SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

AUDITORIA DE CIBERSEGURETAT I DELS CONTROLS GENERALS DE TECNOLOGIES DE LA INFORMACIÓ DEL NOU SISTEMA SEDA DE L'AJUNTAMENT DE VALÈNCIA

Situació a 30 de setembre de 2023

RESUM

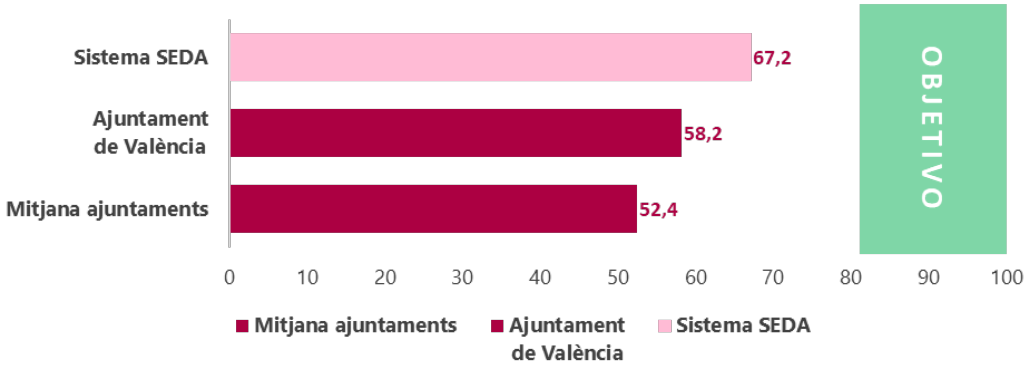
El sistema d'informació per a la gestió de la informació municipal de caràcter economicofinancer i comptable de l'Ajuntament de València ha sigut substituït en 2022 per l'aplicació SEDA. El sistema SEDA és la versió més actual del programari ERP de la companyia SAP.

Aquest canvi ha tingut com a objecte la simplificació dels processos per mitjà de la unificació en un sistema de diverses aplicacions municipals, l'augment de l'eficàcia i eficiència en el compliment de les obligacions legals i garantir la fiabilitat de la informació econòmica municipal.

En sintonia amb els objectius estratègics de la Sindicatura de Comptes, s'ha fet un treball d'auditoria de ciberseguretat específica sobre el sistema SEDA. Aquest informe complementa els resultats de l'*Informe de seguiment de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019* aprovat en 2022.

Com a resultat de la revisió efectuada de 44 controls detallats, cal concloure que el grau de control existent en la gestió dels controls generals de tecnologies de la informació relacionats amb la ciberseguretat del sistema SEDA aconsegueix un índex de maduresa del 67,2%. Tots els controls analitzats han de millorar per a aconseguir l'objectiu del 80% establit per l'Esquema Nacional de Seguretat i hi ha clares possibilitats de millora per a la protecció dels sistemes d'informació.

Contextualitzant els resultats obtinguts en aquesta auditoria en el marc de l'*Informe de síntesi de les auditories de ciberseguretat dels quinze majors ajuntaments i de les tres diputacions de la Comunitat Valenciana de l'exercici 2021*, podem constatar la posició relativa del nivell de maduresa general dels controls de ciberseguretat del sistema SEDA respecte a la mitjana dels controls bàsics de ciberseguretat dels 15 ajuntaments analitzats i amb l'Ajuntament de València.



Així mateix, durant la nostra revisió hem observat, com a part del procés d'obtenció de coneixement del sistema SEDA, que el sistema compleix els requisits funcionals i satisfà les necessitats operatives dels usuaris, i que s'ha realitzat una adequada gestió del

desenvolupament i desplegament del sistema SEDA per part dels responsables del projecte en l'Ajuntament i per part dels adjudicataris del projecte i de la seua direcció.

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar la gestió de la ciberseguretat del sistema SEDA. Entre aquestes aconsellem millorar la configuració de seguretat dels diferents entorns del sistema, finalitzar la licitació per a l'adquisició d'un sistema EDR per a la protecció dels dispositius finals d'usuari de l'Ajuntament, i ampliar el Pla de Contingència per al sistema SEDA de manera que reculla i formalitze la realització periòdica de proves de recuperació planificades per a tots els tipus de còpia existents.

Amb caràcter general continuen vigents les conclusions i les recomanacions realitzades en l'informe esmentat adés, la més important de les quals es refereix a la necessària actualització i aprovació de la Política de Seguretat de la Informació de l'Ajuntament

NOTA

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

Auditoria de ciberseguretat i dels controls generals de tecnologies de la informació del nou sistema SEDA de l'Ajuntament de València

Situació a 30 de setembre de 2023

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. INTRODUCCIÓ

Què és el sistema SEDA

La informació municipal de caràcter economicofinancer i comptable de l'Ajuntament de València s'ha gestionat fins a 2021 a través de diferents sistemes d'informació i aplicacions informàtiques, principalment a través del Sistema d'Informació Econòmic Municipal (SIEM), que era una aplicació desenvolupada pel mateix ajuntament, implantada l'any 1988, que des de llavors es va adaptar i evolucionà segons les necessitats de l'entitat. L'aplicació es mantenia íntegrament des del Servei de Tecnologies de la Informació i Comunicació de l'Ajuntament.

