INFORME 9/2024

AJUNTAMENT DE MATARÓ
CONTROLS BÀSICS DE CIBERSEGURETAT, EXERCICI 2023

SINDICATURA DE COMPTES DE CATALUNYA

INFORME 9/2024

AJUNTAMENT DE MATARÓ
CONTROLS BÀSICS DE CIBERSEGURETAT, EXERCICI 2023

SINDICATURA DE COMPTES DE CATALUNYA

Edició: juliol de 2024

Document electrònic etiquetat per a persones amb discapacitat visual

Pàgines en blanc inserides per facilitar la impressió a doble cara

Autor i editor:

Sindicatura de Comptes de Catalunya
Via Laietana, 60
08003 Barcelona
Tel. +34 93 270 11 61
sindicatura@sindicatura.cat
www.sindicatura.cat

Publicació subjecta a dipòsit legal d'acord amb el que preveu el Reial decret 635/2015, del 10 de juliol

ÍNDEX

ABREVIACIONS

CBCS	Controls bàsics de ciberseguretat
ENS	Esquema Nacional de Seguretat
GPF-OCEX	Guia pràctica de fiscalització dels òrgans de control extern

1. INTRODUCCIÓ

1.1. INFORME

La Sindicatura de Comptes, com a òrgan fiscalitzador del sector públic de Catalunya, d'acord amb la normativa vigent i en compliment del seu Programa anual d'activitats, ha emès aquest informe de seguretat limitada relatiu als controls bàsics de ciberseguretat de l'Ajuntament de Mataró (exclosos els ens dependents) en l'exercici 2023.

Aquesta auditoria de sistemes de la informació, de caràcter limitat, s'ha centrat en la revisió dels 8 controls bàsics de ciberseguretat (CBCS) que estableix la Guia pràctica de fiscalització (GPF-OCEX) 5313, Revisió dels controls bàsics de ciberseguretat, aprovada per la Conferència de Presidents dels Òrgans de Control Extern el 12 de novembre del 2018.

Els controls bàsics de ciberseguretat que inclou aquesta guia es relacionen en el quadre següent:

Quadre 1. Controls bàsics de ciberseguretat

Control	
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 correcció de vulnerabilitats
CBCS 4	Ús controlat de privilegis administratius
CBCS 5	Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors
CBCS 6	Registre de l'activitat dels usuaris
CBCS 7	Còpies de seguretat de dades i sistemes
CBCS 8	Compliment de legalitat

Font: Elaboració pròpia.

L'objectiu general de la fiscalització és proporcionar una avaluació sobre el disseny[1] i l'eficàcia operativa[2] d'aquests 8 controls mitjançant la identificació de deficiències de control intern que puguin afectar negativament la integritat, la disponibilitat, l'autenticitat, la confidencialitat i traçabilitat de les dades, la informació i actius de l'entitat, i la identificació d'incompliments normatius relacionats amb la ciberseguretat.

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

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

Atesa la naturalesa de l'objecte material a revisar, ha estat necessari delimitar i concretar quins sistemes s'havien d'analitzar. S'han revisat les aplicacions que sustenten els processos de gestió comptable i pressupostària i la gestió tributària i recaptatòria com també uns tipus d'elements que formen part de la infraestructura de tecnologia d'informació general i que donen servei a tots els processos de gestió de l'entitat, els quals són fonamentals per al bon funcionament dels sistemes d'informació i la ciberseguretat:

- Controlador de domini
- Programari de virtualització
- Equips d'usuari (una mostra)
- Elements de la xarxa de comunicacions
- Elements de seguretat

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació a 31 desembre del 2023, data sobre la qual s'han calculat els índexs de maduresa que figuren en l'informe.

A més de valorar l'índex de maduresa d'aquests 8 controls, s'ha ampliat el treball efectuat amb la valoració de la governança que exerceixen els òrgans de govern i de les accions dutes a terme per l'Ajuntament per complir el Reial decret 311/2022, del 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS).

Aquest treball s'emmarca dins l'eix estratègic 1, de millora del procés de fiscalització i l'impacte dels informes en els serveis públics, inclòs en el Pla estratègic de la Sindicatura 2022-2028, pel qual s'incorporen auditories de sistemes de la informació en el programa anual. Per dur a terme aquesta auditoria s'ha contractat serveis a una empresa especialitzada en seguretat informàtica i el personal de la Sindicatura ha dirigit i supervisat el treball.[3]

En l'apartat 3, Conclusions, s'inclouen les conclusions a què s'ha arribat a partir del treball realitzat, i en el 4, Recomanacions, hi ha les recomanacions sobre millores en la gestió de les activitats desenvolupades en alguns dels aspectes que s'han posat de manifest durant la realització del treball.

Atès el caràcter limitat de la revisió, el seu objectiu no és emetre una opinió de seguretat raonable sobre la confiança que mereix el sistema auditat en relació amb el nivell de ciberseguretat implantat. No obstant això, l'auditoria proporcionarà informació rellevant sobre el grau de ciberseguretat i ciberresiliència de l'entitat i sobre possibles accions de millora aconsellables.

3. D'acord amb el que preveu l'apartat 10 de la GPF-OCEX 5311, fins que a les plantilles dels òrgans de control extern no s'incorporin auditors de sistemes d'informació i experts en ciberseguretat, es disposa del recurs de contractar experts externs i professionals especialitzats per cobrir aquest dèficit de coneixements.

1.2. ENS FISCALITZAT

1.2.1. Activitats i organització

El municipi de Mataró és un ens local les competències i funcions del qual es regeixen pel Decret legislatiu 2/2003, del 28 d'abril, pel qual s'aprova el text refós de la Llei municipal i de règim local de Catalunya, i per la Llei de l'Estat 7/1985, del 2 d'abril, reguladora de les bases del règim local, i per totes les altres disposicions específiques i complementàries.

L'Ajuntament disposa d'un reglament orgànic municipal propi que regula el règim organitzatiu i de funcionament dels seus òrgans.

a) Òrgans de govern i ens dependents de l'Ajuntament

Els òrgans de govern de l'Ajuntament de Mataró són el Ple, l'alcalde, els tinents d'alcalde, la Junta de Govern Local i els regidors de regidories delegades.

Com a òrgans complementaris, en l'exercici fiscalitzat, disposava dels següents: les comissions informatives, la Comissió Especial de Comptes, la Comissió Especial d'Organització, els grups municipals, els portaveus i la Junta de Portaveus.

Pel que fa als ens dependents, en l'exercici 2023 l'Ajuntament tenia constituïdes 2 entitats públiques empresarials locals, 2 societats mercantils i 3 fundacions; a més, tenia adscrits 3 consorcis.

Aquests ens eren els següents:

