INFORME 16/2024

AJUNTAMENT DE SANTA COLOMA DE GRAMENET
CONTROLS BÀSICS DE CIBERSEGURETAT, EXERCICI 2023

SINDICATURA DE COMPTES DE CATALUNYA

INFORME 16/2024

AJUNTAMENT DE SANTA COLOMA DE GRAMENET
CONTROLS BÀSICS DE CIBERSEGURETAT, EXERCICI 2023

SINDICATURA DE COMPTES DE CATALUNYA

Edició: novembre 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	Control bàsic 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 fiscalització de seguretat limitada relatiu als controls bàsics de ciberseguretat de l'Ajuntament de Santa Coloma de Gramenet (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 detallen 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: GPF-OCEX 5313.

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 que l'auditor consideri si el control, individualment o en combinació amb altres controls, és capaç de preveure de manera eficaç, 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.

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 30 de maig de 2024, 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, el treball efectuat s'ha ampliat 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, 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 d'activitats de la institució. Per dur a terme aquesta auditoria s'han 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 dut a terme, 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, l'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'article 46 de la llei 18/2010, del 7 de juny, de la Sindicatura de comptes, i l'apartat 10 de la GPF-OCEX 5311, fins que a les plantilles dels òrgans de control extern no s'hi incorporin auditors de sistemes d'informació i experts en ciberseguretat, es disposa del recurs de contractar experts externs i professionals especialitzats.

1.2. ENS FISCALITZAT

1.2.1. Activitats i organització

El municipi de Santa Coloma de Gramenet 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 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 bàsics de l'Ajuntament de Santa Coloma de Gramenet són el Ple, la Comissió de Govern, l'alcaldessa, els tinents d'alcalde i la Comissió Especial de Comptes.

En l'exercici fiscalitzat, l'Ajuntament disposava dels òrgans complementaris següents: la Comissió Informativa Permanent, les Comissions Especials, la Junta de Portaveus, els presidents dels Grups Municipals, els Consells i Comissions Sectorials de Participació, el Consell d'Entitats Ciutadanes i els regidors de Districte.

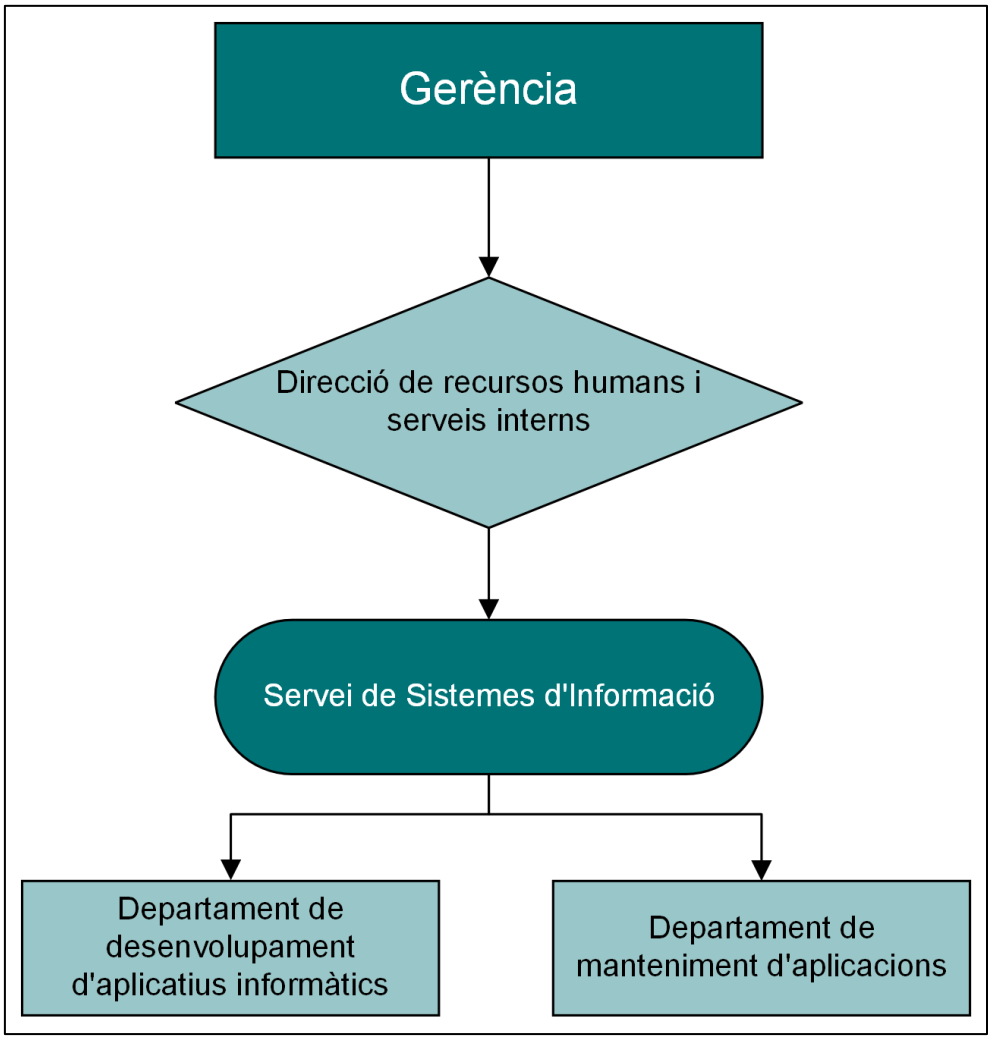
Pel que fa als ens dependents, en l'exercici 2023 l'Ajuntament tenia constituït 1 organisme autònom i 3 societats mercantils. Aquests ens eren els següents:

- Patronat de la Música de Santa Coloma de Gramenet
- GRAMEIMPULS, SA
- GRAMEPARK, SA
- BressolGramenet, SA

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

La unitat de Servei de Sistemes d'Informació té la missió d'oferir les eines informàtiques i de comunicacions necessàries per tal que els treballadors de l'Ajuntament puguin dur a terme les seves tasques de manera que s'optimitzin els recursos econòmics i personals al seu abast. 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



Font: Elaboració pròpia a partir de les dades facilitades per l'Ajuntament.

Els principals serveis que presta la unitat són els següents:

- Suport informàtic. Assistència remota i presencial als usuaris davant les incidències relacionades amb el programari i el maquinari que l'Ajuntament posa al seu abast perquè duguin a terme les seves tasques.

- Desenvolupament i manteniment d'aplicacions. Anàlisi, desenvolupament i implantació de noves aplicacions. Manteniment correctiu i evolutiu de les aplicacions internes. Seguiment i implantació de noves versions, i donar compte de les incidències al proveïdor d'aplicacions externes.

- Gestió d'usuaris. Gestió d'alta i baixa de comptes d'usuaris, els seus perfils i els seus privilegis d'accés, tant a l'aplicació com als recursos compartits.

- Manteniment de la infraestructura dels sistemes d'informació i comunicació. Conjunt de tasques de manteniment correctiu i preventiu dels elements que formen la infraestructura dels sistemes d'informació i comunicacions, com per exemple la instal·lació i actualització de noves versions de programari, microprogramari i execució de còpies de seguretat, entre altres. Monitorització de sistemes automatitzats i aplicacions i actuacions en cas d'incidència.

En l'exercici 2023 el nombre de places assignades a aquesta unitat era de 17, ocupades amb 4 funcionaris de carrera, 9 funcionaris interins i 4 laborals.

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: o El procediment està formalitzat (documentat i aprovat) i actualitzat. o 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: o Se segueix un procediment, malgrat que pot no estar formalitzat o presentar aspectes de millora (detall, nivell d'actualització, etc.). o 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: o Se segueix un procediment, malgrat que pot no estar formalitzat. o El resultat de les proves d'implementació i eficàcia operativa és satisfactori. • Cobreix en línies generals l'objectiu de control, però: o No se segueix un procediment clar. o Les proves realitzades per verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius malgrat que no són generalitzats).
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.
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.

Nivell	Índex	Descripció
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 els següents:

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%.

La guia CCN-STIC-824[4] 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%.