Aquest sistema s'ha substituït l'any 2022 per SEDA, que és el nou sistema d'informació i gestió economicofinancer de l'Ajuntament de València, que gestiona des de la fase d'elaboració del pressupost fins a la rendició d'informació als diferents intervinents en matèria economicofinancera, i té per objecte:

- Simplificar els processos unificant en un sistema integrat les deu aplicacions utilitzades fins ara per a la gestió econòmica, financera i comptable, que estaven tecnològicament obsoletes.

- Augmentar l'eficàcia i l'eficiència en el compliment de les obligacions legals respecte a tramitació, obtenció, remissió i publicació d'informació.

- Garantir la fiabilitat de la informació econòmica eliminant duplicitats i minimitzant errors, ja que el nou sistema ho facilita en basar-se en la dada única.

- Establir un sistema adaptat a les necessitats d'interoperabilitat que permeta desenvolupar una major coordinació entre els diferents nivells de l'Administració pública.

- Aportar més transparència i seguretat als processos de l'Ajuntament.

Des del punt de vista tècnic, SEDA utilitza com a plataforma tecnològica el producte S/4 HANA, que és la versió més actual del programari ERP (per les sigles en anglés, *enterprise resource planning*) de la companyia SAP, que s'ofereix en mode PaaS,[1] és a dir, "plataforma com a servei" des d'un núvol privat.

[1] PaaS és una de les modalitats de servei en el núvol. PaaS proporciona al client totes les capacitats, funcionalitats i serveis corresponents a processament, emmagatzematge, xarxes i sistema operatiu. Un núvol PaaS proporciona a l'entitat usuària la capacitat d'implementar aplicacions desenvolupades o adquirides per a la seua utilització posterior.

L'Ajuntament va adjudicar el contracte[2] per al desenvolupament i implantació de SEDA el 17 de gener de 2020. L'aplicació va entrar en funcionament l'1 de gener de 2022.

Figura 1. Dades rellevants del projecte

3.740.100 euros de cost total	**24 mesos de treball**
10 aplicacions substituïdes	**+400 usuaris afectats**
Data d'adjudicació del contracte 17/1/2020	**Data d'entrada en funcionament 1/1/2022**

Per què realitzem aquesta auditoria

L'article 6 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, inclou entre les seues funcions, a més de les referides al control extern de la gestió economicofinancera del sector públic valencià i dels seus comptes, aquelles que d'acord amb l'ordenament jurídic siguen convenients per a assegurar adequadament el compliment dels principis financers, de legalitat, d'eficàcia, d'economia i de transparència exigibles al sector públic, així com la sostenibilitat ambiental i la igualtat de gènere. D'altra banda, l'article 11 de la mateixa llei estableix que, en el desenvolupament de la seua funció fiscalitzadora, la Sindicatura de Comptes està facultada per a **verificar la seguretat i fiabilitat dels sistemes informàtics** que suporten la informació economicofinancera, comptable i de gestió.

El Pla Estratègic 2019-2022 de la Sindicatura de Comptes inclou la digitalització del sector públic valencià i la transformació digital de l'Administració com un dels quatre elements o tendències fonamentals[3] que ha de considerar la Sindicatura de Comptes en la seua activitat fiscalitzadora. Conseqüentment, en l'annex I d'aquest document es va incloure la transformació digital de l'Administració com a àrea prioritària d'actuació per a la Sindicatura.

[2] Expedient 04101/2019/58-SER. "Sist. Gestió Economicofinancer tecnologia SAP S/4 HANA (lot 1), Sist. Inform. Gestió RH Personal tecn. SAP HCM on HANA (lot 2) i 2 oficines tècniques impuls transf. digital - PMO (lots 3 i 4)."

[3] Vegeu l'apartat 2.4 del Pla Estratègic 2019-2022 de la Sindicatura de Comptes.

En l'*Informe de seguiment* [en 2022] *de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019*, aprovat el 15 de desembre de 2022 pel Consell de la Sindicatura, s'analitza la situació a 31/12/2021 dels controls bàsics de ciberseguretat (CBCS) de l'Ajuntament. En aquest informe es va incloure la revisió dels controls relacionats amb el sistema SEDA perquè en aquella data estava en la fase final d'implantació i es va indicar que, a causa de la seua importància per al control intern de l'Ajuntament i davant les ciberamenaces creixents, seria objecte d'una auditoria de ciberseguretat específica de més profunditat, els resultats de la qual es presenten en aquest informe.

Les raons per a fer aquesta auditoria sobre l'eficàcia dels controls de ciberseguretat relacionats amb SEDA són:

a) Els controls de ciberseguretat, bàsicament els controls generals de tecnologies de la informació (CGTI), han de garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les dades.