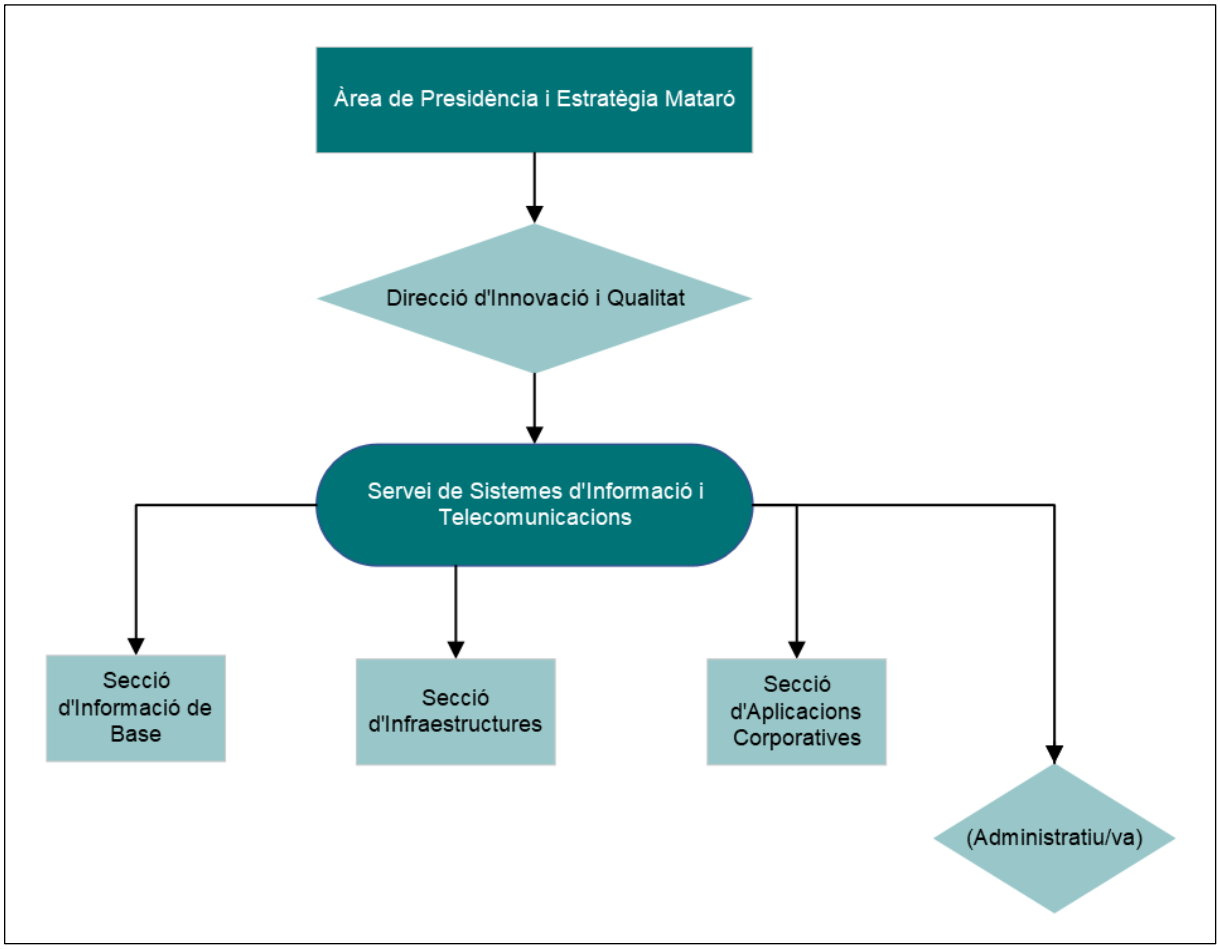
- Mataró Audiovisual[4]
- Parc Tecnocampus Mataró[4]
- Aigües de Mataró, SA
- Promocions Urbanístiques de Mataró, SA
- Fundació Privada Hospital Sant Jaume i Santa Magdalena de Mataró
- Fundació Tecnocampus Mataró-Maresme
- Fundació Unió de Cooperadors de Mataró pel Foment de l'Economia Social i la Rehabilitació Urbana
- Consorci per al Tractament de Residus Sòlids Urbans del Maresme
- Consorci Transversal Xarxa d'Activitats Culturals (CTXAC)
- Consorci Museu d'Art Contemporani de Mataró

4. Entitat pública empresarial local.

b) Organització de la unitat de Servei de Sistemes d'Informació i Telecomunicacions

Des de la unitat de Servei de Sistemes d'Informació i Telecomunicacions es defineix, planifica i executa l'estratègia tecnològica. Aquesta unitat organitzativa depèn de la Direcció d'Innovació i Qualitat, adscrita a l'Àrea de Presidència i Estratègia Mataró. La dependència i l'organització bàsica de la unitat es mostra en el gràfic següent:

Gràfic 1. Organigrama funcional de la unitat de Servei de Sistemes d'Informació i Telecomunicacions



Font: Elaboració pròpia.

Els principals objectius estratègics de la unitat de Servei de Sistemes d'Informació i Telecomunicacions són:

- Desenvolupar i mantenir eines tecnològiques que donin suport a l'execució i la gestió dels processos de la institució implementant metodologies i millors pràctiques de l'enginyeria de programari.

- Garantir l'existència d'una informació cartogràfica i alfanumèrica veraç, fiable, contrastada i actualitzada del terme municipal per a la gestió i planificació d'aquest territori i la seva població.

- Implementar i gestionar una plataforma tecnològica que sigui fiable, íntegra i altament disponible, que admeti els processos de l'Ajuntament, millorant així l'acompliment dels funcionaris en les seves respectives activitats.

- Gestionar els sistemes d'informació i comunicació moderns i amb el grau d'eficiència adient per donar resposta als objectius estratègics.

En l'exercici 2023 el nombre de places assignades a aquesta unitat era de 16, ocupades amb 14 funcionaris de carrera, 1 funcionari interí i 1 persona contractada mitjançant un pla d'ocupació.

2. METODOLOGIA

Els resultats del treball s'han avaluat d'acord amb el que preveu l'apartat 7 de la GPF-OCEX-5313 tenint en compte l'anàlisi i avaluació dels CBCS a 2 nivells.

Per cada control global la guia defineix una sèrie de subcontrols, de cada un dels quals s'ha extret una valoració en funció de les proves d'auditoria i evidències obtingudes sobre la seva eficàcia, i que s'han qualificat de la manera següent:

Quadre 2. Valoració de cada subcontrol

Nivell	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 verificar implementació i eficàcia operativa ha estat satisfactori.
Control força efectiu	• En línies generals, compleix amb l'objectiu de control, si bé pot haver-hi certs aspectes no coberts al 100% i: - Se segueix un procediment, malgrat que pot no estar formalitzat o presentar aspectes de millora (detall, nivell d'actualització, etc.). - Les proves realitzades per verificar la implementació són satisfactòries. - S'han detectat incompliments en les proves realitzades per verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	• Cobreix de manera molt limitada l'objectiu de control i: - Se segueix un procediment, malgrat que pot no estar formalitzat. - El resultat de les proves d'implementació i eficàcia operativa és satisfactori. • Cobreix en línies generals l'objectiu de control, però: - No se segueix un procediment clar. - Les proves realitzades per verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius malgrat que no són generalitzats).

Nivell	Descripció
Control no efectiu o no implementat	• 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).

Font: GPF-OCEX- 5330.

Un cop revisats els resultats obtinguts en els subcontrols de cada CBCS i tenint en compte la seva importància relativa per al compliment de l'objectiu del control, s'han avaluat els 8 controls aplicant el model de nivell de maduresa dels processos ponderat en una escala de zero a 100. En el quadre següent es detallen els nivells de maduresa dels processos.

Quadre 3. Nivells de maduresa

Nivell	Índex	Descripció
0 – Inexistent	0	Aquesta mesura no està essent aplicada en aquest moment.
1 – 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 el fracàs del procés depèn de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depèn de si es té personal d'alta qualitat.
2 – Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan diferents persones realitzen determinats procediments, però no hi ha procediments escrits ni activitats formatives. L'eficàcia del procés depèn de la bona sort i de la bona voluntat de les persones. Hi ha un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. El resultat és imprevisible si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.
3 – 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 processos garanteixen la coherència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establerta i procediments per garantir una reacció professional davant dels incidents. Es fa un manteniment regular. Les possibilitats d'èxit són elevades, malgrat que sempre queda el factor d'allò desconegut (o no planificat). L'èxit és més que bona sort: s'ha de treballar. Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2, i que es gestiona en el nivell 3.

Nivell	Índex	Descripció
4 – Gestionat i mesurable	90	La Direcció controla i mesura el seguiment dels procediments i adopta mesures correctores quan convé. Es disposa d'un sistema de mesures i mètriques per conèixer el seguiment (eficàcia i eficiència) dels processos. La Direcció és capaç d'establir objectius qualitatius a assolir i disposa de mitjans per valorar si s'han assolit 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 és només qualitativa.
5 – 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 reflectir els canvis en els objectius de negoci, utilitzant-los com a indicadors en la gestió de la millora dels processos. En aquest nivell l'organització és capaç de millorar el funcionament dels sistemes a base d'una millora contínua dels processos a partir dels resultats de les mesures i els indicadors.