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

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

òrgans de govern i analitzada a partir del que preveu la GPF-OCEX 5314, Governança de la ciberseguretat i la seva auditoria. Es destaquen els aspectes següents:

- L'existència de polítiques de seguretat de la informació aprovades pels òrgans de govern 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 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 Santa Coloma de Gramenet amb l'abast i la metodologia descrits en l'apartat 1.1 i en 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 fiscalització realitzada i els indicadors reflecteixen la situació a 30 de maig del 2024. El grau de control en la gestió dels CBCS arriba a un índex de maduresa general del 57,25%, 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:

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	60,00	N2	75,00
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	45,00	N1	56,25
CBCS 4	Ús controlat de privilegis administratius	40,00	N1	50,00
CBCS 5	Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors	30,00	N1	37,50
CBCS 6	Registre de l'activitat dels usuaris	70,00	N2	87,50
CBCS 7	Còpies de seguretat de dades i sistemes	78,00	N2	97,50
CBCS 8	Compliment de legalitat	60,00	N2	75,00
Índex general		**57,25**	**N2**	**71,56**

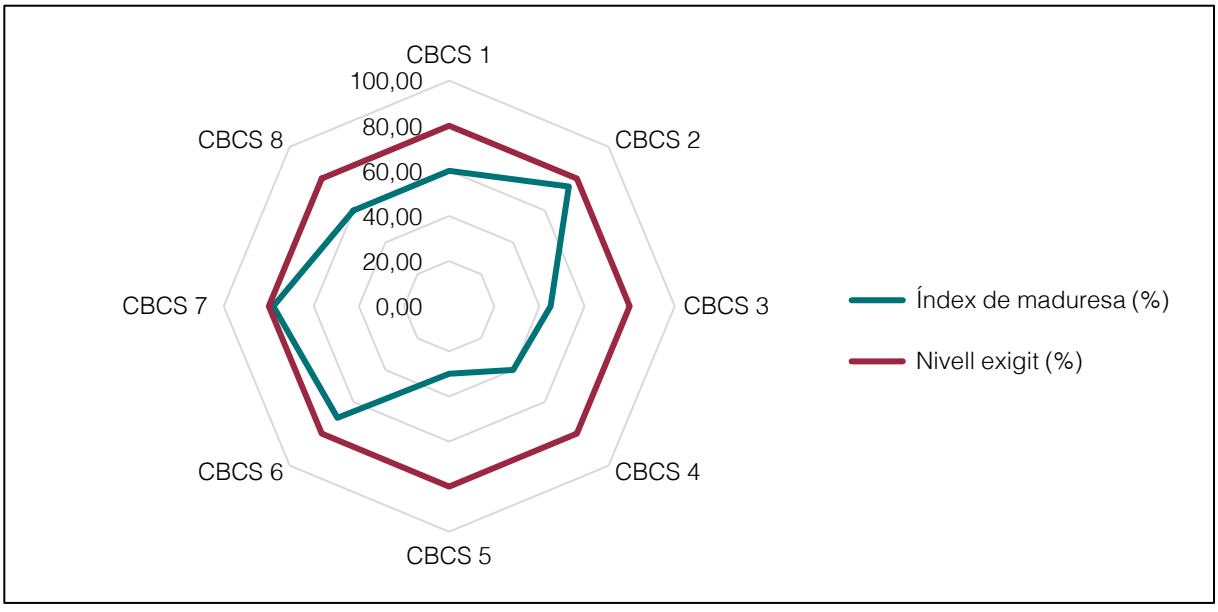
Font: Elaboració pròpia.

* Existeixen 6 nivells de maduresa, que s'identifiquen i es defineixen en el quadre 3.

L'índex de compliment general dels CBCS és del 71,56%, 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 7, Còpies de seguretat de dades i sistemes, que assoleix un índex de maduresa del 78% i un de compliment del 97,50%. 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 30% i un de compliment del 37,50%.

En el cas del CBCS 3, Procés continu d'identificació i correcció de vulnerabilitats, el 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 l'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 de govern 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.

Existeix un compromís amb la ciberseguretat per part dels òrgans de govern de l'Ajuntament i dels gestors i responsables de les àrees revisades, no obstant això, s'han identificat mancances rellevants que dificulten la implementació d'un sistema efectiu que garanteixi la ciberresiliència. Les mancances més significatives són les següents (vegeu l'apartat 5.2):

- Els òrgans de govern no han aprovat la política de seguretat de la informació ni tampoc les normes i procediments de seguretat que tenien redactades.