   Aquests controls tenen una gran importància, ja que la seua ineficàcia o mal funcionament impediria confiar en els controls sobre el processament de la informació (CPI) establits en SEDA. La gran complexitat tècnica de la plataforma tecnològica utilitzada aconsellava realitzar una auditoria en profunditat per a revisar que la seua configuració es l'adequada.

b) Gran increment dels ciberatacs al sector local.

   En els últims anys, les entitats locals s'han convertit en un objectiu preferent dels ciberdelinqüents, i creixen les amenaces i els atacs patits pels ajuntaments. Uns CGTI sòlids representen la defensa més eficaç davant d'aquestes ciberamenaces en un entorn d'administració electrònica avançada que se sustenta en sistemes d'informació cada vegada més complexos i intensament interconnectats. L'auditoria dels CGTI o controls de ciberseguretat proporciona confiança respecte de l'eficàcia de les ciberdefenses de l'ajuntament. En aquest sentit, aquesta auditoria complementa l'informe esmentat adés sobre els CBCS[4] de l'Ajuntament de València.

c) Obligacions legals.

   A més, els controls de seguretat de la informació, que són el nucli dels CGTI, són de compliment obligat d'acord amb la normativa d'aplicació, especialment l'Esquema Nacional de Seguretat (ENS).

Addicionalment, en el moment d'emetre aquest informe, la Sindicatura està fent una auditoria específica dels controls de processament de la informació en la gestió de la Tresoreria de l'Ajuntament, que es troben suportats pel sistema SEDA. Els resultats d'aquesta auditoria es publicaran en un informe independent.

[4] Els CBCS són un subconjunt dels CGTI.

Objectius de l'auditoria

Ateses les raons anteriors, els objectius de l'auditoria han sigut:

a) Conéixer l'entorn tecnològic dels sistemes que donen suport a SEDA i identificar els riscos principals relacionats amb la seguretat de la informació.

b) Identificar els CGTI existents per a mitigar els riscos anteriors i els que possibiliten el funcionament adequat dels CPI existents en SEDA.

c) Revisar i concloure sobre el disseny, implementació i l'eficàcia operativa dels CGTI existents en el sistema SEDA o que s'hi relacionen i sobre el grau de confiança que proporcionen, mesurat a través del seu índex de maduresa, per a:

- garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les transaccions i les dades, i
- servir de fonament per al bon funcionament dels CPI.

Abast

Aquesta auditoria s'ha centrat en l'anàlisi de la situació dels CGTI relacionats amb l'aplicació SEDA, que proporciona suport als processos de l'àrea econòmica, financera i comptable.

Hem seleccionat per a la revisió i avaluació els controls bàsics de ciberseguretat (CBCS), excepte el CBCS 1, "Inventari i control de dispositius físics", i el CBCS 8, "Compliment normatiu i governança de ciberseguretat", per ser de gestió general de l'ajuntament i independents de SEDA, i hem inclòs dos CGTI de gran importància per a la configuració de la seguretat de SEDA, els "Controls d'accés a usuaris" i els de "Desenvolupament d'aplicacions i gestió de canvis".

En total hem revisat 44 controls detallats, agrupats en els 8 controls principals assenyalats en el quadre 1, considerats rellevants per al procés economicofinancer.

El període revisat ha comprés des de l'1 de gener de 2022 fins al 30 de setembre de 2023, data a què es refereix la situació dels indicadors de l'índex de maduresa.

Metodologia

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

El contingut de les dues guies, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS, que és de compliment obligat per a tots els ens públics. Aquesta alineació facilita la realització de les auditories de ciberseguretat per part de la Sindicatura i coadjuva a la implantació de l'ENS en els ens auditats, ja que pràcticament tots els subcontrols o controls detallats que verifica la Sindicatura estan exigits per l'ENS.

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

Per a valorar la situació dels controls hem utilitzat el model de nivell de maduresa dels processos ja que, a més de ser un sistema àmpliament acceptat, permet establir objectius i realitzar comparacions entre entitats diferents i veure l'evolució al llarg del temps. La metodologia utilitzada està plenament alineada amb el que s'estableix en l'Esquema Nacional de Seguretat (ENS).

Encara que ho exigeix l'ENS, no hem obtingut evidència de la classificació de seguretat (alt, mitjà o baix) del sistema SEDA per part de l'Ajuntament. Als efectes d'aquest informe, hem considerat que li correspon una classificació de categoria de seguretat MITJANA, que és la més habitual en els sistemes que suporten processos de gestió administrativa i economicofinancers. El nivell de maduresa requerit per l'ENS per a aquest tipus de sistemes és el nivell 3 (N3), procés definit i un índex de maduresa del 80%.

Els resultats detallats obtinguts per a cada un dels CGTI revisats es mostren en el quadre 1.

Confidencialitat

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

2. CONCLUSIONS

Amb caràcter general continuen vigents les conclusions sobre els CBCS i les recomanacions realitzades en el nostre *Informe de seguiment* [en 2022] *de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019*.

Per la importància que té per a l'establiment d'una adequada ciberseguretat en el conjunt de l'Ajuntament, hem de destacar que a 30 de setembre de 2023 continuava pendent d'actualitzar i aprovar la política de seguretat de la informació.