Font: GPF-OCEX-5313.

Per determinar el nivell de maduresa mínim requerit s'ha de tenir present que 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 afectés la seguretat de la informació o dels sistemes, amb repercussió en la capacitat organitzativa per:

- Aconseguir els seus objectius
- Protegir els actius a càrrec seu
- Complir amb les seves obligacions diàries de servei
- Respectar la legalitat vigent
- Respectar els drets de les persones

A fi de poder determinar l'impacte que un incident d'aquest tipus tindria sobre l'organització, i poder establir la categoria del sistema, s'han de tenir en compte les 5 dimensions de seguretat que els controls de ciberseguretat han de garantir: la confidencialitat, la integritat, la disponibilitat, l'autenticitat i la traçabilitat.

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

Els nivells mínims d'exigència o de maduresa requerits per l'ENS en funció de la categoria de cada sistema són:

Quadre 4. Nivell de maduresa exigit a les categories de sistemes

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%)

Font: Guia de seguretat de les TIC. CCN-STIC-824. Informe nacional de l'estat de seguretat de sistemes TIC.

Els sistemes auditats en aquesta fiscalització, tenint en compte els serveis i la informació que gestionen i d'acord amb el criteri de l'ENS, s'haurien de considerar com una categoria de seguretat mitjana.

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

Governança de la ciberseguretat

A l'efecte d'aquest treball, s'entendrà per governança de la seguretat de la informació i les comunicacions el conjunt de responsabilitats i activitats realitzades pels òrgans de govern amb l'objectiu de proporcionar una direcció estratègica en aquesta matèria, garantint que s'aconsegueixin els objectius, verificant que el risc es gestioni adequadament i comprovant que els recursos s'utilitzen de manera responsable.

Els principals elements d'una bona governança de la ciberseguretat s'inclouen, de manera implícita, en l'ENS i en la normativa relativa a la protecció de dades de caràcter personal, i ambdues normes es revisen en el CBCS 8.

Tot i això, atesa la importància que té per a la ciberresiliència, es destaca de manera explícita l'avaluació que la Sindicatura fa de la governança existent basant-se en la implicació dels òrgans superiors i analitzada a partir dels aspectes següents:

- L'existència de polítiques de seguretat de la informació aprovades pel titular de l'òrgan superior i la seva revisió periòdica.
- La disposició de normativa i procediments de seguretat degudament aprovats i comunicats a les parts interessades.
- L'assignació de rols i de responsables en matèria de seguretat. El responsable de la informació i el del servei poden ser la mateixa persona, però aquest ha de ser diferent del responsable de la seguretat i del sistema.
- L'existència d'un comitè de seguretat de la informació.
- Recursos humans i materials destinats a millorar els controls de la ciberseguretat.

3. CONCLUSIONS

La Sindicatura de Comptes de Catalunya, en virtut del que disposa la seva llei de creació, d'acord amb el que preveu el Programa anual d'activitats, de conformitat amb els principis fonamentals de fiscalització dels òrgans de control extern i les normes internacionals d'auditoria adaptades al sector públic, ha fiscalitzat amb una seguretat limitada els controls bàsics de ciberseguretat de l'Ajuntament de Mataró amb l'abast i la metodologia descrits en l'apartat 1.1 i l'apartat 2 d'aquest informe, respectivament.

En els apartats següents s'inclouen les conclusions més significatives que s'han posat de manifest amb motiu del treball de seguretat limitada realitzat, en els aspectes de la ciberseguretat.

1) Índex de maduresa general

La guia CCN-STIC-824[5] presenta una sèrie d'indicadors de maduresa i de compliment que permeten aportar informació resumida sobre l'estat de la seguretat en els organismes públics. Aquests indicadors s'han adaptat per poder-los aplicar als treballs de revisió dels 8 CBCS per permetre avaluar l'estat de les mesures de seguretat de l'ens auditat.

Els indicadors són els següents:

- Índex de maduresa, que sintetitza, en tant per cent, el nivell de maduresa assolit per l'entitat respecte del conjunt de controls de ciberseguretat.

- Índex de compliment, que també avalua el nivell de maduresa obtingut, però en relació amb l'exigència aplicable en cada cas segons la categoria del sistema. És a dir, compara l'índex de maduresa assolit amb el nivell mínim que s'exigeix per a aquesta categoria en l'ENS. Per a aquesta fiscalització el nivell mínim exigit és l'N3 – Procés definit, amb un percentatge del 80%.

La fiscalització realitzada i els indicadors reflecteixen la situació a 31 de desembre del 2023. El grau de control en la gestió dels CBCS arriba a un índex de maduresa general del 53,11%, que correspon a un nivell N2 – Repetible, però intuïtiu. És a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

Els resultats de les conclusions sobre el nivell de maduresa es fonamenten en els processos teòrics, en els procediments aprovats i també en la verificació de la seva aplicació pràctica, considerant els subcontrols que configuren cada CBCS. Els resultats es mostren detalladament en el quadre següent:

5. Guia de seguretat de les TIC. CCN-STIC-824. Informe nacional de l'estat de seguretat de sistemes TIC.

Quadre 5. Índex de maduresa, nivell de maduresa i índex de compliment

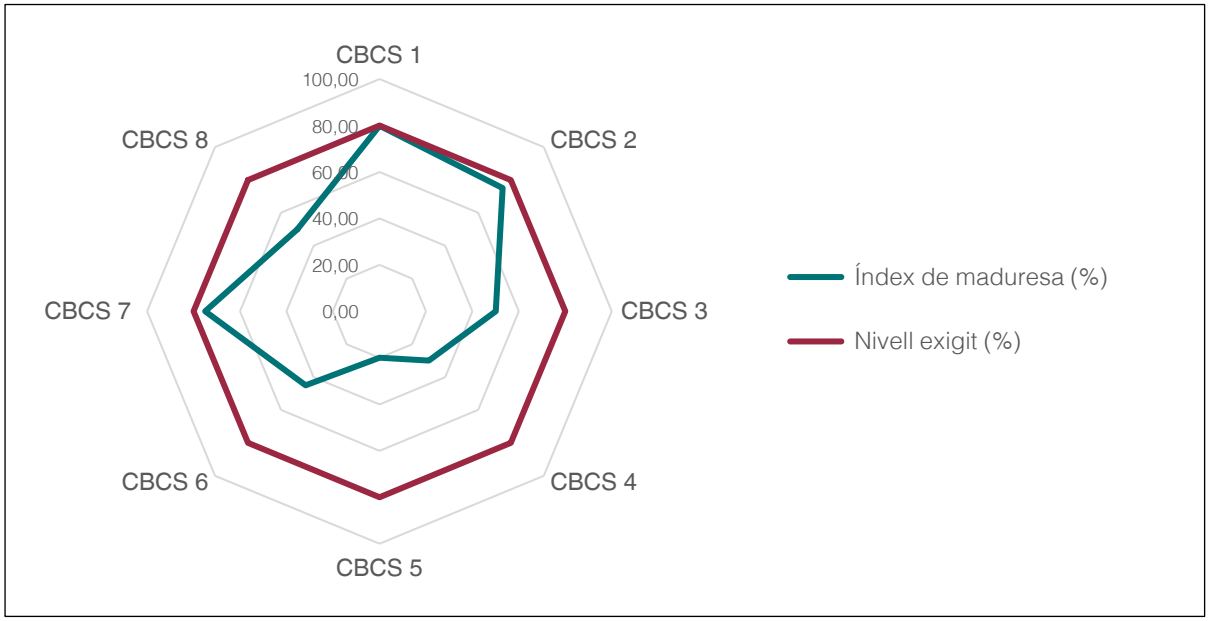
Control		Índex de maduresa (%)	Nivell de maduresa	Índex de compliment (%)
CBCS 1	Inventari i control de dispositius físics	79,90	N2	99,88
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	75,00	N2	93,75
CBCS 3	Procés continu d'identificació i correcció de vulnerabilitats	50,00	N2	62,50
CBCS 4	Ús controlat de privilegis administratius	30,00	N1	37,50
CBCS 5	Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors	20,00	N1	25,00
CBCS 6	Registre de l'activitat dels usuaris	45,00	N2	56,25
CBCS 7	Còpies de seguretat de dades i sistemes	75,00	N2	93,75
CBCS 8	Compliment de legalitat	50,00	N2	62,50
Índex general		**53,11**	**N2**	**66,39**

Font: Elaboració pròpia.

