha informat de l'adopció de diverses iniciatives per a esmenar deficiències observades, algunes esmenades i altres pendents en el moment d'emetre l'informe.

En les valoracions del nivell de maduresa dels controls, hem tingut en compte només les millores ja implantades i en funcionament en el moment de la nostra revisió, però hi ha altres iniciatives en marxa per a atendre bona part de les recomanacions que hem efectuat el disseny i l'eficàcia operativa de les quals es podran avaluar en un informe de seguiment posterior.

NOTA

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

Informe d'auditoria de ciberseguretat de l'Empresa Municipal de Transports de València, SAU

Exercici 2020

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX

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. Cada vegada més un major nombre d'aspectes de la gestió pública es realitza amb el suport de complexos sistemes, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de les amenaces de tota mena provinents del ciberespai, i s'han multiplicat els incidents de seguretat dels quals són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials, tant econòmiques com en la prestació dels serveis públics.

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

Considerant que les empreses públiques locals no són alienes a la problemàtica plantejada per la ciberseguretat, el Consell de la Sindicatura de Comptes va acordar incloure en el programa anual d'actuació de 2020 (PAA2020) la realització d'una auditoria de ciberseguretat de l'Empresa Municipal de Transports de València, SAU, focalitzada en les àrees d'ingressos per transport de viatgers, comptabilitat i de tresoreria.

El PAA2020 també estableix que la Sindicatura realitzarà una auditoria dels comptes de 2019 de l'EMT, centrada en les àrees d'ingressos per transport de viatgers i de la tresoreria, que es publicarà en un informe específic.

Consideracions sobre el frau experimentat per l'EMT

Durant l'exercici 2019, l'EMT ha sigut víctima d'un tipus d'estafa coneguda com a *frau del CEO*[1] que ha tingut com a conseqüència econòmica la pèrdua d'una quantitat superior a quatre milions d'euros.

A fi de dilucidar les deficiències de gestió i seguretat que han possibilitat la perpetració de l'estafa i depurar les responsabilitats sobre aquestes, s'han iniciat durant 2019 i 2020 una comissió d'investigació per part del Consell d'Administració de l'EMT, un procés judicial i una investigació del Tribunal de Comptes, treballs actualment en curs i els resultats dels quals es troben pendents de conclusió i/o publicació.

Aquesta auditoria no té com a objecte incidir en aquest frau i no seran revisats els fets concrets a través dels quals s'ha materialitzat l'estafa, que ja estan sent investigats pels organismes competents i no hem d'interferir en les actuacions judicials en curs.

No obstant això, i de conformitat amb l'enfocament de riscos recollit en les normes d'auditoria, durant la planificació i execució de l'auditoria sí que s'han tingut en consideració les circumstàncies generals del frau i hem inclòs en l'àmbit de la revisió les àrees d'interés relacionades amb els fets, en particular l'àrea de tresoreria, atesos els riscos de possible falta d'eficàcia dels controls de seguretat de la informació en aquesta àrea.

2. RESPONSABILITATS DELS ÒRGANS DE L'ENTITAT EN RELACIÓ AMB ELS CONTROLS DE CIBERSEGURETAT

El Ple de l'Ajuntament de València, òrgan que d'acord amb els Estatuts de l'EMT assumeix les funcions de la Junta General, té la responsabilitat d'impulsar en l'entitat, com a empresa subjecta al dret privat i la titularitat de la qual és 100% de l'Ajuntament, la implementació de mesures equivalents a l'Esquema Nacional de Seguretat (ENS).

D'altra banda, el Consell d'Administració de l'EMT és l'òrgan responsable que hi haja uns controls interns adequats, i és el **màxim responsable de la seguretat dels sistemes d'informació i les comunicacions**. D'acord amb les seues competències, el Consell ha de garantir que el funcionament de l'entitat resulte 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 complisquen les propietats següents, que coincideixen

[1] Segons el Centre Criptològic Nacional, "els atacs de *business email compromise* (BEC), habitualment coneguts com a *frau al CEO*, són un tipus d'atacs en auge en els últims anys, ja que requereixen en general poc coneixement tècnic i inversió en infraestructura –fonamentalment l'engany es basa en enginyeria social–, però poden arribar a reportar grans quantitats de diners als delinqüents".

"Aquest tipus de frau consisteix en el fet que un empleat d'alt rang o amb capacitat per a fer transferències o accés a dades de comptes rep un correu, suposadament del seu cap, ja siga el seu CEO, president o director de l'empresa. En aquest missatge li demana ajuda per a una operació financera confidencial i urgent. Si l'empleat no s'adona que és un missatge fraudulent podria respondre al seu suposat cap i caure en l'engany."

amb les cinc dimensions de la seguretat de la informació que estableix l'ENS: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.

La implicació del Consell i del director gerent és, potser, el factor més important per a la implantació amb èxit d'un sistema de gestió de la seguretat de la informació (SGSI). Aquesta s'ha de materialitzar en aspectes com ara:[2]

- Formular i aprovar la política de seguretat de la informació (PSI) i difondre-la a la totalitat dels membres de l'organització, així com, si és el cas, a proveïdors i clients.
- Assignar els rols i responsabilitats en seguretat de la informació.
- Proporcionar els recursos necessaris i assegurar que s'implanten programes de conscienciació, formació i capacitació.
- Decidir els criteris d'acceptació del risc i els nivells acceptables de risc.
- Autoritzar la implementació i operació de l'SGSI.
- Dirigir les revisions periòdiques de la PSI i vetlar per la realització de les auditories internes.

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls 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, com també que planifiquem i executem l'auditoria amb la finalitat d'obtindre una avaluació dels controls de ciberseguretat.

Àmbit objectiu

Aquesta fiscalització està focalitzada en la revisió d'una sèrie de controls de seguretat de les tecnologies de la informació i les comunicacions implantats en els sistemes que suporten dos dels processos de gestió més rellevants, relacionats amb sengles àrees que estan sent auditades per un altre equip de fiscalització de la Sindicatura. Aquestes àrees són la gestió de tresoreria (de molt alt risc, tal com han acreditat les circumstàncies dels

[2] *Guía de Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*.

últims mesos i s'han assenyalat en l'apartat 1 anterior) i els ingressos per transport de viatgers (activitat principal de l'entitat). També hem inclòs dins del nostre abast la comptabilitat.

Atés l'elevat risc d'aquestes àrees, l'auditoria de la ciberseguretat ha consistit en la revisió de dos grups de controls en aquestes àrees:

1. Revisió dels **controls bàsics de ciberseguretat (CBCS)**.

2. Revisió d'altres **controls generals de tecnologies de la informació rellevants** per a la seguretat de les aplicacions de gestió, addicionals als CBCS.

Considerem rellevants el conjunt de controls revisats perquè la seua absència o el mal funcionament representaria una deficiència significativa o una debilitat material de control intern i sobre la seguretat dels processos assenyalats.

En l'apèndix 1 es proporciona un major detall tant de l'àmbit objectiu de l'auditoria (quins controls s'han revisat) com de la metodologia utilitzada.

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls en 2020. La auditoria es va iniciar el 4 de juny de 2020 i el treball de camp va finalitzar el 30 de setembre de 2020.

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 les guies pràctiques de fiscalització *GPF-OCEX 5313 Revisió dels controls bàsics de ciberseguretat (CBCS)* i *GPF-OCEX 5330 Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica*, i en la resta de les seccions aplicables del *Manual de fiscalització* de la Sindicatura de Comptes. En total s'han revisat 53 subcontrols o controls detallats, agrupats en els 15 controls principals que s'assenyalen en el quadre 1.

Aquesta auditoria s'ha realitzat en coordinació amb un altre equip d'auditoria de la Sindicatura que està realitzant la fiscalització de regularitat, per al qual també hem revisat els controls interns informatitzats de les aplicacions de gestió relacionades i els resultats de la qual s'integraran en l'informe que emeten. Per a l'execució del treball també s'ha comptat amb la col·laboració d'experts externs.

Hem avaluat la situació dels controls 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'n l'evolució al llarg del temps. La metodologia utilitzada està plenament alineada amb el que estableix l'Esquema Nacional de Seguretat.

D'acord amb aquesta metodologia, els sistemes d'informació revisats estan classificats com de categoria de seguretat MITJANA, i el nivell de maduresa requerit o objectiu és *N3, procés definit*[3] i un índex de maduresa del 80%.

Confidencialitat

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

4. CONCLUSIONS

Baix índex de maduresa dels controls de ciberseguretat

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que el grau de control existent en la gestió dels controls de ciberseguretat assenyalats en l'apartat 3 aconsegueix un **índex de maduresa del 51,5%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls en general es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment.

L'índex de maduresa real està lluny de l'objectiu del 80% i del nivell de maduresa N3.

Agregant els resultats obtinguts per categories de controls, segons la classificació de controls inclosa en la *GPF-OCEX 5330 Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica*, s'obtenen els resultats detallats mostrats en el quadre 1.

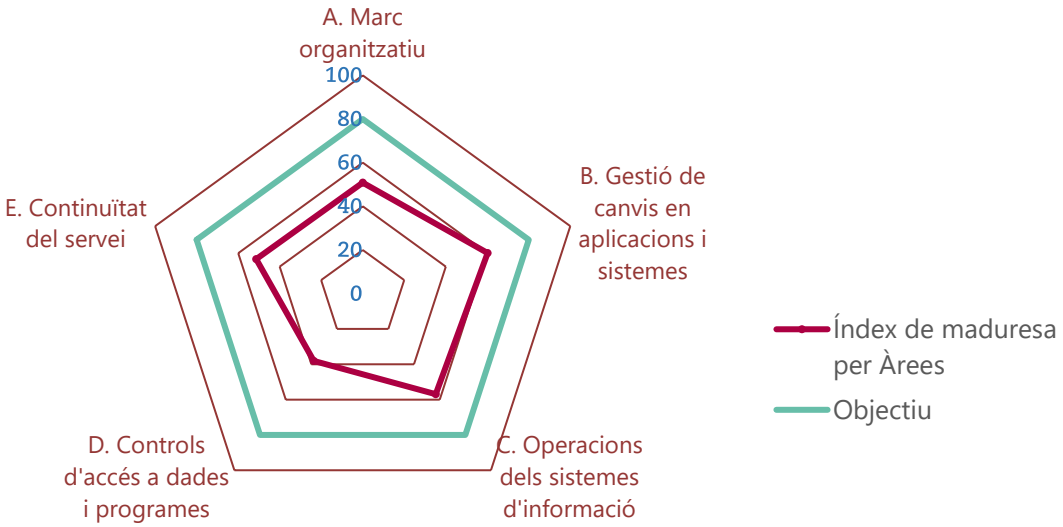
[3] Els nivells de maduresa es descriuen en el quadre 4 de l'apèndix 1.