- No s'ha creat el Comitè de Seguretat de la Informació ni el Comitè de Seguretat Corporativa tal com estableix la política de seguretat definida.

- No existeixen determinats rols clau en l'organització, com el responsable de seguretat. De fet, no han estat nomenats cap dels 4 responsables en matèria de seguretat que determina l'ENS.

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'Ajuntament 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

A la finalització de la redacció d'aquest informe (juliol del 2024) l'Ajuntament no havia acreditat l'adequació a l'ENS i no ha treballat de manera proactiva en l'aprovació de la normativa ni dels procediments que li faltaven per donar compliment al Reial decret 311/2022. Tampoc ha designat els 4 responsables que determina l'ENS els quals permetrien la coordinació efectiva de les àrees i l'adopció de mesures de millora contínua. Pel que fa als 2 comitès de seguretat, l'Ajuntament no ha avançat en la seva creació.

En relació amb els 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 que s'han d'adoptar per al compliment de la legalitat.

1. Els òrgans de govern haurien de promoure l'aprovació de la normativa de seguretat existent i incentivar actuacions que fomentessin la cultura en matèria de ciberseguretat amb una direcció estratègica i coordinada.

2. Caldria aprovar els manuals i protocols existents i formalitzar-ne per aquells procediments que falten però que de manera informal i periòdica està duent a terme el personal de l'Ajuntament.

3. 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.

4. 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.

5. S'haurien de fer revisions periòdiques dels registres d'activitat i indicar en la documentació del sistema els esdeveniments de seguretat que seran auditats i el temps que els responsables els han de retenir abans de l'eliminació.

6. Per fer un ús racional dels privilegis d'administrador, caldria que els usuaris amb aquest privilegi disposin addicionalment d'un usuari nominatiu sense privilegis per dur a terme les tasques habituals.

7. Caldria dedicar esforços a corregir, en un temps raonable, les no conformitats i incidències detectades en l'auditoria de protecció de dades.

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 CBCS 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 s'apliquen correctament els 7 primers controls hi ha una important reducció del risc davant de possibles ciberatacs.

5.1. CONTROLS BÀSICS DE CIBERSEGURETAT

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 els annexos 2 i 3, respectivament, de la guia esmentada.

A continuació es presenten les troballes de l'auditoria que sustenten les conclusions i recomanacions d'aquest informe, com a resultat de la revisió dels 8 CBCS. 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 dels dispositius físics 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 ha dissenyat i redactat un procediment per a la recepció, l'inventari, la configuració i l'assignació d'equips personals als usuaris, però aquest no ha estat aprovat pels òrgans responsables. Així mateix, també ha definit el procediment d'assignació d'equips i el model que cal formalitzar per controlar l'entrega d'actius.

S'ha comprovat que l'Ajuntament ha desenvolupat un programari propi que li permet inventariar i controlar els actius físics, però l'eina no permet l'actualització automàtica ni contínua de l'inventari.

No s'ha obtingut evidència que els canvis d'ubicació d'un actiu s'hagin recollit en l'inventari i l'Ajuntament no efectua revisions periòdiques per mantenir aquest inventari actualitzat.

El control d'actius físics no autoritzats que duu a terme l'Ajuntament han posat de manifest una sèrie de debilitats que s'han notificat directament a l'Ajuntament.

De les evidències obtingudes en la revisió d'aquest control, relatiu al control d'actius físics, la valoració general assoleix un 60% 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.

5.1.2. 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 executar 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 del control de programari i s'ha comprovat que disposa d'un procediment documentat per sol·licitar la instal·lació de programari, però no ha estat aprovat.

Encara que no es permet que els usuaris puguin instal·lar programari sense demanar autorització, i que l'Ajuntament disposa d'una llista d'aplicacions restringides, el control és insuficient, ja que no es disposa d'un inventari de programari, el llistat d'aplicacions restringides no està actualitzat i no es du a terme periòdicament un control del programari no autoritzat.