L'índex de compliment general dels CBCS és del 66,39%, que és el resultat de comparar l'índex de maduresa assolit amb el nivell requerit del sistema d'acord amb l'ENS, que, tal com s'ha dit, per a aquesta fiscalització és el nivell N3.

En el gràfic següent es presenta l'índex de maduresa de cada CBCS respecte de l'objectiu previst segons el que l'ENS requereix:

Gràfic 2. Índex de maduresa i objectius dels CBCS



Font: Elaboració pròpia.

Com es pot observar, cap dels controls arriba a un índex de maduresa del 80%, però n'hi ha 3 amb índexs molts propers. El millor resultat correspon al CBCS 1, Inventari i control de dispositius físics, que assoleix un índex de maduresa del 79,90% i un de compliment del 99,88%. La pitjor situació és la del CBCS 5, Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors, amb un índex de maduresa del 20% i un de compliment del 25%.

En el cas del CBCS 4, Ús controlat de privilegis administratius, i el CBCS 5, Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors, el nivell de maduresa aconseguit és el nivell N1, que significa que el procés existeix però no es gestiona.

El nivell assolit dels controls revisats mostra una efectivitat insuficient. Cal tenir en compte que l'Ajuntament hauria de tenir una categoria del sistema de nivell mitjà, que correspon a un nivell de maduresa N3 – Procés definit (vegeu l'apartat 5.1).

2) Governança de la ciberseguretat

Els òrgans superiors de l'Ajuntament són els principals responsables de l'existència dels controls adequats sobre els sistemes d'informació i les comunicacions, i la seva implicació, compromís i lideratge constitueixen, probablement, el factor més important per a la implantació eficaç d'un sistema de gestió de la seguretat de la informació que garanteixi la ciberresiliència de l'entitat.

S'ha pogut verificar l'existència d'aquesta implicació i compromís amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament i dels gestors i responsables de les àrees revisades. No obstant això, s'han identificat mancances que dificulten la implementació d'un sistema completament efectiu que garanteixi la ciberresiliència. Les mancances més significatives són les següents (vegeu l'apartat 5.2.):

- La política de seguretat de la informació no està completa ni actualitzada.
- No s'han formalitzat ni aprovat totes les normes i els procediments de seguretat necessaris.
- Hi ha dependència jeràrquica entre el responsable de seguretat i el responsable del sistema.
- L'any 2017 es va crear el Comitè de Seguretat en Protecció de Dades, perquè fes les funcions del Comitè de Seguretat de la Informació, però no s'ha reunit mai.

3) Compliment normatiu

La revisió del compliment de legalitat en matèria relacionada amb la ciberseguretat ha posat de manifest un nivell de compliment insatisfactori. Els màxims òrgans de direcció de l'Ajun-

tament tenen la responsabilitat de garantir un nivell adequat de compliment de les normes legals i han d'impulsar les mesures necessàries per esmenar la situació (vegeu l'apartat 5.1.8).

4) Aplicació del Reial decret 311/2022

L'Ajuntament està treballant en l'adaptació a l'Esquema Nacional de Seguretat promovent una sèrie d'accions i impulsant l'aprovació de la normativa que li faltava. A la finalització de la redacció d'aquest informe (juny del 2024) l'Ajuntament no havia acreditat l'adequació a l'ENS.

Pel que fa als 4 controls addicionals revisats sobre la gestió dels usuaris i els drets d'accés als sistemes, requerits per complir amb el que preveu el Reial decret 311/2022, s'han observat uns índexs de maduresa superiors al CBCS 4, ús controlat de privilegis administratius, amb índexs de compliment per sobre del 70%, tot i que no assoleixen el nivell mínim de seguretat exigit per la falta de procediments documentats de les pràctiques que habitualment es duen a terme (vegeu l'apartat 5.3).

4. RECOMANACIONS

A continuació s'inclouen les recomanacions sobre alguns aspectes que s'han posat de manifest durant el treball de fiscalització de seguretat limitada d'acord amb l'objecte i abast de l'informe descrits en la introducció, que ajudarien l'Ajuntament a millorar els nivells de maduresa dels controls indicats en l'apartat anterior. També s'assenyalen les mesures per al compliment de la legalitat que han d'adoptar-se.

1. Els òrgans de govern haurien de promoure la revisió i actualització de la normativa de seguretat existent i incentivar actuacions que fomentin la cultura en matèria de ciberseguretat amb una direcció estratègica i coordinada.

2. Caldria formalitzar en manuals i protocols tots els procediments que de manera informal i periòdica està duent a terme el personal de l'Ajuntament.

3. Atès que l'Ajuntament disposa de 2 inventaris per al control dels dispositius físics, un amb la informació dels equips servidors i dels dispositius de xarxa i l'altre amb la dels equips d'usuaris, es recomana unificar-los en una única eina per facilitar-ne el control i la gestió.

4. La unitat responsable de sistemes de la informació hauria d'elaborar un pla de manteniment del programari i identificar i actualitzar tots els sistemes operatius que estan fora del període de suport.

5. Caldria elaborar un llistat de programari autoritzat i dur a terme revisions periòdiques i amb una freqüència mínima en els dispositius per detectar el programari no autoritzat.

6. Elaborar i aprovar un procediment unificat de gestió d'usuaris amb privilegis d'administració que defineixi les directrius per a tots els sistemes de l'entitat.

7. S'haurien de fer revisions periòdiques dels registres d'activitat i centralitzar els registres de tots els sistemes en una sola eina.

5. RESULTATS DE LA FISCALITZACIÓ

En la GPF-OCEX 5311, Ciberseguretat, seguretat de la informació i auditoria externa, es destaca la importància creixent que les qüestions relacionades amb la ciberseguretat estan adquirint en la gestió de les administracions públiques.

Totes les entitats públiques han d'implementar controls sobre la seguretat de la informació i les comunicacions, d'acord amb les directrius establertes en l'ENS, que és d'obligat compliment.

Atès l'abast tan ampli de les mesures que preveu l'ENS, la seva complexitat i la intensa dedicació que requereix una revisió completa del seu compliment, el 12 de novembre del 2018, en la Conferència de Presidents dels Òrgans de Control Extern es va aprovar la GPF-OCEX- 5313, en la qual es van definir 8 controls bàsics de ciberseguretat que mantenien la màxima coherència amb els postulats de l'ENS.

Els 8 CBCS són controls globals formats per 26 subcontrols, detallats en el quadre 8 de l'annex. Si aquests controls s'apliquen correctament impliquen una reducció al voltant del 85% del risc davant de ciberatacs.

5.1. PROCEDIMENTS DE FISCALITZACIÓ I EXECUCIÓ DEL TREBALL

Els procediments d'aquesta fiscalització i l'execució del treball de camp segueixen el contingut de la GPF-OCEX 5313, i en concret els qüestionaris i fitxes de revisió inclosos en l'annex 2 i 3, respectivament, de la guia esmentada.

Com a resultat de la revisió dels 8 CBCS, a continuació es presenten les troballes de l'auditoria que sustenten les conclusions i recomanacions d'aquest informe. La informació es mostrarà mantenint la màxima confidencialitat possible, atès el caràcter sensible de la informació revisada i el risc que la seva difusió significaria sobre la seguretat dels sistemes

de la informació de l'entitat. La informació totalment detallada només s'ha facilitat a l'Ajuntament.

5.1.1. Inventari i control de dispositius físics (CBCS 1)

El CBCS 1 ajuda les organitzacions a definir què cal defensar. L'inventari ha de ser tan complet com sigui possible, i en qualsevol cas s'ha de saber què hi ha a la xarxa perquè pugui ser defensat i, posteriorment, impedir que dispositius no autoritzats s'uneixin a la xarxa.