Quadre 1. Índex de maduresa per àrees dels controls de ciberseguretat de l'EMT

Àrees	Controls principals	Índex de maduresa	
A. Marc organitzatiu	A.1 Compliment de legalitat (CBCS 8)	41,7%	**50,9% (N2)**
	A.3 Formació i conscienciació	60,0%	
B. Gestió de canvis en aplicacions i sistemes	B.3 Gestió de canvis	60,2%	**60,2% (N2)**
C. Operacions dels sistemes d'informació	C.1 Inventari de maquinari (CBCS 1)	63,8%	**56,9% (N2)**
	C.1 Inventari de programari (CBCS 2)	70,0%.	
	C.2 Gestió de vulnerabilitats (CBCS 3)	60,7%.	
	C.3 Configuracions segures (CBCS 5)	49,5%	
	C.4 Registre de l'activitat dels usuaris (CBCS 6)	51,8%	
	C.5 Serveis externs	49,8%	
	C.8 Gestió d'incidents	53,1%	
D. Controls d'accés a dades i programes	D.1 Ús controlat de privilegis administratius (CBCS 4)	38,6%	**38,1% (N1)**
	D.2 Mecanismes d'identificació i autenticació	40,3%	
	D.3 Gestió de drets d'accés	36,4%	
	D.4 Gestió d'usuaris	37,3%	
E. Continuïtat del servei	E.1 Còpies de seguretat de dades i sistemes (CBCS 7)	51,3%	**51,3% (N2)**
	General		51,5% (N2)

I d'una manera més sintètica i gràfica, la situació observada dels controls queda reflectida en el gràfic 1.

Gràfic 1. Índex de maduresa, per àrees, dels controls de ciberseguretat de l'EMT



Es requereix major conscienciació i més recursos dedicats a la seguretat de la informació

A la vista dels resultats obtinguts en la revisió dels controls de ciberseguretat, considerem que, **encara que existeix un cert nivell de control, hi ha possibilitats de millora, per la qual cosa és necessari que tant el Consell d'Administració com el Ple de l'Ajuntament de València, en la seua condició de junta general de la societat, 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 des dels òrgans de govern a tots els nivells i departaments de l'EMT.

L'esmena de les debilitats de control assenyalades i de les deficiències dels controls de ciberseguretat que s'assenyalen al llarg de l'informe requerirà actuacions i inversions, tant en mitjans materials com personals, que han de ser adequadament planificades.

Governança insuficient de la seguretat de la informació

L'EMT disposa d'una *Política de seguretat de la informació* (PSI), que **no ha sigut aprovada pel Consell d'Administració**, màxim òrgan de direcció de l'EMT, tal com requereixen l'ENS i la norma UNE-EN ISO/IEC 27001/27002, ni compleix tots els requisits establits en les dues normes.

La gestió de la seguretat dels sistemes d'informació requereix establir una organització de la seguretat, que ha de determinar amb precisió els diferents actors que la conformen, les seues funcions i responsabilitats, així com la implantació d'una estructura que les suporte i

els mecanismes de coordinació i resolució de conflictes, a més de designar un **comité de gestió de la seguretat de la informació**, de manera que la governança de la seguretat de la informació estiga adequadament estructurada.

La PSI que aprove el Consell d'Administració ha de recollir amb claredat les responsabilitats sobre la gestió, administració i seguretat dels sistemes descentralitzats (els gestionats de manera autònoma pels departaments), ja que la PSI actual no reflecteix fidelment les particularitats del model organitzatiu de l'entitat. L'administració de sistemes d'informació, que de manera general realitza l'Àrea de Desenvolupament, és assumida en determinats casos pels mateixos departaments de l'entitat, que administren les aplicacions específiques que suporten els processos crítics dels seus departaments. Aquesta situació no resulta recomanable, ja que dificulta la capacitat operativa del responsable de seguretat com a figura que ha de vetlar per l'aplicació homogènia de mesures de seguretat en el conjunt dels sistemes de l'entitat i la seua coherència en un entorn de sistemes administrats per diferents departaments. A més, existeix un risc elevat que els departaments no tinguen les competències professionals requerides per a l'administració de sistemes i que els interessos departamentals no es troben alineats amb els principis de la seguretat de la informació aprovats per l'organització.

La situació dels controls d'accés privilegiat s'ha de millorar

Hi ha greus deficiències en els controls relacionats amb els usuaris administradors dels sistemes, particularment en aquells gestionats de manera autònoma pels departaments corresponents (identificats més endavant en l'informe com a "sistemes descentralitzats") i que proporcionen suport a processos crítics de negoci.

Les mancances detectades, entre les quals destaquen una aplicació insuficient del principi de mínim privilegi i una gestió deficient dels registres d'activitat dels usuaris administradors, tenen un cost reduït de correcció i un alt impacte en el nivell general de ciberseguretat de l'entitat.

Durant el tràmit d'al·legacions, l'EMT ens ha informat de l'existència d'una proposta de treball per a la resolució d'aquestes deficiències. Hem verificat l'existència d'aquesta proposta i del pla de treball, que inclou les modificacions necessàries quant a la gestió adequada de drets d'accés i privilegis administratius dels usuaris, registres d'activitat i aplicació adequada del principi de mínim privilegi. Quan s'emet aquest informe, aquestes accions estaven en fase d'implantació.

Grau insuficient d'adequació a la normativa de ciberseguretat

La revisió del compliment de legalitat en matèria relacionada amb la ciberseguretat ha posat de manifest un nivell insatisfactori d'adequació a la normativa de ciberseguretat. L'Ajuntament de València i el Consell d'Administració de l'EMT tenen la responsabilitat d'impulsar un grau d'implementació de mesures equivalents a l'Esquema Nacional de Seguretat, en el marc del compliment de la normativa en matèria de protecció de dades, i han de promoure les accions necessàries per a esmenar aquesta situació.

Altres constatacions de l'auditoria

En l'apèndix 2 s'assenyalen les constatacions de l'auditoria que sustenten les conclusions d'aquest apartat, i les recomanacions es destaquen en l'apartat següent.

5. RECOMANACIONS

A més de les deficiències de control significatives assenyalades en l'apartat 4 anterior, que han de ser esmenades amb urgència, com a resultat de l'auditoria realitzada procedeix efectuar les recomanacions que s'assenyalen a continuació, per a l'atenció de les quals l'EMT 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 i que incloga les revisions periòdiques de maquinari i la seua actualització, incloses les dates d'aquestes revisions.

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

2. Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga:

   - L'elaboració de llistes de programari autoritzat (llistes blanques), la implantació de les mesures tècniques que impedisquen l'execució del no autoritzat i la realització de revisions periòdiques del programari.
   - La definició d'un pla de manteniment de la totalitat del programari utilitzat en l'entitat, incloent-hi tant el gestionat per part de l'EMT com el gestionat per part de tercers.
   - La revisió, identificació i actualització dels sistemes que es troben fora del període de suport.

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

3. Aprovar un procediment d'identificació i solució de vulnerabilitats que formalitze i amplie el procés actual, que s'aplique a la totalitat de sistemes de l'entitat 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 basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.

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

4. Formalitzar 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:

   - Aplicació del principi de mínim privilegi en l'assignació de permisos a usuaris en tots els sistemes d'entitat (això és especialment aplicable al departament financer).
   - 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 hauran de realitzar-se amb usuaris nominatius. Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.
   - La creació i utilització de diferents comptes per a un mateix usuari amb diferents nivells de privilegis administratius, adequant l'assignació de permisos als diferents tipus de tasques que calga realitzar.
   - Incloure els comptes per a administració de sistemes utilitzats pels serveis de manteniment externs.

5. Activar i gestionar els registres d'activitat en tots els sistemes de l'entitat, habilitant específicament els registres que detallen les accions dels usuaris administradors.

Sobre el control d'accés a dades i programes (D2, D3 i D4)

6. Finalitzar i aprovar el procediment de control d'accessos, actualment en estat d'esborrany, incloent-hi el detall necessari sobre la identificació i autenticació dels usuaris, la gestió i provisió de drets d'accés amb el principi del mínim privilegi i la gestió continuada. Aquest procediment ha de preveure tant els sistemes centralitzats com els descentralitzats.

7. Millorar el procés d'autenticació del sistema que suporta el procés comptable, per mitjà de la configuració adequada dels mecanismes i eines existents en la plataforma, i aplicar adequadament el criteri de mínim privilegi en l'assignació de drets d'accés a aquest sistema.

Sobre les configuracions segures del programari i maquinari (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, 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.[4]

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 la documentació d'un procés de revisió dels *logs*. Per a aquesta revisió és aconsellable la centralització de *logs* en sistemes dedicats a aquest efecte.

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

10. 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, les ubicacions, els responsables, les proves de restauració i els requisits de protecció de les còpies. La política de còpies de seguretat ha de basar-se en les necessitats de disponibilitat i conservació de la informació, requisits que hauran de ser especificats pels diferents serveis de l'entitat.

    El procediment ha de preveure la gestió del servei prestat pel proveïdor extern per a la realització de còpies, basat en l'establiment d'acords de nivell de servei entre les parts i el monitoratge d'indicadors.

Sobre la formació i conscienciació (A3)

11. Desenvolupar un pla de formació i conscienciació en matèria de seguretat de la informació que implique i motive els empleats, des dels llocs operatius fins a l'alta direcció, tenint present els riscos als quals s'exposen els diferents col·lectius i adaptant el contingut a cada un.

Sobre la gestió de canvis (B3)

12. Aprovar formalment un procediment per a la gestió contínua de qualsevol canvi en aplicacions i sistemes, tant en la seua configuració com en els components i arquitectura, que especifique i amplie les accions actualment implantades, que

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

definisca els rols necessaris per a assumir les diferents responsabilitats i que assigne els rols corresponents al personal competent per a això.

Sobre la gestió de serveis externs (C5)

13. Aprovar formalment un procediment per a la gestió contínua dels serveis externs contractats per l'EMT, que definisca tant els passos previs a la contractació del servei com les activitats de gestió durant la seua prestació, i que especifique el següent:

    - La definició de les característiques i requisits del servei, els requisits de seguretat, els acords de nivell de servei, les responsabilitats de les dues parts i les conseqüències de l'incompliment dels acords establits. En definitiva, és el contingut mínim aconsellable que ha de ser inclòs en els plecs de prescripcions tècniques.
    - Les activitats destinades a mesurar el compliment de les obligacions de servei i els acords de nivell de servei, així com el personal responsable de realitzar-les.