Respecte del programari amb suport del fabricant, s'ha observat que no existeix un pla de manteniment d'aquest programari d'acord amb les especificacions dels fabricants. El departament d'informàtica controla la data de finalització de suport dels fabricants i defineix plans de migració per aquest programari, però durant la fiscalització s'ha posat de manifest que existeixen servidors amb sistemes operatius que es troben fora de suport del fabricant.

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 i 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

La unitat de Servei de Sistemes d'Informació és l'encarregada d'identificar vulnerabilitats, i per determinades tasques de suport i d'actualització dels sistemes ha contractat els serveis en una empresa externa.

L'Ajuntament disposa de sistemes de prevenció d'intrusions però no fa escanejos de vulnerabilitat ni tests d'intrusió de manera periòdica. Tampoc fa auditories de codi font dels desenvolupaments interns de programari.

Per identificar vulnerabilitats no disposa de cap eina concreta, però utilitza diferents mitjans, com ara la subscripció a comunicacions de fabricants o d'organismes de referència: el Centre Criptogràfic Nacional, entre d'altres.

Pel que fa als procediments, l'Ajuntament en té 2 de documentats. Per una banda el de notificació i gestió d'incidències i per l'altra el d'actualització i instal·lació de pedaços als servidors.

S'ha posat de manifest que en algunes ocasions les accions efectuades no es corresponien amb les previsions definides en els manuals. Tanmateix, malgrat les mancances en la definició d'alguns procediments s'ha pogut comprovar que l'Ajuntament disposa d'eines per gestionar i instal·lar pedaços i actualitzacions de seguretat.

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 45% 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.

5.1.4. 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

La gestió de l'assignació de privilegis d'administració en els sistemes revisats varia segons el sistema. En general, l'Ajuntament ha fet un ús restringit dels usuaris amb permisos d'administració i disposa d'una eina específica per registrar aquests usuaris per sistemes.

S'ha verificat que no existeix un procediment formal per a l'alta i la baixa en els sistemes ni consta aprovat el procediment que regula l'inventari d'usuaris administradors. Pel que fa a l'assignació d'identificadors únics en funció del rol, no existeix homogeneïtat. Per una banda, s'ha detectat l'ús de comptes no nominatius compartits i per una altra, usuaris nominatius amb privilegis d'administrador.

L'Ajuntament no disposa d'una política que defineixi específicament els mecanismes d'autenticació dels comptes d'administració dels sistemes abans de posar-los en explotació o un cop posats en producció. A més, no hi ha cap procediment de fortificació o reforçament de la seguretat dels sistemes abans de posar-los en funcionament i les contrasenyes no compleixen totes les regles bàsiques de seguretat.

Els registres d'activitat del directori actiu són emmagatzemats i revisats, encara que s'ha constatat que en certs programes no es monitoritzen els registres d'activitat i això ha estat comunicat a l'Ajuntament pels canals establerts.

De les evidències obtingudes en la revisió d'aquest control, relatiu a l'ús controlat de privilegis administratius, la valoració general assoleix un 40% 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 assegura que l'entitat hagi reforçat les configuracions predeterminades dels fabricants de programari i maquinari de dispositius mòbils, portàtils, equips de sobretaula i servidors, que estan orientades a facilitar-ne l'ús i no necessàriament a garantir 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 realitza algunes accions per fortificar o reforçar la seguretat dels sistemes dels actius abans de la seva posada en marxa però no disposa d'un procediment documentat, de guies de fortificació ni fa servir plantilles de configuració de seguretat a tots els sistemes. Tampoc fa proves de seguretat dels sistemes abans de passar a producció per comprovar que compleixen els criteris en matèria de seguretat.

Encara que els usuaris no poden modificar la seguretat dels sistemes, s'han trobat debilitats en els controls que realitza 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 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.

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

El CBCS 6 està definit per establir 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. Un atac al sistema 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

De la revisió de les activitats efectuades per l'Ajuntament per al registre de l'activitat dels usuaris s'ha constatat que no existeix un procediment formalment aprovat i que l'Ajuntament no disposa d'un pla que garanteixi la capacitat d'emmagatzematge atenent al volum i a la política de conservació. Es registra l'activitat del directori actiu, del sistema de fitxers, de l'antivirus i d'algunes aplicacions.