En aquest apartat formulem les conclusions específiques relacionades amb la ciberseguretat i els CGTI del sistema SEDA resultat de l'auditoria realitzada.

L'índex de maduresa dels CGTI relacionats amb la ciberseguretat del sistema SEDA ha de millorar per a aconseguir l'objectiu establit per l'ENS.

Com a resultat de la revisió efectuada, cal concloure que el grau de control existent en la gestió dels CGTI del sistema SEDA revisats aconsegueix un **índex de maduresa del 67,2%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls en general es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment.

Després de la revisió de 44 subcontrols o controls detallats, agrupats en els 8 controls principals, agregant els resultats obtinguts segons la classificació inclosa en la GPF-OCEX 5330, "Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica", s'obtenen els resultats mostrats en el quadre 1.

Quadre 1. Índex de maduresa per àrees dels controls de ciberseguretat

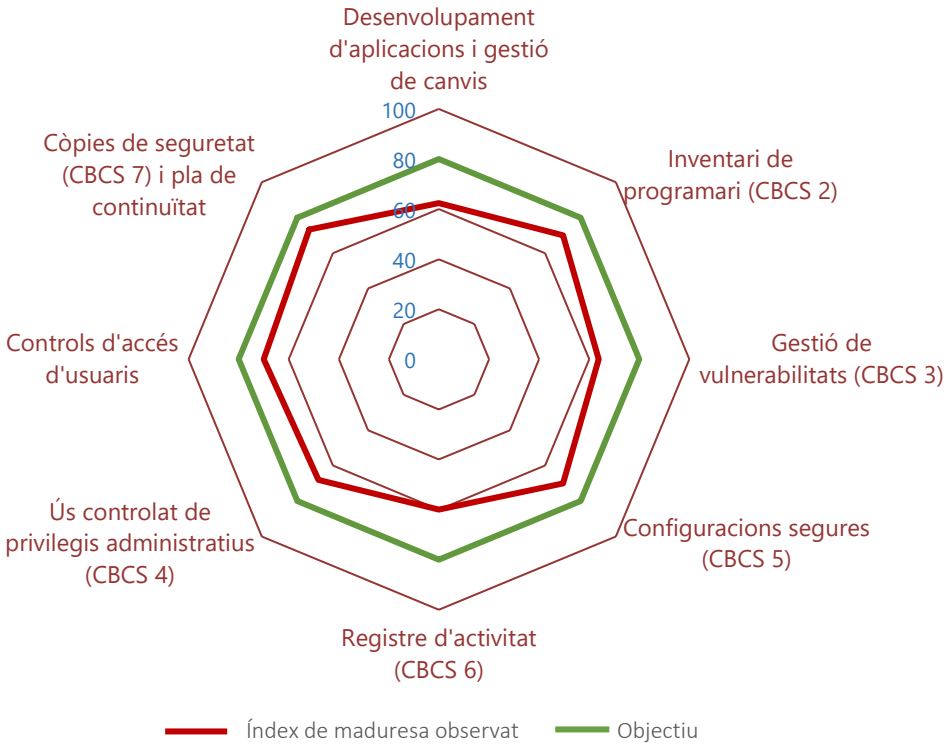
Àrees	Controls principals	Índex de maduresa
B. Canvis en aplicacions i sistemes	B2/B3 Desenvolupament d'aplicacions i gestió de canvis	62,4%
C. Operacions dels sistemes d'informació	C.1 Inventari de programari (CBCS 2)	70,0%
	C.2 Gestió de vulnerabilitats (CBCS 3)	63,8%
	C.3 Configuracions segures (CBCS 5)	70,0%
	C.4 Registre d'activitat (CBCS 6)	60,0%
D. Controls d'accés a dades i programes	D.1 Ús controlat de privilegis administratius (CBCS 4)	68,0%
	D2/D3/D4 Controls d'accés d'usuaris	70,0%
E. Continuïtat del servei	E.1 Còpies de seguretat de dades i sistemes (CBCS 7)	73,3%
	General	**67,2%**

En l'apèndix es comenta amb detall la situació observada d'aquests controls.

El nivell d'efectivitat en els controls analitzats ha de millorar, ja que cap aconsegueix el nivell del 80% objectiu i hi ha clares possibilitats de millora per a aconseguir el nivell de maduresa N3 requerit per l'ENS per a la protecció dels sistemes d'informació de nivell mitjà. En l'apartat 5 es realitzen les recomanacions pertinents amb aquesta finalitat.