Sobre la gestió d'incidents (C8)

14. Aprovar formalment un procediment per a la gestió d'esdeveniments i incidents de seguretat que reculla el pla d'actuació després de la seua detecció. El procediment hauria d'incloure:

    - la definició dels rols necessaris per a assumir les diferents responsabilitats,
    - l'assignació d'aquests rols al personal competent,
    - l'escalat al responsable de la seua gestió,
    - la presa de decisions urgents,
    - l'assignació de recursos per a l'anàlisi, resposta i investigació dels incidents,
    - la comunicació a parts interessades internes i externes,
    - la implantació de mesures per a evitar incidents similars i
    - la millora contínua del procés de gestió.

Sobre el compliment de la legalitat (CBCS 8)

15. Implantar les mesures necessàries perquè el sistema de gestió de la seguretat de la informació de l'EMT siga coherent amb els requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat, o equivalents. Específicament, l'EMT ha de:

    - Actualitzar la *Política de seguretat de la informació* actual, de manera que satisfaça tots els requisits establits en l'ENS i/o s'adeqüe a les pràctiques de la norma UNE-

EN ISO/IEC 27001.[5] En especial, ha de ser aprovada pel Consell d'Administració, d'acord amb l'article 11 de l'ENS i les recomanacions de la norma UNE-EN ISO/IEC 27001.

- El Consell d'Administració ha de designar els diferents actors en matèria de seguretat de la informació, en particular el Comité de Seguretat de la Informació i el responsable de seguretat, entre altres. La gestió de la seguretat dels sistemes d'informació exigeix establir una organització de la seguretat, que ha de determinar amb precisió els diferents actors que la conformen, les seues funcions i responsabilitats, així com la implantació d'una estructura que les suporte i els mecanismes de coordinació i resolució de conflictes.[6]

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

    - Aplicar la totalitat de mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.
    - Planificar i executar les auditories de compliment en matèria de protecció de dades.

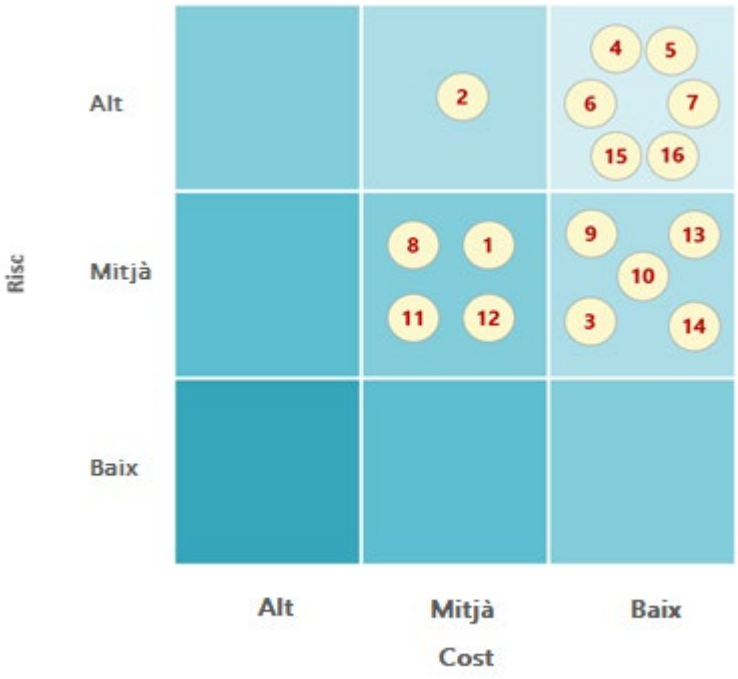
Priorització de les recomanacions

A fi que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic 2 següent es mostra la classificació de les recomanacions segons els criteris combinats de risc potencial que cal mitigar i cost de la seua implantació.

[5] *UNE-EN ISO/IEC 27001 Tecnologia de la informació. Tècniques de seguretat. Sistemes de gestió de la seguretat de la informació. Requisits*.

[6] Vegeu l'article 10 de l'ENS i la *Guia de seguretat de les TIC CCN-STIC 801 ENS Responsabilitats i funcions*.

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, hem comunicat als responsables de l'EMT altres recomanacions amb una relació de risc potencial que cal mitigar i cost de la seua implantació menys favorable que les anteriors.

Durant la fase d'al·legacions, la Direcció de l'EMT ha emfatitzat en el procés de millora del sistema de seguretat de la informació emprés per l'entitat durant els dos exercicis anteriors i en la seua intenció d'atendre les recomanacions realitzades. En les valoracions del nivell de maduresa dels controls hem tingut en compte només les millores ja implantades i en funcionament en el moment de la nostra revisió, a més d'haver-hi altres iniciatives en marxa, en fase de planificació o d'implantació, per a atendre bona part de les recomanacions que hem realitzat, el disseny i l'eficàcia operativa de les quals podran ser avaluades en un informe posterior de seguiment.

APÈNDIX 1
Metodologia aplicada

Àmbit objectiu

Aquesta fiscalització està focalitzada en la revisió de la ciberseguretat i els controls de tecnologies de la informació (TI) dels sistemes que suporten dos dels processos de gestió més rellevants, com són la gestió de tresoreria (de molt alt risc, tal com han acreditat les circumstàncies dels últims mesos en l'EMT) i els ingressos per transport de viatgers (activitat principal de l'entitat).

Les aplicacions identificades com a significatives per a la gestió dels processos de tresoreria i ingressos i sobre les quals s'han revisat els controls rellevants són les següents:

- CTI, per a la gestió dels ingressos per transport de viatgers.
- EXPERT, per a la gestió de la comptabilitat i tresoreria.

Atés l'elevat risc d'aquestes àrees, el treball ha consistit en la revisió de dos grans blocs:

Revisió dels controls bàsics de ciberseguretat (CBCS)

S'ha aplicat la metodologia establida en la *GPF-OCEX 5313, Revisió dels controls bàsics de ciberseguretat*, que inclou la revisió de set controls que han sigut degudament referenciats amb l'Esquema Nacional de Seguretat, i la verificació del compliment de diverses normes relacionades amb la seguretat de la informació.

Els huit CBCS establits en la GPF-OCEX 5313 són els següents:

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

La revisió ha inclòs els controls relacionats amb els sistemes identificats com a significatius per a la gestió dels processos de tresoreria i ingressos:

- les aplicacions informàtiques que suporten la gestió dels ingressos per transport de viatgers, la comptabilitat i la tresoreria,
- 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, s'han analitzat els tipus d'elements següents:

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

Revisió d'altres controls generals de TI rellevants per a les aplicacions de gestió dels processos de tresoreria i ingressos

Atés que hem qualificat el risc d'auditoria d'aquestes àrees com a ALT, hem considerat necessari ampliar els CBCS amb una altra sèrie de set CGTI addicionals, del total de controls detallats en la *GPF-OCEX 5330. Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica*. Aquests controls addicionals els considerem rellevants perquè la seua absència o el mal funcionament representa una deficiència significativa o una debilitat material de control intern sobre les aplicacions de gestió dels processos de tresoreria i ingressos, que estan sent auditats per un altre equip d'auditoria (i els nostres resultats els seran d'utilitat).

Els set controls, addicionals als CBCS, identificats com a rellevants per als objectius d'aquesta auditoria, són els següents:

- Formació i conscienciació (A.3.3)
- Gestió de canvis (B.3)
- Serveis externs (C.5)
- Gestió d'incidents (C.8)
- Mecanismes d'identificació i autenticació (D.2)
- Gestió de drets d'accés (D.3)
- Gestió d'usuaris (D.4)

Aplicabilitat de l'Esquema Nacional de Seguretat (ENS)

En el CBCS 8 s'ha revisat el compliment amb determinats aspectes que es consideren rellevants de la normativa bàsica en matèria de seguretat dels sistemes i de la informació.

És convenient aclarir que, atés que l'ens auditat és una societat mercantil, l'obligació sobre el compliment normatiu ha de ser matisada pels motius que exposem a continuació:

- L'EMT és una entitat de dret privat el capital de la qual és íntegrament públic, ja que pertany íntegrament a l'Ajuntament de València.

- L'àmbit subjectiu d'aplicació del Reial Decret 3/2010, de 8 de gener (modificat pel Reial Decret 951/2015), pel qual s'aprova l'Esquema Nacional de Seguretat, es troba determinat per les lleis 39/2015 i 40/2015. De l'anàlisi d'aquestes lleis es desprén que el Reial Decret 3/2010 serà aplicable a les entitats de dret privat vinculades o dependents de l'Administració de les entitats locals en les matèries en què els siga aplicable la normativa pressupostària, comptable, de control financer, de control d'eficàcia i contractació, d'acord amb el que es disposa en la Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local, així com en l'exercici de les funcions públiques que els hagen sigut atribuïdes estatutàriament, quan es regisquen per les previsions de la Llei 39/2015, d'1 d'octubre, de Procediment Administratiu Comú de les Administracions Públiques en els termes establits per aquesta.[7]

  A la vista dels articles 3 i 24 dels estatuts socials de l'EMT, aprovats el 31 de maig de 2013, **considerem que el Reial Decret 3/2010, de 8 de gener (ENS), no és d'aplicació directa en l'entitat**, atés que l'EMT no està subjecta a les disposicions de la Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local, i les funcions públiques que se li han atribuït estatutàriament no es regeixen per les previsions de la Llei 39/2015, d'1 d'octubre.

- La disposició addicional primera, "Mesures de seguretat en l'àmbit del sector públic", de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals, disposa el següent en el punt 2: "Els responsables enumerats en l'article 77.1 d'aquesta llei orgànica hauran d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguen de les previstes en l'Esquema Nacional de Seguretat, així com **impulsar un grau d'implementació de mesures equivalents en les empreses o fundacions vinculades als mateixos subjectes al dret privat**."

  Considerant que l'EMT inclou en el seu Registre d'Activitats del Tractament un total de 28 tractaments de dades personals relatives a 13 dels 14 processos de negoci identificats per l'empresa, podem inferir que el compliment de la disposició addicional primera, i per consegüent **el deure d'impulsar la implementació de mesures**

[7] Així es troba recollit en la *Guia CCN-STIC-830 Àmbit d'aplicació de l'Esquema Nacional de Seguretat*, del Centre Criptològic Nacional.

equivalents a l'ENS, és aplicable a la totalitat de matèries, processos i sistemes de l'EMT.

- La Sindicatura considera que la implementació de les mesures de seguretat recollides en l'ENS constitueix un requisit fonamental del control intern de les entitats públiques, atés que la seua implementació suposa *de facto* la implantació efectiva d'un sistema de gestió de la seguretat de la informació (SGSI) equivalent a l'impulsat per la norma UNE-EN ISO/IEC 27001.

Per les raons exposades, l'adequació a l'ENS s'ha inclòs en aquest treball com a part fonamental per a la valoració del nivell de maduresa del control intern, així com el compliment del deure d'impulsar un grau d'implementació de mesures equivalents a l'ENS en l'EMT per part dels òrgans superiors de l'EMT.