Pel que fa a l'emmagatzematge, s'ha constatat que els esdeveniments del directori actiu, antivirus i tallafocs s'envien a una eina externa d'administració d'esdeveniments i informació, la qual els correlaciona. Aquesta eina és gestionada per un centre d'operacions de seguretat contractat a una empresa externa.

Tot i els registres d'activitats que realitza l'Ajuntament, no existeix un servidor que centralitzi els registres generats pels diferents sistemes.

Un programa específic s'encarrega de l'auditoria de l'activitat dels usuaris, però monitoritza únicament el directori actiu i el sistema de fitxers, i emmagatzema els registres en una base de dades del programari. L'eina d'administració d'esdeveniments i informació de seguretat fa revisions automatitzades dels registres, però aquestes revisions no són generals a tots els sistemes.

De les evidències obtingudes en la revisió d'aquest control, relatiu al registre de l'activitat dels usuaris, la valoració general assoleix un 70% 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 determina 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 està definit i és adequat, però no s'ha aprovat formalment. Per fer les còpies, l'Ajuntament fa servir una aplicació específica i es fan, tant en disc com en cinta.

S'ha comprovat que el contingut de les còpies és el definit en el procediment escrit i abasta el directori actiu, les bases de dades SQL, els servidors crítics i el repositori de fitxers.

Pel que fa a les proves de restauració, encara que se'n fan a partir de les còpies de seguretat, no existeix un calendari definit per fer-les i no queda documentat quan s'han efectuat. S'ha comprovat que només es documenta, mitjançant un full de càlcul, quan es fan recuperacions a sol·licitud d'algun usuari.

Aquestes còpies de seguretat gaudeixen de la mateixa seguretat que les dades originals, tant pel que fa a l'accés com a l'emmagatzematge i el transport. Només els administradors del sistema poden accedir al sistema de còpies de seguretat i al sistema de fitxers de les còpies. A més, es fan còpies de seguretat que no són accessibles a través de la xarxa.

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 78% 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

Des del 2014, l'Ajuntament disposa d'un document amb la política de seguretat. Aquest document, però, no està aprovat ni actualitzat.

Per altra banda, l'Ajuntament ha fet una auditoria de compliment de l'ENS per als sistemes de categoria mitjana i alta, però no ha dut a terme el procés d'adequació ni hi ha hagut la certificació de l'ENS. Tanmateix, ha formalitzat la declaració d'aplicabilitat de l'ENS, encara que aquesta declaració no està actualitzada.

L'Ajuntament no ha formalitzat ni ha tramès 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 2019, l'Ajuntament va adscriure, de manera provisional, un funcionari com a delegat de protecció de dades. A la data de finalització del treball (30 de maig del 2024) no s'havia proveït el lloc de treball pel procediment reglamentàriament establert. Aquest nomenament provisional es va notificar a l'Autoritat Catalana de Protecció de Dades.

No es disposa d'una anàlisi de riscos dels tractaments de dades, i el registre d'activitats de tractament no està actualitzat ni degudament aprovat. Per altra banda, l'any 2023 es va fer una auditoria en matèria de protecció de dades personals amb un resultat de 4 no conformitats.

c) Compliment de legalitat del registre de factures

L'Ajuntament disposa de l'auditoria de sistemes del registre comptable de factures de l'exercici 2022, d'acord amb la Llei 25/2013, del 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures del sector públic, la qual els òrgans de control intern han d'elaborar anualment.

Del contingut d'aquesta auditoria s'ha evidenciat que no s'ha revisat la gestió de la seguretat en aspectes relacionats amb la confidencialitat, l'autenticitat, la integritat, la traçabilitat i la disponibilitat de les dades i els serveis de gestió d'acord amb el que estableix la Guia per a les auditories dels registres comptables de factures elaborada per la Intervenció General de l'Administració de l'Estat.

d) Índex de maduresa

De les evidències obtingudes en la revisió d'aquest control, relatiu al compliment de legalitat, la valoració general assoleix un 60% 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[5] 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, és el president i la Junta de Govern. Ells són els responsables de garantir que el funcionament de l'organització és conforme a les normes aplicables i que existeixen 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 de l'ens.