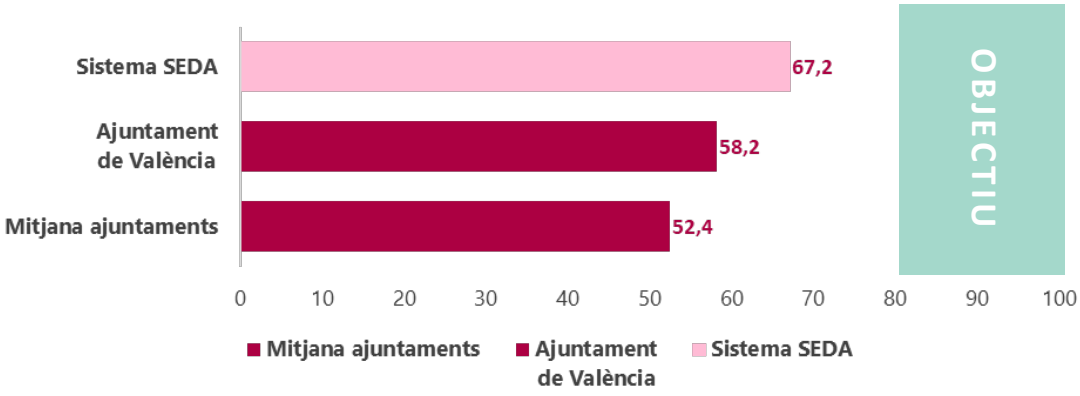
La situació observada dels controls queda reflectida en el gràfic 1.

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



Contextualitzant els resultats obtinguts en aquest treball en el marc de l'*Informe de síntesi de les auditories de ciberseguretat dels quinze majors ajuntaments i de les tres diputacions de la Comunitat Valenciana. Exercici 2021*, podem constatar (vegeu el gràfic 2) la posició relativa del nivell de maduresa general dels controls de ciberseguretat del sistema SEDA respecte a la mitjana dels controls bàsics de ciberseguretat a 31/12/2021 dels 15 ajuntaments analitzats i amb l'Ajuntament de València.

Gràfic 2. Índexs de maduresa comparats



S'ha realitzat una adequada gestió del projecte de desenvolupament i desplegament del sistema SEDA i el sistema compleix els requisits funcionals i satisfà les necessitats operatives dels usuaris.

Encara que revisar la gestió del projecte d'implantació de SEDA no ha format part dels objectius d'aquesta auditoria, durant la seua execució, com a part del procés d'obtenció de coneixement del sistema SEDA, hem constatat que aquesta gestió s'ha realitzat amb un bon nivell de competència per part dels responsables del projecte a l'Ajuntament i per part dels adjudicataris del projecte i de la seua direcció.

Hem verificat per mitjà d'entrevistes amb determinats responsables que:

- S'ha realitzat una aplicació adequada de les metodologies de gestió de projectes i de desenvolupament d'aplicacions.
- Hi ha hagut una elevada implicació dels responsables de projecte i el suport dels òrgans superiors de l'Ajuntament, factor clau per al desenvolupament i la implantació reeixida d'un projecte TI tan complex.
- S'ha efectuat una execució competent del projecte per part de l'adjudicatari i una adequada direcció independent d'aquest.
- S'ha fet una adequada gestió de requisits funcionals facilitant l'adaptació de l'eina a les necessitats operatives dels diferents serveis.

Aquesta gestió adequada del projecte ha tingut, com a conseqüències més destacables:

- El compliment dels objectius de projecte definits sobre la base dels requisits funcionals identificats.
- El compliment de terminis planificats per a la posada en operació del sistema sense excedir el pressupost.
- L'acceptació i adaptació per part dels usuaris finals a la nova aplicació i als nous processos de gestió associats.
- L'absència d'incidències rellevants que hagen minvat la capacitat operativa del sistema i la confiança de l'organització en la nova aplicació.

3. RESPONSABILITATS DELS ÒRGANS DE L'AJUNTAMENT

Els òrgans superiors de l'Ajuntament són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions. D'acord amb les seues competències, han de garantir que el funcionament de l'entitat resulte conforme amb les normes aplicables i que els controls interns proporcionen una garantia raonable que la informació, els serveis i els sistemes d'informació que els donen suport complisquen les propietats

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

Addicionalment a la responsabilitat sobre la seguretat dels sistemes d'informació, l'establiment i l'aplicació pràctica de les mesures de seguretat l'han d'assumir els òrgans i rols designats en les polítiques de seguretat de la informació aprovades per l'Ajuntament, principalment el Comité de Seguretat TIC i el responsable de seguretat.

D'altra banda, la responsable funcional de SEDA ha definit, durant les fases de desenvolupament i desplegament del sistema, els requisits per al seu desenvolupament, la validació de les proves funcionals realitzades, la tipologia d'usuaris i la seua assignació al personal de l'Ajuntament exercint funcions de responsable del servei i de la informació per a aquest sistema.

4. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

El nostre objectiu ha sigut obtindre una seguretat limitada i concloure sobre la situació dels controls generals de tecnologies de la informació revisats, proporcionar una avaluació sobre el seu disseny i implementació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control.

Per a això, hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura i recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica, com també que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CGTI revisats.

Ateses les especials característiques del treball realitzat sobre els sistemes d'informació, aquest l'ha efectuat la Unitat d'Auditoria de Sistemes d'Informació de la Sindicatura de Comptes (UASI), amb l'assistència d'una firma especialitzada.

Considerem que l'evidència d'auditoria obtinguda proporciona una base suficient i adequada per a fonamentar les nostres conclusions sobre l'estat dels CGTI relacionats amb el sistema SEDA, d'acord amb l'abast limitat que s'ha assenyalat.