Objectiu del control

Gestionar activament (inventariar, revisar i corregir) tots els dispositius de maquinari a la xarxa, de manera que només els dispositius autoritzats hi tinguin accés.

Situació del control

L'Ajuntament disposa de 2 inventaris de dispositius físics. En el primer hi consten els equips, servidors, dispositius de xarxa, etc., mitjançant una eina específica, i en l'altre, els equips d'usuari, que es gestionen amb una base de dades interna des del Servei de Sistemes d'Informació i Telecomunicacions.

S'ha comprovat que els 2 inventaris es troben complets i compleixen els requeriments del control, però no s'han formalitzat per escrit els procediments per donar d'alta o baixa d'aquests inventaris els actius.

La xarxa està segmentada en diferents VLAN[6] que només permeten els ports i serveis estrictament necessaris per a l'organització. S'ha constatat que es disposa d'un programari per controlar els actius connectats a l'organització, i aquest programari es revisa periòdicament per detectar en la xarxa equips no autoritzats i la seva ubicació. No obstant això, s'han detectat algunes mancances que s'han comunicat a l'Ajuntament.

De les evidències obtingudes en la revisió d'aquest control, relatiu al control d'actius físics, la valoració general assoleix un 79,90% d'índex de maduresa, que correspon a un nivell de maduresa N2 – Repetible, però intuïtiu; és a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

6. Xarxa d'àrea local virtual (VLAN per les sigles en anglès: Virtual LAN). És una tecnologia de xarxes que permet crear xarxes lògiques independents dins de la mateixa xarxa física.

5.1.2. Inventari i control de programari autoritzat i no autoritzat (CBCS 2)

La finalitat del CBCS 2 és assegurar que només està permès executar programari autoritzat en els sistemes de l'organització i que s'impedeix l'execució de programari potencialment vulnerable.

Objectiu del control

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

Situació del control

S'ha analitzat la gestió que fa l'Ajuntament de l'inventari i control de programari i s'ha verificat que el procediment perquè els treballadors de l'Ajuntament sol·licitin la instal·lació de programari no està documentat.

Sens perjudici que es revisa el programari amb la mateixa eina que s'utilitza per a l'inventari de maquinari, el recurs es considera insuficient ja que l'Ajuntament no disposa d'un llistat de programari autoritzat ni duu a terme periòdicament un control del programari no permès.

Respecte del programari amb suport del fabricant, l'Ajuntament disposa de sistemes operatius sense aquest suport i, a més, no hi ha cap pla de manteniment d'aquest programari.

També s'ha comprovat que, tot i que l'Ajuntament no disposa d'eines específiques per controlar i impedir la instal·lació de programari no autoritzat, els usuaris no són administradors locals i per tant no tenen la capacitat d'instal·lar programari.

De les evidències obtingudes en la revisió d'aquest control, relatiu al control de programari autoritzat i no autoritzat, la valoració general assoleix un 75% d'índex de maduresa, que correspon a un nivell de maduresa N2 – Repetible, però intuïtiu, és a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

5.1.3. Procés continu d'identificació i correcció de vulnerabilitats (CBCS 3)

El CBCS 3 està definit per identificar i, si escau, eliminar les debilitats tècniques existents en els sistemes d'informació de l'organització permet reduir la probabilitat que els sistemes siguin vulnerables.

Objectiu del control

Disposar d'un procés continu de revisió que permeti obtenir informació sobre noves vulnerabilitats, identificar-les, corregir-les i reduir la finestra d'oportunitat dels atacants.

Situació del control

L'Ajuntament utilitza diferents mitjans per identificar vulnerabilitats, com la subscripció a comunicacions de fabricants o d'organismes de referència, com pot ser el Centre Criptogràfic Nacional, entre d'altres.

La priorització de la resolució de les vulnerabilitats i els defectes de seguretat identificats es fa mitjançant un procediment informal basat en la gestió de riscos, i aquest procediment no consta formalment documentat.

S'ha observat que l'Ajuntament disposa d'eines per gestionar i instal·lar pedaços i actualitzacions de seguretat, malgrat que el procediment a seguir per a la instal·lació de pedaços no està degudament formalitzat.

De les evidències obtingudes en la revisió d'aquest control, relatiu al procés continu d'identificació i correcció de vulnerabilitats, la valoració general assoleix un 50% d'índex de maduresa, que correspon a un nivell de maduresa N2 – Repetible, però intuïtiu; és a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

5.1.4. Ús controlat de privilegis administratius (CBCS 4)

El CBCS 4 garanteix que els privilegis d'administració de sistemes estiguin assignats únicament als empleats que els necessiten, segons les funcions que exerceixen, i que l'entitat pugui atribuir les accions administratives a usuaris individuals.

Objectiu del control

Desenvolupar processos i utilitzar eines per identificar, controlar, prevenir i corregir l'ús, l'assignació i la configuració de privilegis administratius en ordinadors, xarxes i aplicacions.

Situació del control

Tots els comptes d'administració estan registrats en un programa al qual només tenen accés els tècnics de la secció d'infraestructures i el cap de servei.

Només disposa de privilegis administratius el personal de sistemes, amb un únic usuari d'administració per a tots els membres del servei. La resta del personal de l'Ajuntament no disposa de privilegis i tots tenen un identificador únic.

En relació amb els mecanismes d'autenticació, les contrasenyes compleixen les regles bàsiques de seguretat, però s'ha comprovat que hi ha certes mancances en aquests mecanismes.

Les contrasenyes per defecte dels comptes que no s'utilitzen o bé les que són estàndard s'eliminen o es reanomenen abans de la posada en funcionament d'un sistema, però sense que es compleixin tots els requisits de fortificació necessaris.

El control de l'ús dels comptes d'administració que realitza l'Ajuntament ha posat de manifest una sèrie de debilitats que ja s'han notificat a l'Ajuntament.

De les evidències obtingudes en la revisió d'aquest control, relatiu a l'ús controlat de privilegis administratius, la valoració general assoleix un 30% d'índex de maduresa, que correspon a un nivell de maduresa N1 – Inicial / *ad hoc*; és a dir, els processos existeixen, però no es gestionen o la seva gestió no està organitzada correctament.

5.1.5. Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors (CBCS 5)

El CBCS 5 controla si les configuracions predeterminades dels fabricants estan orientades a facilitar-ne l'ús i no necessàriament la seguretat. És important que es reconfigurin els sistemes d'acord amb els estàndards de seguretat.

Objectiu del control

Establir una configuració base segura per a dispositius mòbils, portàtils, equips de sobretaula i servidors, i gestionar-la activament utilitzant un procés rigorós de gestió de canvis i configuracions, per evitar que els atacants explotin serveis i configuracions vulnerables.

Situació del control

L'Ajuntament duu a terme algunes accions per fortificar o reforçar la seguretat dels sistemes abans de la seva posada en marxa, però no disposa d'un procediment documentat per fer-ho. Les accions no són suficients ni tan completes com haurien de ser.

També s'han trobat debilitats en els controls de l'Ajuntament en relació amb la detecció de canvis no autoritzats o erronis de la configuració per poder corregir-los en un període de temps oportú.

De les evidències obtingudes en la revisió d'aquest control, relatiu a les configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors, la valoració general assoleix un 20% d'índex de maduresa, que correspon a un nivell de maduresa N1 – Inicial / *ad hoc*; és a dir, els processos existeixen, però no es gestionen o la seva gestió no està ben organitzada.

5.1.6. Registre de l'activitat dels usuaris (CBCS 6)

El CBCS 6 controla si tots els sistemes i aplicacions tenen habilitades les traces d'auditoria, incloses les respostes a les preguntes des d'on, qui, què i quan, i si tenen definides accions d'alerta. En el supòsit d'un atac al sistema, aquest podria passar desapercebut de manera indefinida i amb danys irreversibles si no hi ha un registre d'auditoria.