Les GPF-OCEX 5313, GPF-OCEX 5330 i l'Esquema Nacional de Seguretat

Aquesta auditoria està basada en les guies pràctiques de fiscalització ***GPF-OCEX 5313 Revisió dels controls bàsics de ciberseguretat*** i ***GPF-OCEX 5330 Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica***, aprovades per la Conferència de Presidents dels Òrgans de Control Extern (OCEX) el 12/11/2018, que formen part del *Manual de fiscalització* de la Sindicatura de Comptes i que poden consultar-se en el nostre web. Per a més detall sobre la metodologia utilitzada ens remetem a aquestes guies.

El contingut de les dues guies, 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 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 estan exigits per l'ENS.

Els controls generals de TI inclouen els CBCS i comprenen, de manera general, la totalitat dels requisits previstos en l'ENS. Els controls generals de TI es classifiquen de la manera següent:

Quadre 2. Els controls generals de tecnologies de la informació i l'ENS

	Controls generals de TI	Mesures de seguretat de l'ENS
A. Marc organitzatiu	**A.1 Compliment de legalitat (CBCS 8)**	org.1
	A.2 Estratègia de seguretat	org.2
	A.3 Organització i personal de TI	
	A.4 Marc normatiu i procedimental de seguretat	mp.per
B. Gestió de canvis en aplicacions i sistemes	B.1 Adquisició d'aplicacions i sistemes	
	B.2 Desenvolupament d'aplicacions	mp.sw.1 i 2
	B.3 Gestió de canvis	op.exp.5
C. Operacions dels sistemes d'informació	**C.1 Inventari de maquinari (CBCS 1)**	op.exp.1
	C.1 Inventari de programari (CBCS 2)	op.exp.1 i 2
	C.2 Gestió de vulnerabilitats (CBCS 3)	op.exp.3 i 4
	C.3 Configuracions segures (CBCS 5)	op.exp.2 i 3
	C.4 Registre de l'activitat dels usuaris (CBCS 6)	op.exp.8 i 10
	C.5 Serveis externs	op.ext.1 i 2
	C.6 Protecció davant de programari maliciós	op.exp.6
	C.7 Protecció de les instal·lacions i infraestructures	mp.if
	C.8 Gestió d'incidents	op.exp.7 i 9
	C.9 Monitoratge	
D. Controls d'accés a dades i programes	**D.1 Ús controlat de privilegis administratius (CBCS 4)**	op.acc.4
	D.2 Mecanismes d'identificació i autenticació	op.acc.1 i 5
	D.3 Gestió de drets d'accés	op.acc.4
	D.4 Gestió d'usuaris	op.acc
	D.5 Protecció de les xarxes i comunicacions	mp.com
E. Continuïtat del servei	**E.1 Còpies de seguretat de dades i sistemes (CBCS 7)**	mp.info.9
	E.2 Pla de continuïtat	op.cont.2 i 3
	E.3 Alta disponibilitat	mp.if.9

L'auditoria de les 15 àrees assenyalades en negreta en el quadre anterior ha inclòs la revisió de 53 subcontrols o controls detallats.

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

Els CBCS i els controls generals de TI són controls globals formats per diversos subcontrols detallats. Totes les nostres comprovacions tenen per finalitat contrastar la seua situació real en

l'entitat amb les bones pràctiques recollides en les GPF-OCEX 5313 i 5330, en les quals s'especifica amb el màxim detall els aspectes comprovats en cada control.

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

Avaluació dels resultats del treball

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

Subcontrols

Els CBCS i els controls generals de TI 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 3. 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	A grans trets, 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-ne 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 en línies generals l'objectiu de control, però: No se segueix un procediment clar. Les proves realitzades per a verificar-ne 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 controls

Per a determinar la situació global de cada control de ciberseguretat hem utilitzat el model de nivell de maduresa dels processos de control d'acord amb el que s'estableix en les *GPF-OCEX 5313* i *GPF-OCEX 5330*, que al seu torn estan basades en *Guia de seguretat CCN-STIC 804* del CCN, usant una escala, tal com es resumeix en el quadre següent.

Quadre 4. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El control no s'està aplicant en aquest moment.
N1 Inicial / ad hoc	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. *L'eficàcia del procés depén de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.*
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. *Es disposa d'un catàleg de processos que es manté actualitzat. Aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant els incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor del desconegut (o no planificat).* *L'èxit és alguna cosa 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 a 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 control 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.

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

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

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

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

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

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, s'han de tindre 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, assegurant que no se n'ha produït l'alteració, pèrdua o destrucció, siga de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.

Disponibilitat	Es tracta de la capacitat d'un servei, un sistema o una informació de ser accessible i utilitzable pels usuaris o processos autoritzats quan aquests ho requerisquen.
Autenticitat	És la propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.
Traçabilitat	És la propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

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

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

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

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

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

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

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[8]

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.

[8] 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.

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

Indicadors globals

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 aplicar-los als CBCS i controls generals de TI, ja que permeten dur a terme tant un resum de l'estat de les mesures de seguretat dels ens auditats als efectes de l'ENS com dels CBCS i controls generals:

- 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.

Dates de l'auditoria

Els treballs d'auditoria es van iniciar al juny de 2020 i van finalitzar al novembre de 2020. Considerem com a fi del treball de camp la data en la qual les constatacions de l'auditoria, les conclusions i l'esborrany previ de l'informe es discuteixen amb els responsables de l'entitat auditada, d'acord amb el que s'estableix en el nostre *Manual de fiscalització*, ja que fins a aquest moment s'admet qualsevol evidència addicional disponible. Per tant, l'informe reflecteix amb caràcter general la situació en aquest moment, ja que és freqüent que, des que s'inicia el treball de camp, determinades deficiències observades i assenyalades als gestors siguen esmenades i considerades d'aquesta manera en les conclusions i en els indicadors.

Finalment, l'informe és sotmés al procediment contradictori de manera formal per mitjà del tràmit d'al·legacions.

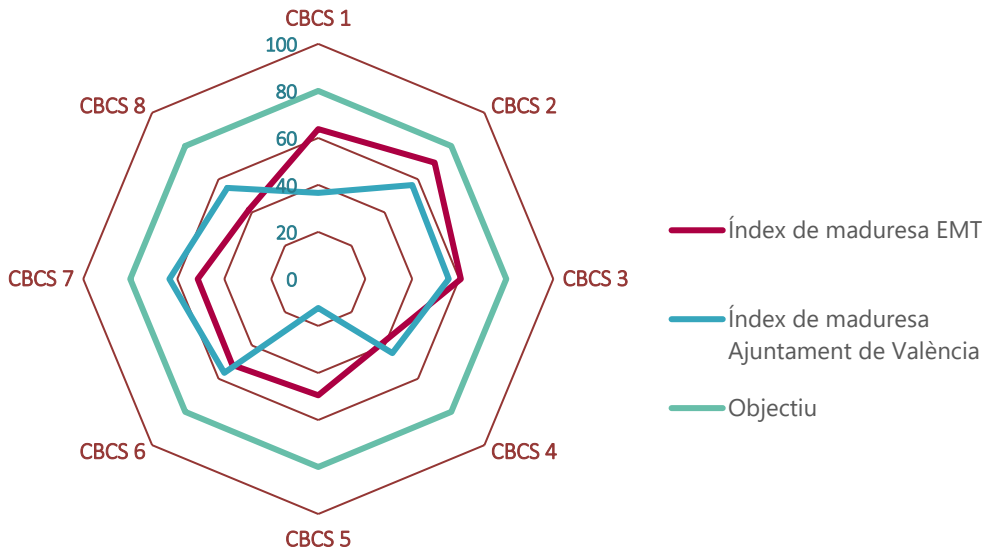
APÈNDIX 2
Situació observada dels controls

A continuació s'assenyalen els principals aspectes sorgits en la revisió dels controls de ciberseguretat de l'EMT. Atés que la informació utilitzada en l'auditoria i els seus resultats detallats 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'EMT perquè puguen adoptar les mesures correctores que consideren necessàries. En aquest apèndix els resultats es mostren de manera sintètica.

1. Situació comparativa dels CBCS

Per a realitzar una anàlisi comparativa en termes homogenis de la situació dels controls de ciberseguretat de l'EMT amb la seua entitat matriu, hem considerat el subconjunt dels CBCS, del total de controls de seguretat que hem revisat en aquesta auditoria, que coincideixen amb els que vam revisar a l'Ajuntament de València, l'informe dels quals[9] es va publicar al març de 2020. El gràfic 3 següent presenta els resultats comparats obtinguts en la revisió dels CBCS en les dues entitats.

Gràfic 3. Comparativa de l'índex de maduresa dels controls bàsics de ciberseguretat de l'EMT i de l'Ajuntament de València



L'índex mitjà de maduresa dels CBCS ha sigut del 53,4% en l'EMT i del 47,5% a l'Ajuntament de València; en els dos casos la situació dels controls de ciberseguretat és clarament millorable i no es pot considerar que els sistemes d'informació estiguen degudament protegits.

[9] Vegeu Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València. Exercici 2019.

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

Hem verificat que l'EMT realitza accions per a l'inventari i control d'actius físics de l'entitat, i que en garanteix un control efectiu. La responsabilitat de l'inventari de dispositius es troba establida en l'Àrea de Desenvolupament, amb el suport d'un proveïdor extern. No obstant això, el procés no s'ha detallat en un procediment formalment aprovat.

L'EMT disposa d'un inventari de gestió automatitzada per a l'administració dels actius, que inclou tots els elements de maquinari propietat de l'entitat: servidors, equips d'usuaris, dispositius de xarxa, telèfons mòbils, monitors, impressores, etc. No obstant això, els dispositius de xarxa s'introdueixen en l'inventari de manera manual, no automatitzada.

Les màquines virtuals no s'inclouen en aquest inventari ni tampoc es troben inventariades per cap altre sistema. Aquesta mancança pot limitar l'aplicació posterior d'altres controls de seguretat rellevants sobre els dispositius no controlats.

D'altra banda, si bé no es disposa d'un sistema que impedisca la connexió de dispositius físics no autoritzats a la xarxa, sí que es disposa de diferents controls compensatoris robustos que detecten, impedisquen o limiten l'activitat dels dispositius físics no autoritzats en el sistema d'informació.

En síntesi, hi ha un cert nivell de control sobre l'inventari de dispositius físics i la valoració global del control aconsegueix un índex de maduresa del 63,8%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

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

Hem analitzat la gestió que realitza l'EMT sobre l'inventari i control de programari i hem verificat que, encara que la responsabilitat de l'inventari de programari es troba establida en la política de seguretat vigent per mitjà del requisit de mantindre un inventari d'actius, el procés implantat no s'ha detallat en un procediment formalment aprovat.