Els procediments realitzats en una auditoria de seguretat limitada són reduïts en comparació amb els que es requereixen per a obtindre una seguretat raonable, però s'espera que el nivell de seguretat siga, d'acord amb el judici professional de l'auditor, significatiu per als destinataris de l'informe.

Com a part d'una auditoria de conformitat amb la normativa reguladora de l'activitat dels òrgans de control extern, apliquem el nostre judici professional i mantenim una actitud d'escepticisme professional durant tota l'auditoria. Així mateix, oferim propostes correctores a les deficiències trobades en el curs de l'auditoria, per a la qual cosa es

formulen les recomanacions pertinents que contribuïsquen a incrementar l'eficàcia del sistema de control intern i l'eficiència dels processos de gestió.

Ens comuniquem amb l'òrgan de govern de l'entitat en relació, entre altres qüestions, amb l'abast i el moment de realització de l'auditoria planificats i les constatacions significatives de l'auditoria, així com qualsevol altre aspecte significatiu que identifiquem en el transcurs de l'auditoria.

5. RECOMANACIONS

Amb caràcter general continuen sent aplicables les recomanacions realitzades en el nostre *Informe de seguiment* [en 2022] *de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019*.

Amb la finalitat d'ajudar a esmenar les deficiències identificades en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 2, en aquest apartat realitzem les recomanacions relacionades amb el sistema SEDA, dirigides al Comité de Seguretat TIC i a la resta de rols de seguretat designats o que es designen d'acord amb la política de seguretat de la informació de l'Ajuntament, que està pendent d'actualitzar-se.

Sobre el desenvolupament d'aplicacions i la gestió de canvis (B2/B3)

1. Aprovar formalment un procediment per a la gestió contínua de canvis en SEDA, que especifique els requisits següents:

   - Registre de totes les sol·licituds de canvi, inclosos els urgents a causa de necessitats sobrevingudes o per a la solució d'incidències i els originats des de l'equip tècnic o des dels responsables funcionals del servei.
   - Avaluació de les sol·licituds tenint en compte els riscos de seguretat.
   - Autorització dels canvis per part del personal responsable, abans que passen a producció.
   - Realització de proves, amb caràcter previ a la implantació del canvi i acceptació per part de l'usuari final i dels responsables funcionals corresponents.
   - Planificació de la posada en funcionament del canvi.
   - Millorar la gestió documental del procés i incloure tota la informació necessària.

Sobre l'inventari i control de programari autoritzat (C1/CBCS 2)

2. Elaborar i aprovar un procediment per a la gestió de components del sistema SEDA, que incloga les mesures actualment implantades:

   - L'inventari i control de components instal·lats en el sistema.

- La gestió de llicències.
- La gestió de versions dels diferents components a fi d'assegurar el suport del fabricant.
- La gestió d'interfícies i connexions amb elements externs al sistema i les mesures de seguretat aplicades a aquestes.

Sobre el procés continu d'identificació i solució de vulnerabilitats (C2/CBCS 3)

3. Elaborar i aprovar un procediment per a la identificació i resolució de vulnerabilitats del sistema SEDA, que incloga, a més de les mesures actualment implantades, la priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.

Sobre les configuracions segures del programari i maquinari (C3/CBCS 5)

4. Millorar la configuració de seguretat dels diferents entorns del sistema, producció, preproducció i desenvolupament.

5. Finalitzar la licitació per a l'adquisició d'un sistema EDR per a la protecció dels dispositius finals d'usuari (*endpoint*) de l'Ajuntament.

Sobre el registre d'activitat dels usuaris (C4/CBCS 6)

6. Elaborar i aprovar formalment un procediment per al tractament de registres d'activitat dels usuaris del sistema SEDA, que especifique, com a mínim, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs* (encara que aquest procés no és d'aplicació obligatòria segons l'ENS).

Sobre l'ús controlat de privilegis administratius (D1/CBCS 4)

7. Elaborar i aprovar un procediment que descriga la gestió dels usuaris que disposen de drets d'accés privilegiats sobre el sistema SEDA.

Sobre el control d'accés dels usuaris (D2/D3/D4)

8. Elaborar i aprovar un procediment de control d'accés per al sistema SEDA que descriga el control implantat en l'actualitat i incloga el detall necessari sobre la identificació i autenticació dels usuaris, la gestió i provisió de drets d'accés i la seua gestió continuada. També hauria d'analitzar-se la conveniència d'utilitzar eines automatitzades per a gestionar aquest procés, que actualment es realitza de manera manual.

Sobre la còpia de seguretat de dades i sistemes (E1/CBCS 7)

9. Ampliar el pla de contingència per al sistema SEDA de manera que reculla i formalitze la realització periòdica de proves de recuperació planificades per a tots els tipus de còpia existents.