Objectiu del control

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

Situació del control

L'Ajuntament disposa de diversos sistemes per gestionar els registres d'activitat. Pel que fa a l'emmagatzematge de *logs* s'ha observat un control força efectiu. No obstant això, no s'ha formalitzat documentalment quins esdeveniments de seguretat han de ser auditats i amb quina periodicitat, el temps de retenció abans d'eliminar-los ni el personal autoritzat a accedir-hi.

De les evidències obtingudes en la revisió d'aquest control, relatiu al registre de l'activitat dels usuaris, la valoració general assoleix un 45% d'índex de maduresa, que correspon a un nivell de maduresa N2 – Repetible, però intuïtiu; és a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

5.1.7. Còpies de seguretat de dades i sistemes (CBCS 7)

El CBCS 7 controla si l'organització té una capacitat fiable de recuperació de dades, quan es descobreixen atacants dels sistemes, ja que sovint aquests atacants fan canvis significatius de les configuracions i el programari, i pot ser extremadament difícil eliminar tots els aspectes de la seva presència en els sistemes.

Objectiu del control

Utilitzar processos i eines per fer la còpia de seguretat de la informació crítica amb una metodologia provada que permeti recuperar la informació en un temps oportú.

Situació del control

El procediment de les còpies de seguretat no està documentat formalment però s'ha comprovat que des del Servei de Sistemes d'Informació i Telecomunicacions es fan còpies de seguretat de tots els sistemes crítics, carpetes compartides i dades sensibles, amb els requisits necessaris per permetre recuperar les dades perdudes.

Aquestes còpies de seguretat gaudeixen de la mateixa seguretat que les dades originals, tot i que no es creen còpies de seguretat fora de línia ni s'utilitza criptografia per al xifratge de la informació.

No hi ha un calendari definit per a la realització de proves de restauració a partir de les còpies de seguretat i únicament es fan restauracions per necessitat.

De les evidències obtingudes en la revisió d'aquest control, relatiu a les còpies de seguretat de dades i sistemes, la valoració general assoleix un 75% d'índex de maduresa, que correspon a un nivell de maduresa N2 – Repetible, però intuïtiu; és a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

5.1.8. Compliment de legalitat (CBCS 8)

La normativa que afecta directament els sistemes de la informació és àmplia i variada. Amb el CBCS 8 es revisa el compliment dels principals aspectes normatius relacionats amb la seguretat de la informació.

Objectiu del control

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

Situació del control

a) Compliment de l'ENS

L'Ajuntament disposa d'una política de seguretat de la informació, aprovada per decret d'Alcaldia l'any 2019, en la qual es van nomenar els principals responsables de la gestió i la seguretat informàtica. Aquesta política, però, no compleix tots els requisits exigits per l'ENS.

Per altra banda, a la finalització del treball (31 de desembre del 2023) l'Ajuntament no havia fet l'auditoria de compliment de l'ENS per als sistemes de categoria mitjana i alta, no havia formalitzat la declaració d'aplicabilitat de l'ENS, ni havia formalitzat ni enviat les dades necessàries per a l'Informe de l'estat de la seguretat (Informe INES).

b) Compliment de la Llei orgànica de protecció de dades i del Reglament general de protecció de dades

L'any 2021, l'Ajuntament va designar una funcionària de carrera com a delegada de protecció de dades, de manera provisional i en forma d'encàrrec de funcions, i en la data de finalització del treball no s'havia proveït el lloc de treball pel procediment establert reglamentàriament.

No es disposa d'una anàlisi de riscos dels tractaments de dades ni s'ha dut a terme l'auditoria de protecció de dades.

c) Compliment de la legalitat del registre de factures

S'han auditat els sistemes del registre comptable de factures de l'exercici 2022, i s'ha observat que compleixen els criteris exigits per la Llei 25/2013, de 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures del sector públic.

Índex de maduresa

De les evidències obtingudes en la revisió d'aquest control, relatiu al compliment de legalitat, la valoració general assoleix un 50% d'índex de maduresa, que correspon a un nivell de maduresa N2 – Repetible, però intuïtiu; és a dir, els processos segueixen una pauta regular quan diferents persones duen a terme determinats procediments, però no hi ha procediments escrits ni activitats formatives.

5.2. GOVERNANÇA DE LA CIBERSEGURETAT

La governança és el procés d'establir i mantenir un marc de referència, i donar suport a l'estructura i els processos de gestió. Exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització.

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

Els òrgans superiors tenen una implicació i un compromís amb la ciberseguretat que ha quedat evident durant el treball de fiscalització i que implica que es faci una valoració positiva de la governança de ciberseguretat.

Tot i aquest compromís per part dels responsables, en la fiscalització s'han posat de manifest les debilitats següents:

- L'any 2019, l'Ajuntament va aprovar la política de seguretat, però aquesta política no ha estat revisada ni actualitzada.
- Hi ha una manca d'activitat efectiva i continuada del Comitè de Seguretat.
- Existeixen determinats incompliments normatius, detallats en l'apartat 5.1.8.

5.3. APLICACIÓ DEL REIAL DECRET 311/2022

El Reial decret 3/2010, de 8 de gener, va regular l'ENS i va determinar la política de seguretat que s'havia d'aplicar en la utilització de mitjans electrònics. El 5 de maig del 2022 va entrar en vigor el Reial decret 311/2022, que derogava l'anterior i que va actualitzar el marc normatiu i el va adequar al context estratègic existent per garantir la seguretat en l'administració digital.

D'acord amb els objectius i l'abast descrits en l'apartat 1.1, un cop revisats els 8 controls bàsics s'ha ampliat la valoració efectuada de la situació de l'Ajuntament amb una selecció addicional de controls revisats i la revisió de les accions efectuades.

Aquesta anàlisis ha tingut 2 vessants: la primera ha estat l'avaluació d'una selecció de controls addicionals relacionats amb la gestió dels usuaris i els drets d'accés als sistemes, i la segona, la revisió de les accions dutes a terme per l'Ajuntament entre la finalització del treball de camp i la redacció de l'informe per assolir el compliment del Reial decret 311/2022.

En la GPF-OCEX 5330, Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica, es preveuen 24 controls generals, classificats en 5 categories, alineats amb els requeriments que preveu l'ENS. D'aquests 24 controls, 7[7] es refereixen als controls bàsics analitzats i valorats en els apartats anteriors.

Per ampliar la valoració efectuada dels 8 controls bàsics, la Sindicatura ha inclòs la revisió de 4 controls addicionals classificats en la categoria de Controls d'accés a dades i programes, per considerar-los els més rellevants d'entre els controls generals que faltava revisar. En el quadre següent s'inclouen tots els controls de la categoria seleccionada.

7. El CBCS 1 i 2 estan inclosos en el mateix control general C1, Inventari de maquinari i programari, de la GPF-OCEX 5330.

Quadre 6. Controls d'accés a dades i programes

D.1: Ús controls de privilegis administratius (CBCS 4)*
D.2: Mecanisme d'identificació i autenticació
D.3: Gestió de drets d'accés
D.4: Gestió d'usuaris
D.5: Protecció de xarxes i comunicacions

Font: GPF-OCEX-5330.
* Analitzat en l'apartat 5.1.4.

L'execució del treball de valoració d'aquests 4 controls segueix el contingut de la GPF-OCEX 5330, i en concret els qüestionaris inclosos en l'annex 3 de la guia.

Els índexs de cada control addicional revisat es detallen en el quadre següent:

Quadre 7. Índex de maduresa i de compliment dels controls ampliats

Control	Índex de maduresa	Nivell de maduresa	Índex de compliment
D.2: Mecanisme d'identificació i autenticació	56,00	N2	70,00
D.3: Gestió de drets d'accés	63,30	N2	79,10
D.4: Gestió d'usuaris	60,00	N2	75,00
D.5: Protecció de xarxes i comunicacions	76,00	N2	95,00
Índex general*	**63,80**	**N2**	**79,80**

Font: Elaboració pròpia.
* El CBCS 4 té un índex de maduresa i de compliment del 30% i del 37,5%, respectivament, que no s'ha tingut en compte en la valoració d'aquests controls addicionals.