L'EMT disposa d'un inventari de gestió automatitzada per a l'administració dels actius, entre els quals s'inclou el programari gestionat per l'Àrea de Desenvolupament. L'inventari inclou, entre altra informació, el programari instal·lat en els dispositius de l'entitat, la versió, el nombre de llicències disponibles i el nombre de llicències instal·lades.

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

La gestió del llicenciament i el manteniment d'aplicacions es realitzen per mitjà d'un procés adequat, però no formalitzat.

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

Considerem que hi ha un cert nivell de control sobre l'inventari i el programari autoritzat, però hi ha possibilitats de millora. La valoració global del control aconsegueix un índex de maduresa del 70,0%, 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.

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

Hem analitzat la gestió de vulnerabilitats realitzada per l'EMT i hem observat que es realitzen diferents accions a fi d'identificar i solucionar vulnerabilitats. A pesar que aquestes accions s'han implantat de manera efectiva en tots els sistemes, no s'han documentat formalment i aprovat.

La identificació de vulnerabilitats es realitza sobre tots els sistemes que hem revisat, per mitjà de la realització d'exercicis de *hacking* ètic per part de tercers gràcies a contractes de manteniment, a través d'eines que permeten la identificació automàtica de vulnerabilitats i per mitjà de subscripció a llistes de difusió de fabricants i organismes de referència.

El procés de priorització i resolució, encara que parcialment efectiu, es gestiona de manera informal, atés que no es troba recollit en un procediment, ni s'utilitzen eines específiques de priorització de vulnerabilitats o eina de *workflow*.

Sobre l'aplicació de pedaços i actualitzacions de seguretat, aquests s'apliquen de manera sistemàtica sobre els sistemes adquirits a proveïdors i l'actualització dels quals s'estableix en els contractes de manteniment amb tercers. Es disposa d'eines que permeten la gestió centralitzada d'actualitzacions i pedaços de seguretat dels sistemes Windows i dels elements de l'electrònica de xarxa.

Considerem que hi ha un cert nivell de control, però hi ha possibilitats de millora. La valoració global del control aconsegueix un índex de maduresa del 60,7%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

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

Hem analitzat les accions que realitza l'EMT per al control dels comptes d'administració i hem verificat que no n'hi ha un control efectiu i fiable.

La gestió de l'assignació de privilegis administratius en els sistemes revisats es realitza amb diferent grau d'efectivitat depenent del sistema i de manera independent per a cada un, atés que no ha sigut formalment aprovat ni implantat un procediment que establisca les polítiques comunes de gestió de privilegis administratius per al conjunt de sistemes de l'EMT. La gestió de privilegis administratius la realitza l'Àrea de Desenvolupament, excepte per a determinades aplicacions dels sistemes descentralitzats, que són directament administrats pels responsables dels departaments afectats i que suporten processos crítics de l'entitat.

S'ha detectat l'ús de comptes no nominatius compartits en alguns dels sistemes revisats, la qual cosa dificulta la traçabilitat de les accions en cas d'incidents. Aquesta deficiència es troba parcialment compensada per un adequat inventari i control en l'ús dels comptes.

S'han identificat com a deficiències greus de control la inadequada aplicació del principi de mínim privilegi en aplicacions descentralitzades que suporten processos crítics de negoci, la configuració incorrecta dels comptes d'administració dels serveis de manteniment externs de determinats sistemes revisats i un control insuficient en la definició i gestió dels mecanismes d'autenticació utilitzats pels sistemes.

Únicament es fa una correcta aplicació de l'ús dedicat de comptes d'administració en sistemes gestionats per l'Àrea de Desenvolupament.

El registre de l'activitat dels usuaris administradors tampoc es troba correctament configurat en els sistemes descentralitzats, la qual cosa representa una greu deficiència de control que dificulta la gestió en cas d'incident de seguretat. Per a la resta dels sistemes revisats, gestionats per l'Àrea de Desenvolupament, si bé no existeix un procés sistemàtic per a realitzar una configuració específica i homogènia dels registres d'activitat dels administradors, aquests registres es troben activats i són emmagatzemats i gestionats.

Considerem que hi ha un deficient nivell de control sobre els comptes d'usuaris administradors, per la qual cosa s'haurà de dedicar esforços i recursos per a millorar-lo. La valoració global d'aquest control aconsegueix un índex de maduresa del 38,6%, que es correspon amb un nivell de maduresa *N1, inicial / ad hoc;* és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada.

6. Sobre el control d'accés a dades i programes (D2, D3, D4)

Hem analitzat les accions de l'organització per al control dels accessos dels comptes d'usuari sobre els sistemes que suporten els processos de comptabilitat i ingressos i hem verificat que no n'hi ha un control totalment efectiu.

La responsabilitat de la gestió d'usuaris, els seus privilegis i el control dels accessos als sistemes es troba parcialment establida en la política de seguretat aprovada. No obstant això, aquesta no s'ha desenvolupat en un procediment que detalle les accions necessàries.

Els mecanismes utilitzats per a la identificació i autenticació d'usuaris poden considerar-se efectius o parcialment efectius en els dos sistemes. No obstant això, s'han identificat clares oportunitats de millora amb un cost d'implantació reduït, particularment en el procés d'autenticació de l'aplicació comptable. El procés d'identificació i autenticació de l'aplicació d'ingressos ha sigut recentment redissenyat i permet l'autenticació única (*single sign-on*) amb el directori actiu, a més de proporcionar majors nivells d'automatització per a l'usuari i compensar parcialment algunes de les mancances i oportunitats de millora identificades.

La gestió d'usuaris és adequada o parcialment adequada en els dos sistemes. Hem verificat que en l'aplicació comptable únicament es troben habilitats els comptes d'aquells usuaris

que per les seues funcions han de fer ús de l'eina i que s'ha implantat un procés de gestió d'usuaris de manera informal però efectiva.

En el cas del sistema que suporta els ingressos, hem identificat que no existeix un procés de gestió i revisió d'usuaris locals al sistema, fet que suposa una deficiència de control significativa. No obstant això, la implantació de l'autenticació única amb el directori actiu i de mesures de limitació d'accés en l'electrònica de seguretat de xarxa compensen parcialment o totalment els riscos derivats de la deficiència detectada.

La gestió de drets d'accés no aconsegueix els nivells de control adequats, particularment per a l'aplicació comptable. Hem evidenciat que en aquest sistema no s'ha aplicat adequadament el criteri de mínim privilegi en l'exercici de provisió de drets d'accés als usuaris, i aquesta és una deficiència de control que considerem significativa. Hem evidenciat que es troba en curs una modificació dels perfils de determinats usuaris per a adequar els seus privilegis als requeriments dels seus llocs de treball. Durant la fase d'al·legacions, se'ns ha informat de l'existència d'una proposta i pla de treball per a fer extensiva aquesta modificació a tots els usuaris del sistema. Hem verificat la documentació que suporta l'existència d'aquest pla de treball i que aquesta iniciativa es troba en fase d'implantació en el moment d'emetre aquest informe.

En el cas de l'aplicació d'ingressos, únicament disposa de mecanismes limitats per a l'adequació dels drets d'accés als llocs de treball dels usuaris. No obstant això, hem verificat que, en la mesura de les capacitats del sistema, sí que s'ha realitzat una aplicació correcta del criteri de mínima funcionalitat en la gestió de drets d'accés als usuaris.

En síntesi, hi ha un deficient nivell de control sobre l'accés dels usuaris a dades i programes i la valoració global del control aconsegueix un índex de maduresa del 38,0%, que es correspon amb un nivell de maduresa *N1, inicial / ad hoc*; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada.

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

Hem analitzat les accions realitzades per al control de la configuració segura en aplicacions i dispositius i hem verificat que no existeix un procediment formalment aprovat a aquest efecte. L'entitat realitza accions per a aplicar una configuració de seguretat en determinats sistemes, però aquestes accions no són suficients per a assegurar l'efectivitat del control.

Encara que s'ha evidenciat que es disposa de plantilles per a la configuració de determinats dispositius, aquestes plantilles no tenen caràcter de fortificació ni la seguretat per defecte és el seu objecte.

L'entitat disposa d'un entorn de preproducció utilitzat en el procés de gestió de canvis i per a la realització de proves de seguretat en determinats sistemes.

Sobre el monitoratge de les configuracions existents, s'ha establit un control parcialment efectiu sobre els equips d'usuari de l'entitat per mitjà de l'ús combinat de dues de les eines de seguretat implantades.

Hi ha, per tant, un nivell insuficient de control en l'aplicació de configuracions segures en dispositius i programari, per la qual cosa s'haurà de dedicar esforços i recursos per a millorar-la. La valoració global del control aconsegueix un índex de maduresa del 49,5%, 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.

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

Hem analitzat els procediments aplicats per l'EMT per al registre de l'activitat dels usuaris en els diferents sistemes i hem verificat que, encara que es disposa de certs controls relacionats amb aquest procediment, no han sigut formalitzats i aprovats.

Hem verificat que el registre d'activitat es troba activat en la major part dels sistemes revisats, encara que es manté la configuració per defecte que defineix el fabricant.

No obstant això, hem detectat un sistema descentralitzat en el qual, si bé es disposa de funcionalitats que permeten l'activació i emmagatzematge de registres d'activitat, no es troben habilitades. Aquesta mancança suposa una deficiència greu de control, atés que impedeix la traçabilitat de les accions dels usuaris i particularment d'aquells que disposen de privilegis administratius sobre el sistema.

L'EMT disposa de diversos sistemes per a la gestió centralitzada de registres d'activitat de determinats actius, la qual cosa suposa una millora de la configuració bàsica per defecte dels *logs* d'auditoria. No obstant això, aquestes eines no s'integren en 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.

Addicionalment, es disposa d'un sistema de seguretat específic que, encara que no pot ser considerat un SIEM[10] per les seues especificacions tècniques i funcionals, sí que disposa de capacitats avançades de correlació d'incidències i intel·ligència artificial que li permeten la detecció de vulneracions de seguretat sobre la base de l'anàlisi de les dades disponibles.

La valoració d'aquest control aconsegueix un índex de maduresa del 51,8%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però n'hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

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

L'EMT realitza diverses accions per al control de les còpies de seguretat de les dades i sistemes. No obstant això, els controls implantats no es consideren suficients per a estimar que el procés resulte completament efectiu i, addicionalment, aquest no es troba recollit en un procediment documentat i formalment aprovat.

[10] Sistema de gestió d'incidències i informació de seguretat.