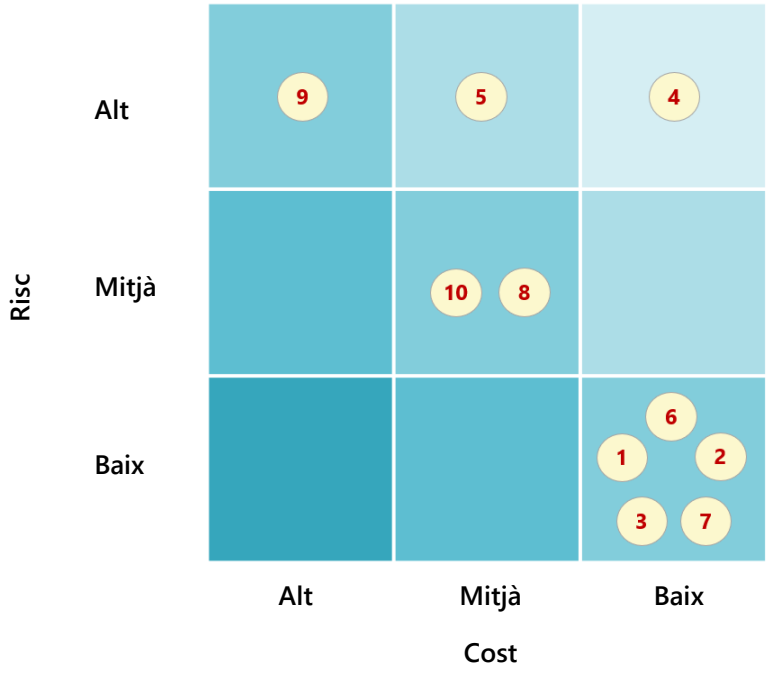
Sobre la disponibilitat dels sistemes

10. Elaborar i aprovar un pla de continuïtat de l'activitat corporatiu i d'aplicació en tot l'Ajuntament, que incloga l'anàlisi sobre elements crítics de negoci existent, l'estratègia de continuïtat, els plans particulars de contingència dels sistemes de l'Ajuntament (inclòs el pla de contingència del sistema SEDA) i l'execució planificada de proves periòdiques del pla. No obstant això, aquest procés no és d'aplicació obligatòria segons l'ENS.

Priorització de les recomanacions

A fi que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic 3 següent es mostra la classificació de les recomanacions segons els criteris combinats de risc potencial a mitigar i cost de la seua implantació.

Gràfic 3. Riscos que s'atenen i cost d'implantació de les recomanacions



APÈNDIX
Situació dels controls auditats

A continuació, es detallen les observacions i deficiències de control obtingudes en la nostra auditoria. En l'apartat 2 d'aquest informe s'han inclòs les conclusions més rellevants i en l'apartat 5, les recomanacions que deriven d'aquesta revisió.

Amb caràcter previ i per a facilitar la comprensió d'algunes observacions que segueixen, assenyalem que els agents que han intervingut en la gestió de l'aplicació SEDA són:

- Responsable funcional de l'Ajuntament: la Viceintervenció de Comptabilitat.
- Responsable tècnic de l'Ajuntament: el Servei de Tecnologies de la Informació i Comunicació.
- Desenvolupador del projecte SEDA i proveïdor del servei *cloud* en modalitat PaaS: l'adjudicatari del contracte de desenvolupament del sistema (lot 1).[5]
- Direcció del projecte: l'adjudicatari del lot 3 del contracte anterior.
- Manteniment del sistema SEDA: l'adjudicatari del contracte de manteniment del sistema.[6]

1. Desenvolupament d'aplicacions i gestió de canvis (B2/B3)

Objectiu de control

Disposar d'un procediment per al desenvolupament d'aplicacions i sistemes de manera que es tinguen en consideració els criteris de seguretat i assegure que els canvis realitzats es gestionen de manera metodològica i n'incloguen l'anàlisi, comunicació i registre.

Per què és important aquest control

Qualsevol canvi realitzat en els sistemes d'informació, si es fa de manera no planificada, pot suposar un risc per al funcionament correcte d'aquests sistemes o facilitar la realització de fraus. La implantació de noves aplicacions o la modificació de les existents sense aplicar els controls d'una bona metodologia podrien posar en risc l'estabilitat dels sistemes d'informació utilitzats en l'entitat.

És essencial en l'execució de les tasques de gestió de canvis i desenvolupament d'aplicacions l'aprovació de procediments que regulen com s'han de fer els canvis en components del sistema i la seua configuració. A més, han de designar-se els òrgans o persones responsables de realitzar i aprovar les diferents fases d'aquests canvis i assegurar que es fan les proves prèvies a la implantació dels canvis en els sistemes de gestió en ús.

[5] El contracte "Sist. Gestió Economicofinancer tecnologia SAP S/4 HANA (lot 1), Sist. Inform. Gestió RH Personal tecn. SAP HCM on HANA (lot 2) i 2 oficines tècniques impuls transf. digital - PMO (lots 3 i 4). Expedient 04101/2019/58-SER" es va adjudicar el 15 de maig de 2020 a l'empresa IECISA.

[6] El contracte "Servei de manteniment correctiu, evolutiu i adaptatiu del Sistema de Gestió Economicofinancer de l'Ajuntament de València, amb tecnologia SAP S/4 HANA (SEDA). Expedient 04101/2022/112-SER2" es va adjudicar el 9 de novembre de 2022 a l'empresa Inetum España, SA.