Durant el treball de fiscalització s'ha evidenciat una implicació i un compromís amb la ciberseguretat insuficient per part dels òrgans de govern, i que, com a conseqüència d'això, l'Ajuntament no té establerta una adequada governança de la ciberseguretat. Les principals debilitats observades són les següents:

- L'Ajuntament disposa de la política de seguretat de la informació redactada i de les normes i els procediments de seguretat, però cap d'ells no ha estat aprovat pels òrgans de govern.

- No han designat el responsable de la informació, del servei, de la seguretat de la informació i del sistema que exigeix l'ENS.

- No s'ha creat el Comitè de Seguretat de la Informació ni el Comitè de Seguretat Corporativa tal com estableix la política de seguretat definida.

- L'Ajuntament no disposa d'un Pla Estratègic TIC o document equivalent, ni tampoc ha fet una anàlisi sobre els riscos que afecten els sistemes d'informació.

5. Definició d'acord amb l'apartat 1 de la GPF-OCEX 5314, Governança de la ciberseguretat i la seva auditoria.

- Existeixen determinats incompliments normatius, detallats en l'apartat 5.1.8.

No obstant això, s'han identificat alguns aspectes positius:

- S'ha verificat l'increment de les inversions previstes per a l'exercici 2024 que permetran desenvolupar projectes i implantar sistemes que tindran un potencial impacte positiu en el nivell de seguretat de l'organització.

- L'Ajuntament ha promogut entre el personal la conscienciació dels riscos existents en ciberseguretat, mitjançant la realització de cursos de formació.

5.3. APLICACIÓ DEL REIAL DECRET 311/2022

El Reial decret 3/2010, del 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 (juliol del 2024) 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[6] 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, perquè s'han considerat els més rellevants dels controls generals que faltava revisar. En el quadre següent s'inclouen tots els controls de la categoria seleccionada:

6. Els 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 (a)	Índex de compliment
D.2: Mecanisme d'identificació i autenticació	58,00	N2	72,50
D.3: Gestió de drets d'accés	62,00	N2	77,50
D.4: Gestió d'usuaris	59,00	N2	73,75
D.5: Protecció de xarxes i comunicacions	59,00	N2	73,75
Índex general (b)	**59,50**	N2	**74,38**

Font: Elaboració pròpia.

Notes:

(a) Existeixen 6 nivells de maduresa que s'identifiquen i es defineixen en el quadre 3.

(b) El CBCS 4 té un índex de maduresa i de compliment del 40% i del 50%, 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 la gestió de drets d'accés, amb un índex de compliment del 77,50%, tot i que els 4 controls tenen índexs de compliment molt similars.

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 que no han estat documentades.

Pel que fa a les feines dutes a terme per l'Ajuntament per donar compliment al Reial decret 311/2022, a la data de redacció d'aquest informe (juliol 2024) no s'havia acreditat l'adequa-

ció a l'ENS. Cal destacar que de manera proactiva no s'està aprovant la política de seguretat, no s'estan aprovant els procediments, no s'estan creant els comitès ni s'estan nomenant els responsables que determina l'ENS que permetrien la coordinació efectiva de les àrees i l'adopció de mesures de millora contínua.

6. RESPONSABILITATS

6.1. DE LA DIRECCIÓ DE L'ENTITAT

Els òrgans de govern 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 reservada 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 controls bàsics de ciberseguretat 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 Santa Coloma de Gramenet el 17 de setembre del 2024 per complir el tràmit d'al·legacions.

Una vegada transcorregut el termini establert no s'ha rebut cap escrit d'al·legacions de l'Ajuntament de Santa Coloma de Gramenet.

APROVACIÓ DE L'INFORME

Certifico que a Barcelona, el 22 d'octubre 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 16/2024, relatiu a l'Ajuntament de Santa Coloma de Gramenet: 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)
2024.11.15 13:49:58 +01'00'

La secretària general

Vist i plau,

SINDICATURA DE COMPTES DE CATALUNYA

Miquel Salazar Canalda - DNI 46319247F (AUT)
2024.11.15 14:54:00 +01'00'

El síndic major