El control de còpies de seguretat es troba completament delegat en un proveïdor extern. La solució implantada disposa de les característiques tècniques adequades per a un procés de realització de còpies de seguretat d'acord amb les necessitats de l'organització. No obstant això, hem verificat que el plec de prescripcions tècniques no detalla els requisits de seguretat ni especifica tots els aspectes necessaris per a assegurar la correcta provisió del servei. De la mateixa manera, la supervisió per part de l'EMT del proveïdor extern i dels serveis rebuts no resulta adequada, atés que no es realitza un seguiment dels nivells de servei per mitjà d'indicadors acordats.

Les polítiques de còpies de seguretat aplicades als sistemes situats en el centre de processament de dades (CPD) de l'EMT les ha desenvolupat el proveïdor extern sense la realització d'una anàlisi prèvia que identifique les necessitats dels diferents serveis, situació que pot comportar l'aplicació d'un conjunt de polítiques de còpia que no satisfaça completament les necessitats de l'organització.

S'ha confirmat que no es realitzen de manera sistemàtica proves de recuperació planificades, si bé hem confirmat que s'han dut a terme recuperacions satisfactòries en les ocasions que s'ha requerit.

Respecte a la protecció de les còpies de seguretat, hem verificat que inclou diferents mecanismes efectius destinats per a això, però pot resultar recomanable l'aplicació de mesures addicionals per a augmentar la protecció davant de determinats riscos als quals es troben exposats els sistemes d'informació, que han sigut comunicats als responsables de l'EMT.

La valoració global del control aconsegueix un índex de maduresa del 51,3%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però n'hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

10. Sobre la formació i conscienciació (A3)

Hem analitzat el procés que segueix l'EMT respecte a la formació i conscienciació del personal en matèria de seguretat de la informació i hem verificat que, encara que s'apliquen mesures relacionades amb aquest aspecte, no han sigut formalment establides per mitjà d'un procediment documentat i aprovat, ni s'inclou l'obligació de dur a terme aquest tipus d'accions en *PSI*.

Les accions de l'EMT relatives a la conscienciació en seguretat de la informació consisteixen principalment en l'enviament de píndoles informatives (comunicacions informatives breus) a partir de publicacions i alertes emeses des de grups d'interés com INCIBE, CCN-CERT i organitzacions de seguretat reconegudes. Aquests enviaments es realitzen de manera periòdica en un procés organitzat i de manera reactiva davant de determinats anuncis i alertes d'interés per a l'organització.

L'EMT es troba en fase de planificació d'un projecte de formació i conscienciació en matèria de seguretat de la informació, en el qual està previst involucrar de manera pràctica tots els

empleats de l'entitat. Sobre la base dels resultats obtinguts en una primera fase d'identificació de vulnerabilitats i deficiències de caràcter humà en les diferents àrees de l'organització, s'estendran les activitats de formació en funció de les necessitats i mancances identificades. Aquest projecte es gestiona de manera conjunta per l'Àrea de Desenvolupament i per la de Recursos Humans.

La valoració global d'aquest control aconsegueix un índex de maduresa del 60,0%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però n'hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

11. Sobre la gestió de canvis (B3)

Hem analitzat les accions respecte al procés de gestió de canvis que segueix l'EMT i hem verificat que, a pesar de no disposar d'un procediment documentat i aprovat formalment a l'efecte, el control resulta efectiu.

S'ha evidenciat que tant els canvis requerits i executats per la mateixa entitat com els canvis sol·licitats per l'EMT i executats per proveïdors es registren i es gestionen per mitjà d'eines automatitzades.

Tots els canvis segueixen el procés de registre, avaluació, aprovació, planificació i execució, en un procés de gestió que pot considerar-se adequadament dissenyat i executat.

Per als canvis que així ho requereixen, la gestió del canvi inclou una fase de realització de proves en entorns de preproducció, entorns que disposen de les mateixes mesures de seguretat que els sistemes productius i en els quals es realitza l'anonimització de les dades en cas de ser necessari.

En analitzar els canvis inclosos en el mostreig, hem pogut observar que, al llarg del seu cicle de vida, intervenen diferents usuaris amb diferents responsabilitats, a pesar que no hagen definit responsables i/o constituït òrgans de gestió de manera formal. De la mateixa manera, durant l'avaluació del canvi es té en compte l'aprovació per part del sol·licitant i la seua implicació en matèria de seguretat de la informació.

Considerem que hi ha un cert nivell de control sobre la gestió de canvis, però hi ha possibilitats de millora. La valoració global d'aquest control aconsegueix un índex de maduresa del 60,2%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però n'hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

12. Sobre la gestió de serveis externs (C5)

Hem analitzat les accions realitzades per a la gestió dels serveis externs i hem verificat que no n'hi ha un procediment formalment aprovat. L'entitat realitza accions que impliquen l'aplicació de mesures destinades a l'efecte, però aquestes accions no són suficients per a assegurar l'efectivitat del control.

S'ha evidenciat que en els plecs de contractació de serveis s'inclouen clàusules on s'especifiquen les característiques i requisits del servei, els acords de nivell de servei, les responsabilitats de les dues parts, les conseqüències de l'incompliment dels acords i, a més d'això, els requisits de confidencialitat i de compliment de la normativa existent en matèria de protecció de dades personals. No obstant això, hem verificat que en determinats plecs hi ha un nivell insuficient de detall i no s'hi inclouen els continguts mínims imprescindibles, fet que impedeix assegurar la provisió d'un nivell de servei que satisfaça les necessitats de l'organització.

D'altra banda, per als proveïdors que així ho requereixen, no s'inclou l'obligació que els serveis prestats per aquests siguen conformes a l'Esquema Nacional de Seguretat i que, a més, disposen de les certificacions de seguretat corresponents.

Així mateix, l'EMT no ha establit formalment un sistema rutinari per a mesurar el compliment de les obligacions i nivells de servei per part dels proveïdors que es trobe basat en els acords formalment disposats i en el mesurament d'aquests nivells de servei per mitjà d'indicadors establits.

En conclusió, hi ha un nivell de control insuficient sobre els serveis externs i la valoració global del control aconsegueix un índex de maduresa del 49,8%, 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.

13. Sobre la gestió d'incidents (C8)

Hem analitzat les accions respecte al procés de gestió d'incidents que segueix l'EMT i hem verificat que, a pesar de no disposar d'un procediment documentat i aprovat formalment a l'efecte, s'han implantat mesures i es duen a terme actuacions amb les quals el control resulta parcialment efectiu, tant en la detecció d'incidències com en la seua gestió i comunicació.

L'EMT disposa de diferents eines destinades a la detecció i gestió d'esdeveniments i incidents de seguretat, així com un servei extern de seguretat gestionada prestat pel centre d'operacions de seguretat (SOC) d'un proveïdor, i proporciona de manera conjunta un adequat nivell de control per a la detecció d'incidències.

Com a norma general, el responsable del Negociat de Sistemes i Aplicacions, amb el suport de l'equip de suport tècnic, és l'encarregat de gestionar els esdeveniments i incidents ordinaris de seguretat informàtica.

Per als incidents que es consideren rellevants, bé pel seu impacte o bé per requerir actuacions amb caràcter d'urgència, s'ha constituït un equip de crisi compost per responsables de diferents negociats per a la presa de decisions. Encara que aquest comité s'ha utilitzat de manera efectiva en determinades ocasions, la seua organització i funcionament no es troben establides en un procediment, formal o informal.

S'ha inclòs en el procés d'actuació de resposta a l'incident una anàlisi de la causa arrel, de la qual s'obté un informe que inclou tant les constatacions identificades durant l'anàlisi com una proposta d'actuacions i mesures tècniques per a evitar futurs atacs similars. Aquest informe, elaborat per a determinats incidents, es transmet al responsable del sistema afectat i al director gerent.

No obstant això, no es du a terme una anàlisi destinada a l'optimització del procés de gestió d'incidents, així com tampoc s'identifiquen totes les parts interessades a fi de comunicar-los els fets esdevinguts.

La valoració global d'aquest control aconsegueix un índex de maduresa del 53,1%, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però n'hi ha controls parcialment establits o els procediments no s'han formalitzat degudament.

14. Sobre el compliment normatiu (CBCS 8)

L'entitat no aconsegueix un nivell satisfactori d'adequació a la normativa legal, per la qual cosa la valoració global sobre el compliment dels aspectes de legalitat que hem verificat és que l'EMT aconsegueix un índex de maduresa del 41,7%. Això es correspon amb un nivell de maduresa *N1*, que indica que hi ha una falta d'observació generalitzada de la normativa.

En relació amb l'ENS

L'EMT no ha realitzat accions específicament orientades a aconseguir un grau d'implementació de mesures de seguretat equivalents als requisits de l'Esquema Nacional de Seguretat. No obstant això, es troba en fase d'implantació d'un sistema de gestió de la seguretat de la informació (SGSI) basat en l'aplicació de la sèrie UNE-ES ISO/IEC 27000, que conté les millors pràctiques recomanades en seguretat de la informació i que resulta en gran manera equivalent a l'ENS.

S'ha formalitzat i remés al CCN l'Informe de l'estat de la seguretat (Informe INES).

Encara que no s'ha realitzat l'auditoria del compliment de l'ENS, sí que s'han realitzat diferents anàlisis referides a la UNE-EN ISO/IEC 27002.

L'EMT ha elaborat una *Política de seguretat de la informació (PSI)*, aprovada pel director de l'Àrea de Desenvolupament al desembre de 2018. El contingut d'aquesta política s'adequa parcialment als requisits establits per l'ENS. No obstant això:

- La política de seguretat de la informació ha de ser aprovada pel Consell d'Administració, màxim òrgan de direcció de l'EMT, tal com requereixen l'ENS i la norma UNE-EN ISO/IEC 27001, i no compleix tots els requisits establits en les dues normes.

- No s'han constituït òrgans de govern de la seguretat que instrumentalitzen les responsabilitats respecte a la seguretat de la informació, com el comité de seguretat

de la informació, ni s'ha establit una organització interna de la seguretat equivalent que establisca un marc de gestió de la seguretat.

- Ha de respectar-se la segregació de funcions que s'estableix en l'article 10 de l'ENS.
- Hi ha deficiències formals en la designació de les persones per als rols definits en *Política de seguretat de la informació*.

  La *PSI* atribueix les funcions de **responsable de seguretat** a dos càrrecs directius de l'entitat, el responsable de sistemes i la responsable de recursos humans. Aquests càrrecs no han sigut adequadament referenciats en el document, atés que no existeixen com a tals en l'organigrama de l'organització.

  L'assignació de funcions i responsabilitats que assumeix cada un dels càrrecs que conformen el rol no es troba detallada i diferenciada en el document i no s'ha produït una acceptació formal per part de les persones sobre les quals recau la responsabilitat.

  En aquesta matèria haurien de seguir-se els criteris establits en *Guia de seguretat de les TIC CCN-STIC 801 ENS Responsabilitats i funcions*.