Pel que fa al resultat de la revisió dels controls i subcontrols seleccionats, destaca principalment la protecció de xarxes i comunicacions, amb un índex de compliment del 95%, seguit de la gestió de drets d'accés, amb un 79,10%.

En conjunt, els subcontrols que integren els aspectes analitzats denoten que l'Ajuntament té índexs de compliment per sobre del 70%, que significa que té unes pràctiques de seguretat implantades que es duen a terme puntualment, i alguna de manera periòdica, però no han estat documentades.

Pel que fa a les feines dutes a terme per l'Ajuntament per donar compliment al Reial decret 311/2022, que a la data de redacció d'aquest informe (juny 2024) no havia acreditat l'adequació a l'ENS, cal destacar les accions següents:

- Els òrgans de govern han promogut l'adequació de la política de seguretat de la informació a la normativa. També han impulsat l'aprovació de la normativa de seguretat que mancava aprovar.

- Els diferents responsables analitzaven els possibles riscos i anaven definint els procediments que s'havia posat de manifest que faltaven analitzar.

- L'Ajuntament ha contractat una empresa consultora que col·labora en l'obtenció del certificat ISO 27001, relatiu a la seguretat i privacitat de la informació.

6. RESPONSABILITATS

6.1. DE LA DIRECCIÓ DE L'ENTITAT

Els òrgans superiors de l'Ajuntament són els responsables que hi hagi uns controls adequats sobre els sistemes d'informació i les comunicacions. D'acord amb les seves competències, han de garantir que el funcionament de l'entitat sigui conforme a les normes aplicables i que els controls interns proporcionin una garantia raonable que la informació, els serveis i els sistemes d'informació que els donen suport compleixin les 5 dimensions de seguretat de la informació que estableix l'ENS: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.

6.2. DE LA SINDICATURA

Els objectius, l'abast i la metodologia utilitzada en el treball de fiscalització de la Sindicatura, d'acord amb el que s'exposa en l'apartat 1.1 i en l'apartat 2, són obtenir una seguretat limitada sobre la situació dels controls bàsics de ciberseguretat revisats.

Els procediments realitzats en una auditoria de seguretat limitada són reduïts en comparació amb els que es requereixen per obtenir una seguretat raonable, però s'espera que el nivell de seguretat sigui, d'acord amb el judici professional de l'auditor, significatiu per als destinataris de l'informe. La seguretat limitada no garanteix que una fiscalització realitzada d'acord amb els principis fonamentals de fiscalització dels òrgans de control extern i les normes internacionals d'auditoria adaptades al sector públic detecti sempre un incompliment quan existeix.

El detall dels resultats de la fiscalització conté informació de caràcter reservat que, en cas que es difongui, podria arribar a afectar seriosament la seguretat dels sistemes d'informació de l'entitat. Per aquest motiu, s'ha proporcionat als responsables corresponents el contingut detallat de cadascun dels controls revisats amb caràcter confidencial i per canals xifrats, perquè es puguin adoptar les mesures correctores oportunes. L'Ajuntament haurà de determinar l'ús i la publicitat que estimi pertinents, d'acord amb la valoració d'aquesta confidencialitat. En conseqüència, els resultats del treball realitzat i les conclusions que consten en aquest informe es presenten de manera sintètica.

7. ANNEX: ELS CONTROLS BÀSICS DE CIBERSEGURETAT I ELS SEUS SUBCONTROLS

Quadre 8. Els CBCS i els seus subcontrols

Control		Objectiu del control	Subcontrols
CBCS 1	Inventari i control de dispositius físics	Gestionar activament tots els dispositius de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguin accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
			CBCS 1-2: Control d'actius físics no autoritzats L'entitat disposa de mesures de seguretat per controlar (detectar i restringir) l'accés a dispositius físics no autoritzats.
CBCS 2	Inventari i control de programari autoritzat	Gestionar activament tot el programari en els sistemes, de manera que només es pugui instal·lar i executar programari autoritzat.	CBCS 2-1: Inventari de programari autoritzat L'entitat disposa d'un inventari de programari complet, actualitzat i detallat.
			CBCS 2-2: Programari amb suport del fabricant El programari utilitzat per l'entitat té suport del fabricant. En cas contrari, es marca en l'inventari com a fora de suport.
			CBCS 2-3: Control de programari no autoritzat L'entitat disposa de mecanismes que impedeixen la instal·lació i l'execució de programari no autoritzat.
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per obtenir informació sobre noves vulnerabilitats, identificar-les, solucionar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats Hi ha un procés per identificar les vulnerabilitats dels components del sistema que assegura que s'identifiquen en temps oportú.
			CBCS 3-2: Priorització de vulnerabilitats Les vulnerabilitats identificades s'analitzen i es prioritzen per resoldre-les segons el risc que suposen per a la seguretat del sistema.
			CBCS 3-3: Resolució de vulnerabilitats Es fa un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que es resolen en el temps previst en el procediment.
			CBCS 3-4: Pedaços L'entitat disposa de procediments i eines que permeten aplicar els pedaços de seguretat publicats pels fabricants en un temps raonable.

Control		Objectiu del control	Subcontrols
CBCS 4	Ús controlat de privilegis administratius	Desenvolupar processos i utilitzar eines per identificar, controlar, prevenir i corregir l'ús i la configuració de privilegis administratius en ordinadors, xarxes i aplicacions.	CBCS 4-1: Inventari i control de comptes d'administració Els privilegis d'administració estan limitats adequadament i l'entitat disposa d'un inventari de comptes d'administració que en facilita el control correcte.
			CBCS 4-2: Canvi de contrasenyes per defecte Les contrasenyes per defecte dels comptes que no s'utilitzen o bé les que són estàndard es canvien abans de l'entrada en producció del sistema.
			CBCS 4-3: Ús exclusiu de comptes d'administració Els comptes d'administració només s'utilitzen per a les tasques estrictament necessàries.
			CBCS 4-4: Mecanismes d'autenticació Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes.
			CBCS 4-5: Auditoria i control de l'ús dels comptes amb privilegis d'administració L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades.
CBCS 5	Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors	Establir, implantar i gestionar la configuració de seguretat, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de prevenir atacs per mitjà de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
			CBCS 5-2: Gestió de la configuració L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seva correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6	Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria)	Recollir, gestionar i analitzar *logs* d'incidències que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de *logs* d'auditoria El *log* d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
			CBCS 6-2: Emmagatzematge de *logs*: conservació i protecció Els *logs* es conserven durant el temps indicat en la política de retenció, de manera que estan disponibles per a la seva consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.

Control		Objectiu del control	Subcontrols
			CBCS 6-3: Centralització i revisió dels registres de l'activitat dels usuaris Els *logs* de tots els sistemes es revisen periòdicament per detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels *logs* d'auditoria, de manera que se'n facilita la revisió.
			CBCS 6-4: Monitoratge i correlació L'entitat disposa d'un SIEM (sistema de gestió d'incidències i informació de seguretat) o una eina d'analítica de *logs* per la correlació i l'anàlisi.
CBCS 7	Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per fer la còpia de seguretat de la informació crítica amb una metodologia provada que permeti la recuperació de la informació en temps oportú.	CBCS 7-1: Còpia de seguretat de dades i sistemes L'entitat fa periòdicament còpies de seguretat automàtiques de totes les dades i configuracions del sistema.
			CBCS 7-2: Proves de recuperació Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica i es duu a terme un procés de recuperació de dades que permeti comprovar que el procés de còpia de seguretat funciona adequadament.
			CBCS 7-3: Protecció de les còpies de seguretat Les còpies de seguretat es protegeixen adequadament per mitjà de controls de seguretat física o xifratge mentre estan emmagatzemades o bé són transmeses a través de la xarxa.
CBCS 8	Compliment de legalitat	L'entitat compleix els requisits legals i reglamentaris que li són aplicables.	CBCS 8-1: Compliment de l'ENS L'entitat compleix els requisits establerts en l'ENS.
			CBCS 8-2: Compliment de la Llei orgànica de protecció de dades i del Reglament general de protecció de dades L'entitat compleix els requisits establerts en la Llei orgànica de protecció de dades i en el Reglament general de protecció de dades
			CBCS 8-3: Compliment de la Llei 25/2013, del 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures. L'entitat compleix els requisits establerts en la Llei 25/2013, del 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures.