Aquestes mancances limiten el reconeixement per part de l'organització de les funcions del responsable de seguretat i minven la seua capacitat operativa, la qual cosa representa un factor de risc important, particularment en un entorn de sistemes descentralitzats en el qual el responsable ha de vetlar per l'aplicació homogènia de mesures de seguretat en la totalitat dels sistemes de l'entitat.

En matèria de protecció de dades personals

L'1 de juny de 2018 es va nomenar la delegada 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 que inclou el detall necessari.

S'ha realitzat una anàlisi de riscos sobre els seus tractaments de dades personals i les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.

Actualment l'entitat es troba immersa en un projecte d'adequació a aquesta normativa. En el marc d'execució del projecte es disposa d'un pla d'acció que recull el seguiment de les activitats desenvolupades i per desenvolupar, partint de una anàlisi diferencial i de l'anàlisi de riscos realitzat.

No obstant això:

- No s'ha realitzat cap auditoria específica en matèria de protecció de dades.
- El registre d'activitats del tractament no s'ha publicat ni és accessible per mitjans electrònics.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

DPD: Delegat de protecció de dades

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

SIEM: Sistema de gestió d'informació i esdeveniments de seguretat

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.

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.

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i descriuran: *a*) l'ús correcte d'equips, serveis i instal·lacions, *b*) el que es considerarà ús indegut i *c*) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, estarà disponible en la intranet corporativa de l'entitat a través d'una adreça URL. La normativa de seguretat de cada entitat 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 per la junta de govern d'un ajuntament o el consell d'administració d'una societat. Ha d'estar accessible per a tots els membres de l'organització i redactada de manera senzilla, precisa i comprensible. Convé que siga breu, i que deixe els detalls tècnics per a altres documents més precisos que ajuden a dur a terme el que s'hi proposa: normes de seguretat i procediments de seguretat.

Procediments de seguretat: Aborden tasques concretes, 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.

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, l'esborrany previ de l'Informe de fiscalització es va discutir amb els responsables de l'Empresa Municipal de Transports de València, SAU, per al seu coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*c* del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'Informe de fiscalització corresponent a l'exercici 2020, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

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

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

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

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

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, d'acord amb la redacció que en fa la Llei de la Generalitat Valenciana 16/2017, de 10 de novembre, i de l'article 55.1.*h* del seu Reglament de Règim Interior i del Programa Anual d'Actuació de 2020 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 15 de desembre de 2021, va aprovar aquest informe de fiscalització.

ANNEX I

Al·legacions presentades

ANNEX II

Informe sobre les al·legacions presentades

ANÀLISI DE LES AL·LEGACIONS EFECTUADES PER L'EMPRESA MUNICIPAL DE TRANSPORTS DE VALÈNCIA, SAU, A L'ESBORRANY DE L'INFORME D'AUDITORIA DE CIBERSEGURETAT DE L'EXERCICI 2020

Per mitjà d'un escrit de la Sindicatura de Comptes amb data 3 de desembre de 2020, es va remetre a l'Empresa Municipal de Transports de València, SAU, (EMT) l'esborrany de l'Informe d'auditoria, perquè efectuara les al·legacions que considerara oportunes. Amb data 21 de desembre de 2020 es van rebre pel registre electrònic les al·legacions formulades,[1] respecte de les quals s'assenyala el que segueix:

Primera al·legació

Apartat 4, "Conclusions", de l'esborrany de l'Informe, primer subapartat: "Baix índex de maduresa dels controls de ciberseguretat"

Comentaris

En l'al·legació s'indica que l'EMT ha aconseguit en un curt període de temps un canvi molt significatiu de l'estat de maduresa de la ciberseguretat. L'escrit d'al·legacions conté un apartat "B) RESUM DE FITES EN MATÈRIA DE SEGURETAT I SISTEMES FINS A L'ANY 2020" per a corroborar aquesta afirmació. En síntesi, s'al·lega que durant els últims anys:

- S'han fet treballs d'auditoria per part de consultores externes que mostren, durant els últims dos anys, una notable millora en els nivells de seguretat de totes les àrees analitzades.

- S'han realitzat inversions rellevants en matèria de seguretat, particularment en els últims dos anys.

- S'ha iniciat la implantació d'un SGSI, la documentació suport del qual es troba en estat d'elaboració o revisió.

- S'han implantat millores en els sistemes i solucions tecnològiques de seguretat d'eficàcia comprovada, algunes de les quals durant la mateixa realització del treball i com a part del pla d'actuacions existent.

En la realització de l'auditoria hem pogut comprovar que s'havien efectuat millores en els controls de ciberseguretat respecte de la situació precedent i que hi havia diverses iniciatives en marxa per a continuar en aquesta línia. En les valoracions del nivell de maduresa dels controls hem tingut en compte totes les millores ja implantades i en funcionament en el moment de la nostra revisió, però no estava dins dels objectius del

[1] Les al·legacions rebudes s'adjunten en l'annex 1. Per raons de seguretat s'ha eliminat la referència concreta a algun element de seguretat en el document adjunt, i per aquesta raó apareix algun espai en blanc.

treball realitzar una anàlisi comparativa amb la situació existent fa dos anys, que per la informació aportada en l'al·legació era clarament pitjor.

A més, hem constatat que, en el marc general de millora de la seguretat, gran part de les recomanacions emeses en l'Informe es troben en fase d'implantació o s'estan planificant, bé com a conseqüència d'aquest treball o com a part del pla d'actuacions existent.

En aquest sentit es valora positivament la disposició de la Direcció per a millorar els controls del sistema d'informació i comunicacions de l'EMT i atendre les recomanacions efectuades, el disseny i l'eficàcia operativa dels quals podran ser avaluades en un informe posterior de seguiment a realitzar per la Sindicatura.

Atés que en aquesta i altres al·legacions s'al·ludeix al fet que l'EMT està en un procés de millora del sistema de seguretat i de les deficiències identificades, s'afegeix un paràgraf al final de l'apartat de recomanacions per a recollir, amb caràcter general, aquesta circumstància.

Conseqüències en l'Informe

Afegir, al final de l'apartat 5, "Recomanacions", un paràgraf amb la redacció següent:

"Durant la fase d'al·legacions, la Direcció de l'EMT ha emfatitzat en el procés de millora del sistema de seguretat de la informació emprés per l'entitat durant els dos exercicis anteriors i en la seua intenció d'atendre les recomanacions realitzades. En les valoracions del nivell de maduresa dels controls hem tingut en compte només les millores ja implantades i en funcionament en el moment de la nostra revisió, a més d'haver-hi altres iniciatives en marxa, en fase de planificació o d'implantació, per a atendre bona part de les recomanacions que hem realitzat, el disseny i l'eficàcia operativa de les quals podran ser avaluades en un informe posterior de seguiment."

Segona al·legació

Apartat 4, "Conclusions", de l'esborrany de l'Informe, segon subapartat: "Es requereix major conscienciació i més recursos dedicats a la seguretat de la informació"

Comentaris

L'EMT assenyala que entre el 2015 i el 2020 la inversió en matèria de seguretat i sistemes ha sigut de 2.139.485,14 euros i que el 90% de les partides s'han configurat o licitat des de l'any 2018, la qual cosa ha permés incrementar el nivell de maduresa i seguretat de l'entitat. No obstant això, en l'al·legació s'indica que "es coincideix amb aquesta conclusió".

Encara que s'han augmentat les inversions en la matèria, es partia d'un punt molt baix i encara hi ha molt de recorregut de millora.

Vegeu comentaris en l'al·legació anterior.

Conseqüències en l'Informe

Es manté la redacció de l'Informe.

Tercera al·legació

Apartat 4, "Conclusions", de l'esborrany de l'Informe, tercer subapartat: "Governança insuficient de la seguretat de la informació"

Comentaris

En relació amb el que s'al·lega en el primer paràgraf: "L'ENS no especifica quin òrgan o lloc directiu en concret té la potestat per a aprovar la política de seguretat i el nomenament dels diferents rols o configuració del comité de seguretat", considerem que un document de polítiques de seguretat de la informació (PSI) ha de ser aprovat al màxim nivell jeràrquic. En aquest cas està aprovat per un director d'àrea, la qual cosa no té molta lògica i planteja dubtes raonables sobre la capacitat per a exigir el compliment de la PSI en establir responsabilitats i compromisos per al Comité executiu de l'EMT, que està en una posició jeràrquica superior a la persona que aprova la PSI.

Segons l'article 11 del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS), la PSI ha de ser aprovada pel "titular de l'òrgan superior corresponent" i "es consideraran òrgans superiors els responsables directes de l'execució de l'acció del govern, central, autonòmic o local".

I l'apartat 3.1, "Política de seguretat [org.1]", de l'ENS assenyala:

"La política de seguretat serà aprovada per l'òrgan superior competent que corresponga, d'acord amb el que s'estableix en l'article 11, i es plasmarà en un document escrit, en el qual, de manera clara, es precise, almenys, el següent:

a) Els objectius o missió de l'organització.

b) El marc legal i regulador en què es desenvoluparan les activitats.

c) Els rols o funcions de seguretat, definint per a cada un els deures i responsabilitats del càrrec, així com el procediment per a la seua designació i renovació.

d) **L'estructura del comité o els comités per a la gestió i coordinació de la seguretat**, detallant el seu àmbit de responsabilitat, els membres i la relació amb altres elements de l'organització.

e) Les directrius per a l'estructuració de la documentació de seguretat del sistema, la seua gestió i accés."

D'altra banda, la guia de seguretat de les TIC *CCN-STIC-805 Política de Seguretat de la Informació* estableix que: "23. La Política de Seguretat de la Informació és un document que

serà aprovat formalment per l'alta direcció de l'organització i tindrà caràcter imperatiu sobre tota l'organització".

Al seu torn, la guia de seguretat de les TIC *CCN-STIC-801 Responsabilitats i funcions en l'ENS* coincideix en el mateix criteri i assenyala: "25. Així doncs, la figura de la Direcció de l'entitat (personificada en el seu titular) cobra una importància cabdal: de la Direcció depén el compromís de l'entitat amb la seguretat i la seua adequada implantació, gestió i manteniment".

A més, l'òrgan que aprove la PSI ha de ser aquell entre les competències del qual es trobe la determinació i assignació pressupostària de l'organisme, circumstància lògica, a la vista que el compliment de l'ENS suposa, en la majoria dels casos, la deguda assignació de recursos que requereix la seua implantació.

Des del punt de vista de les normes ISO 27001/27002, atés el contingut que ha de tindre una PSI/SGSI, només el màxim òrgan de l'EMT té atribucions per a això (vegeu apartat 2 de l'Informe). La UNE-EN ISO/IEC 27001 estableix en el seu apartat 5, "Lideratge", que "l'alta direcció ha d'establir una política de seguretat de la informació". En aquest mateix sentit es manifesta la UNE-EN ISO/IEC 27002: "Les organitzacions haurien de definir una política de seguretat de la informació al màxim nivell que siga aprovada per la direcció i establisca l'enfocament de l'organització per a gestionar els seus objectius de seguretat de la informació".