Font: Elaboració pròpia.

8. TRÀMIT D'AL·LEGACIONS

D'acord amb la normativa vigent, el projecte d'informe de fiscalització va ser tramès a l'Ajuntament de Mataró el 17 de juny del 2024 per complir el tràmit d'al·legacions.

8.1. AL·LEGACIONS REBUDES

L'escrit d'al·legacions presentat per l'Ajuntament de Mataró, signat electrònicament el 2 de juliol de 2024, es reprodueix a continuació. Els annexos als quals fan referència les al·legacions queden dipositats en els arxius de la Sindicatura.

Ajuntament de Mataró

Ajuntament de Mataró
La Riera, 48
www.mataro.cat

CARTA

SR. MANEL RODRIGUEZ TIÓ
SÍNDIC
SINDICATURA DE COMPTES DE CATALUNYA

Benvolgut senyor,

Vist l'informe de fiscalització núm. 28/2023-E que ens han fet arribar, amb el nostre número de registre d'entrada E-08121-2024-042620 del 17 de juny de 2024, corresponent a l'Ajuntament de Mataró sobre Controls bàsics de ciberseguretat, exercici 2023, revisat pel Ple de la Sindicatura de Comptes de Catalunya, perquè us presentem les al·legacions pertinents fins al 2 de juliol de 2024, us informem i adjuntem les corresponents al·legacions prèvies a l'espera de l'emissió de l'informe definitiu.

Al·legació primera

En l'apartat "3. CONCLUSIONS" subapartat "2) Governança de la ciberseguretat" on diu:

> *"L'any 2017 es va crear el Comitè de Seguretat en Protecció de Dades, perquè fes les funcions del Comitè de Seguretat de la Informació, però no s'ha reunit mai"*

L'Ajuntament de Mataró informa que el *Comitè de Seguretat en Protecció de Dades* es va reunir el dia 18 de juliol de 2017 amb el següent ordre del dia :

" Benvolguts i benvolgudes,

Us convoco a la reunió del Comitè de Seguretat el proper dia 18/7/2017 a les 16h a la sala dels lleons amb el següent

Ordre del dia:

1. Aprovació de l'acta 1/2017 de data 26/5/2017.
2. Conclusions auditoria 2016.
3. Pla d'acció.
4. Donar compte reunions Comitè Tècnic
5. Precs i preguntes .

Mataró, 24 de maig de 2017

Juan Carlos Jerez
President del Comitè de Seguretat"

* S'adjunta acta de la reunió en arxiu 01_Reunions_Comite_seguretat.zip

Tanmateix, el comitè tècnic de seguretat s'ha reunit 15 vegades entre el 2018 i el 2022.

* S'adjunten les actes en l'arxiu 02_Reunions_Comite_tecnic_seguretat.zip

Al·legació segona

En l'apartat "3. CONCLUSIONS" subapartat "2) Governança de la ciberseguretat" on diu:

La política de seguretat de la informació no està completa ni actualitzada.

No s'han formalitzat ni aprovat totes les normes i els procediments de seguretat necessaris.

L'Ajuntament de Mataró informa que l'actual política de seguretat es va publicar per Decret d'Alcaldia 3985 el dia 22 de maig de 2019 d'acord amb Reial Decret 951/2015, de 23 d'octubre, de modificació del RD 3/2010, que regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica i que aquesta política dona compliment a l'esmentat RD.

L'Ajuntament de Mataró informa que amb posterioritat, el dia 5 de maig de 2022 es va publicar el "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad" que modifica l'esmentat Esquema Nacional de Seguretat i que actualment l'Ajuntament de Mataró està fent la revisió de la política de seguretat per incorporar el requeriments de la nova norma, con queda palès per la contractació del servei d'assessorament, consultoria, assistència tècnica i jurídica en matèria de protecció de dades i de la implementació de l'esquema nacional de seguretat de l'Ajuntament de Mataró.

https://contractaciopublica.cat/ca/detall-publicacio/a8a06444-e755-41da-aed5-7bcf0f457580/300059942

En el marc d'aquest contracte, l'Ajuntament de Mataró amb el suport de l'empresa adjudicatària ha iniciat les tasques per tal d'elaborar tota la documentació per tal de donar compliment als requisits formals del Reial Decret 311/2022.

A dia d'avui, la Política de Seguretat ha estat actualitzada i s'ha elaborat la Normativa de Seguretat, que es troben en fase de revisió interna a l'espera de la seva aprovació formal i comunicació al conjunt de l'organització.

Al·legació tercera

En apartat "5.1.2 Inventari i control de programari autoritzat i no autoritzat (CBCS 2)", on diu:

> *Sens perjudici que es revisa el programari amb la mateixa eina que s'utilitza per a l'inventari de maquinari, el recurs es considera insuficient ja que l'Ajuntament no disposa d'un llistat de programari autoritzat ni duu a terme periòdicament un control del programari no permès.*

L'Ajuntament de Mataró informa que disposa d'un document "3SPA-Programari_corporatiu_per_ordinadors_personals", on s'especifica "Configuració de programari corporatiu dels ordinadors personals l'Ajuntament de Mataró"

> * S'adjunta document on es mostra l'inventari de programari autoritzat.

Al·legació quarta

En l'apartat "5.1.2 Inventari i control de programari autoritzat i no autoritzat (CBCS 2)", on diu:

> *També s'ha comprovat que, tot i que l'Ajuntament no disposa d'eines específiques per controlar i impedir la instal·lació de programari no autoritzat, els usuaris no són administradors locals i per tant no tenen la capacitat d'instal·lar programari.*

L'Ajuntament de Mataró considera que haver restringit la capacitat d'instal·lar programari és un mecanisme prou robust que evita la necessitat d'instal·lar un programari específic per evitar instal·lacions de programari no autoritzat.

Esperem rebre ben aviat la vostra conformitat i us saludem atentament.

Mataró, a la data de la signatura electrònica

8.2. TRACTAMENT DE LES AL·LEGACIONS

Les al·legacions formulades han estat analitzades i valorades per la Sindicatura de Comptes.

El text del projecte d'informe no s'ha alterat perquè s'entén que les al·legacions trameses són explicacions que confirmen la situació descrita inicialment o perquè no es comparteixen els judicis que s'hi exposen.

APROVACIÓ DE L'INFORME

Certifico que a Barcelona, el 16 de juliol del 2024, reunit el Ple de la Sindicatura de Comptes, presidit pel síndic major, Miquel Salazar Canalda, amb l'assistència dels síndics Anna Tarrach Colls, Manel Rodríguez Tió, Llum Rodríguez Rodríguez, Maria Àngels Cabasés Piqué, Ferran Roquer i Padrosa i Josep Viñas i Xifra, i de la secretària general de la Sindicatura, Marta Junquera i Bernal, actuant com a ponent el síndic Manel Rodríguez Tió, amb deliberació prèvia s'acorda aprovar l'informe de fiscalització 9/2024, relatiu a l'Ajuntament de Mataró, controls bàsics de ciberseguretat, exercici 2023.

I, perquè així consti i tingui els efectes que corresponguin, signo aquesta certificació, amb el vistiplau del síndic major.

SINDICATURA DE COMPTES DE CATALUNYA

Marta Junquera Bernal - DNI 46618081W (SIG)
2024.07.31 08:18:21 +02'00'

La secretària general

Vist i plau,

SINDICATURA DE COMPTES DE CATALUNYA

Miquel Salazar Canalda - DNI 46319247F (SIG)
2024.07.31 08:31:32 +02'00'

El síndic major