Finalment, és important destacar que la conclusió objecte de l'al·legació, encara que té un component de compliment de la normativa en matèria de seguretat de la informació, es refereix fonamentalment al compliment dels controls en matèria de ciberseguretat, que és una àrea crítica del sistema de control intern de l'EMT. Per tant, hem de comparar la situació en aquest punt concret no sols amb el que es preveu en la normativa aplicable, sinó en les millors pràctiques en matèria de control intern. Des dels dos punts de vista considerem que l'"òrgan superior corresponent" o l'"alta direcció" és el Consell d'Administració, si bé podria ser discutible que fora el president o el director gerent, però no considerem raonable que siga un lloc directiu de rang jeràrquic inferior als anteriors.

En relació amb els comentaris de l'al·legació referents a la figura del responsable de seguretat, s'accepta parcialment l'al·legació i es reconsidera i matisa la redacció de l'Informe.

Finalment, respecte de l'últim paràgraf de l'al·legació, només cal assenyalar que un "comité de crisi" no es correspon amb la figura d'un comité de gestió de la seguretat de la informació que s'esmenta en l'Informe.

Conseqüències en l'Informe

Es matisa la redacció, de manera que la conclusió (apartat 4 de l'Informe) al·legada queda així:

"**Governança insuficient de la seguretat de la informació**

L'EMT disposa d'una *Política de seguretat de la informació* (PSI), que **no ha sigut aprovada pel Consell d'Administració**, màxim òrgan de direcció de l'EMT, tal com requereixen l'ENS i la norma UNE-EN ISO/IEC 27001/27002, ni compleix tots els requisits establits en les dues normes.

La gestió de la seguretat dels sistemes d'informació requereix establir una organització de la seguretat, que ha de determinar amb precisió els diferents actors que la conformen, les seues funcions i responsabilitats, així com la implantació d'una estructura que les suporte i els mecanismes de coordinació i resolució de conflictes, a més de designar un **comité de gestió de la seguretat de la informació**, de manera que la governança de la seguretat de la informació estiga adequadament estructurada.

La PSI que aprove el Consell d'Administració ha de recollir amb claredat les responsabilitats sobre la gestió, administració i seguretat dels sistemes descentralitzats (els gestionats de manera autònoma pels departaments), ja que la PSI actual no reflecteix fidelment les particularitats del model organitzatiu de l'entitat. L'administració de sistemes d'informació, que de manera general realitza l'Àrea de Desenvolupament, és assumida en determinats casos pels mateixos departaments de l'entitat, que administren les aplicacions específiques que suporten els processos crítics dels seus departaments. Aquesta situació no resulta recomanable, ja que dificulta la capacitat operativa del responsable de seguretat com a figura que ha de vetlar per l'aplicació homogènia de mesures de seguretat en el conjunt dels sistemes de l'entitat i la seua coherència en un entorn de sistemes administrats per diferents departaments. A més, existeix un risc elevat que els departaments no tinguen les competències professionals requerides per a l'administració de sistemes i que els interessos departamentals no es troben alineats amb els principis de la seguretat de la informació aprovats per l'organització."

Quarta al·legació

Apartat 4, "Conclusions", de l'esborrany de l'Informe, quart subapartat: "La situació dels controls d'accés privilegiat s'ha de millorar"

Comentaris

L'EMT especifica que les principals debilitats trobades estan en els sistemes descentralitzats gestionats per proveïdors externs i que s'esmenaran en el curt termini. De la mateixa manera, s'indica que existeix una proposta de treball i pressupost per a executar-la. S'adjunta la proposta en les al·legacions rebudes.

Hem verificat l'existència de la proposta i pla de treball, que inclou les modificacions necessàries quant a la gestió adequada de drets d'accés i privilegis administratius dels usuaris i l'aplicació adequada del principi de mínim privilegi.

Vegeu també comentaris a la primera al·legació.

Conseqüències en l'Informe

Afegir un tercer paràgraf en el subapartat "La situació dels controls d'accés privilegiats s'ha de millorar", de l'apartat 4, "Conclusions", amb la redacció següent:

"Durant el tràmit d'al·legacions, l'EMT ens ha informat de l'existència d'una proposta de treball per a la resolució d'aquestes deficiències. Hem verificat l'existència d'aquesta proposta i del pla de treball, que inclou les modificacions necessàries quant a la gestió adequada de drets d'accés i privilegis administratius dels usuaris, registres d'activitat i aplicació adequada del principi de mínim privilegi. Quan s'emet aquest informe, aquestes accions estaven en fase d'implantació."

El paràgraf 6, en l'apartat 6 ("Sobre el control d'accés a dades i programes") de l'apèndix 2, queda redactat així:

"La gestió de drets d'accés no aconsegueix els nivells de control adequats, particularment per a l'aplicació comptable. Hem evidenciat que en aquest sistema no s'ha aplicat adequadament el criteri de mínim privilegi en l'exercici de provisió de drets d'accés als usuaris, i aquesta és una deficiència de control que considerem significativa. Hem evidenciat que es troba en curs una modificació dels perfils de determinats usuaris per a adequar els seus privilegis als requeriments dels seus llocs de treball. Durant la fase d'al·legacions, se'ns ha informat de l'existència d'una proposta i pla de treball per a fer extensiva aquesta modificació a tots els usuaris del sistema. Hem verificat la documentació que suporta l'existència d'aquest pla de treball i que aquesta iniciativa es troba en fase d'implantació en el moment d'emetre aquest informe."

Cinquena al·legació

Apartat 4, "Conclusions", de l'esborrany de l'Informe, cinqué subapartat: "Grau insuficient d'adequació a la normativa de ciberseguretat"

Comentaris

L'EMT assenyala, en síntesi, que durant els anys 2019 i 2020 s'han completat fites legalment requerides en el marc d'adequació a l'RGPD i que, atés que en aquest treball no s'han analitzat tots els aspectes de l'RGDP, no es pot concloure que no hi ha una adequació suficient.

La valoració respecte a l'adequació a la normativa de ciberseguretat inclosa en l'apartat de conclusions no fa referència expressa a les mancances concretes identificades, sinó a la responsabilitat d'impulsar mesures equivalents a l'Esquema Nacional de Seguretat, incloent-hi els tractaments de dades personals.

La valoració del compliment normatiu, detallat en l'apèndix 2, apartat 14, s'ha realitzat de manera diferenciada per a l'adequació a l'ENS i a la normativa de protecció de dades. En aquest apartat s'especifiquen mancances rellevants relatives a l'adequació a l'ENS que són les que han tingut efecte negatiu en quantificar l'índex de maduresa del CBCS 8.

Conseqüències en l'Informe

Es matisa la redacció de l'apartat 4, "Conclusions", cinqué subapartat, que queda així:

"La revisió del compliment de legalitat en matèria relacionada amb la ciberseguretat ha posat de manifest un nivell insatisfactori d'adequació a la normativa de ciberseguretat. L'Ajuntament de València i el Consell d'Administració de l'EMT tenen la responsabilitat d'impulsar un grau d'implementació de mesures equivalents a l'Esquema Nacional de Seguretat, en el marc del compliment de la normativa en matèria de protecció de dades, i han de promoure les accions necessàries per a esmenar aquesta situació."

Sisena al·legació

Apartat 5, recomanació núm. 1 de l'esborrany de l'Informe

Comentaris

Confirma el que s'assenyala en l'Informe.

Conseqüències en l'Informe

No es modifica.

Setena al·legació

Apartat 5, 2a recomanació de l'esborrany de l'Informe

Comentaris

Confirma el que s'assenyala en l'Informe.

Conseqüències en l'Informe

No es modifica.

Huitena al·legació

Apartat 5, 3a recomanació de l'esborrany de l'Informe

Comentaris

Confirma el que s'assenyala en l'Informe.

Conseqüències en l'Informe

No es modifica.

Novena al·legació

Apartat 5, recomanacions 4, 5 i 7 de l'esborrany de l'Informe

Comentaris

L'al·legació és anàloga a la quarta al·legació i les conseqüències en l'Informe proposades en aquella són vàlides per a aquesta.

Conseqüències en l'Informe

No es modifiquen les recomanacions.

Desena al·legació

Apartat 5, recomanació núm. 10 de l'esborrany de l'Informe

Comentaris

L'EMT ressalta la posada en marxa del nou sistema de suport durant 2020. En el treball realitzat hem verificat i valorat la qualitat tècnica de la solució implantada, que efectivament disposa de les característiques adequades per a satisfer les necessitats de l'organització.

No obstant això, s'han evidenciat determinades mancances des del punt de vista de la gestió i mesurament dels nivells de servei que limiten la maduresa del control que han de ser esmenades.

Conseqüències en l'Informe

No es modifica.

Onzena al·legació

Apartat 5, recomanació núm. 11 de l'esborrany de l'Informe

Comentaris

Confirma el que s'assenyala en l'Informe.

Conseqüències en l'Informe

No es modifica.

Dotzena al·legació

Apartat 5, recomanació núm. 12 de l'esborrany de l'Informe

Comentaris

Confirma el que s'assenyala en l'Informe.

Conseqüències en l'Informe

No es modifica.

Tretzena al·legació

Apartat 5, recomanació núm. 13 de l'esborrany de l'Informe

Comentaris

L'EMT assenyala la inclusió en els plecs del detall necessari per a dur a terme una adequada gestió dels serveis. Si bé hem verificat la inclusió d'aquests continguts en alguns casos, també hem observat que en altres plecs no estan correctament incorporats. De la mateixa manera, les accions empreses per al mesurament del compliment de les obligacions i nivells de servei no formen part d'un procés rutinari ni s'han establit formalment indicadors.

Es constata per conseqüent que, si bé el control pot ser aplicat de manera eficaç, no es troba assegurada la seua aplicació en tots els casos, cosa que limita el nivell de maduresa.

Conseqüències en l'Informe

No es modifica.

Catorzena al·legació

Apartat 5, recomanacions núm. 15 i 16 de l'esborrany de l'Informe

Comentaris

Ens remetem a l'al·legació núm. 5.

Conseqüències en l'Informe

No es modifica.

Al·legaciones sisena a catorzena

Com s'ha assenyalat en la primera al·legació, en l'escrit d'al·legacions s'al·ludeix al fet que l'EMT està en un procés de millora del sistema de seguretat i de les deficiències identificades, per això s'afegeix un paràgraf al final de l'apartat de recomanacions per a recollir, amb caràcter general, aquesta circumstància.