Situació del control

L'Ajuntament disposa d'una normativa, escrita i formalment aprovada, per a la realització de desenvolupaments a mesura en l'entorn SAP, que inclou una descripció detallada de la metodologia a utilitzar que inclou aspectes rellevants com l'assegurament de la qualitat de codi font.

L'acceptació dels desenvolupaments realitzats s'efectua a través de correu electrònic pel responsable del mòdul al qual està destinat el desenvolupament, i posteriorment per la responsable funcional de l'Ajuntament, i es documenta com a part del procés de gestió de canvis. Hem verificat per mitjà de mostreig sobre les ordres de transport registrades que, per a aquells canvis que per la seua naturalesa ho requereixen, se'n fan proves, però de manera general no es documenten.

Hem verificat que hi ha un control efectiu sobre la gestió de canvis, que és un procés correctament dissenyat i implantat i que, finalitzada la fase de posada en operació del sistema, s'aplica a la totalitat dels canvis efectuats. No obstant això, encara que hi ha procediments aprovats que aborden parcialment la gestió de canvis, no descriuen completament el control.

El control de canvis rep el suport de l'ús combinat d'eines de registre d'incidències corporatives, eines ofimàtiques específiques i subprocessos manuals. Les sol·licituds de canvi es registren i es processen en aquestes eines, que faciliten la seua revisió i aprovació per part dels responsables funcionals, inclosos els canvis urgents a causa de necessitats sobrevingudes o per a la solució d'incidències, que són registrats amb posterioritat a la resolució de la incidència.

Hem verificat que, per a determinats canvis registrats, la informació continguda en el registre és incompleta o imprecisa i, de manera general, no s'inclou informació sobre les proves realitzades ni l'aprovació prèvia al transport a producció.

Quant a capacitat per a l'execució dels canvis, hem realitzat proves per a identificar els usuaris que disposen de privilegis per a promoure canvis en l'entorn de producció i hem verificat que, durant la fase inicial de posada en explotació, hi havia un nombre excessiu d'usuaris amb aquesta capacitat, en una deficient aplicació del principi de mínim privilegi. No obstant això, aquesta deficiència de control s'ha esmenat una vegada finalitzada la fase inicial de posada en operació del sistema.

Es disposa d'entorns de desenvolupament i de preproducció separats del de producció. Aquests entorns s'han configurat considerant requisits de seguretat, i les rutes de transport entre aquests es troben adequadament configurades. A més, hem verificat que s'han aplicat configuracions de seguretat sobre modificació de paràmetres amb afecció als diferents entorns, encara que s'han identificat possibilitats de millora.

La valoració d'aquest control aconsegueix un **índex de maduresa del 62,4%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però els procediments no s'han formalitzat documentalment.

2. Inventari de programari (CBCS 2)

Objectiu de control

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

Per què és important aquest control

Mantindre un inventari actualitzat de programari és important, ja que permet conéixer què cal protegir.

Situació del control

L'Ajuntament ha establit un control efectiu per a la gestió dels mòduls de l'aplicació SEDA, les llicències associades i les interfícies autoritzades amb altres aplicacions. No obstant això, no es disposa d'un procediment escrit i aprovat que definisca les mesures de control implantades.

L'Ajuntament realitza, a través de l'adjudicatari del contracte de manteniment del sistema, la gestió i revisió dels mòduls desplegats en SEDA a través d'una eina propietària proporcionada pel fabricant del sistema. Es fa periòdicament la revisió dels components instal·lats i es verifica que els mòduls desplegats en el sistema es troben en versions suportades pel fabricant. En aquestes revisions s'inclou tant la verificació dels components del sistema com dels sistemes operatius, bases de dades i altres sistemes subsidiaris.

A més, l'Ajuntament efectua una gestió correcta i exhaustiva del llicenciament de l'aplicació. Aquesta gestió es fa de manera conjunta per l'adjudicatari del manteniment del sistema i la responsable funcional de l'aplicació a l'Ajuntament, i inclou la gestió d'usuaris del sistema, les seues funcions, els permisos necessaris per a la seua execució i les llicències necessàries. Aquesta gestió contínua del llicenciament permet contindre i limitar els costos associats a l'explotació del sistema, i proporciona els recursos únicament als empleats que per les seues funcions necessiten fer ús de l'aplicació.

Hem verificat que hi ha un control efectiu sobre les comunicacions del sistema amb elements externs. L'Ajuntament disposa d'un inventari actualitzat de les interfícies del sistema SEDA amb sistemes externs, inventari que es troba correctament actualitzat i mantingut. A més, hem comprovat que s'han aplicat mesures de seguretat específiques per a la protecció d'aquestes interfícies, particularment les que requereixen l'accés a carpetes del sistema, incloent-hi una correcta gestió dels usuaris i els seus privilegis d'accés.

A més, per a les comunicacions entre sistemes SAP, hem verificat que hi ha un inventari de connexions per a l'intercanvi de dades i ens han indicat que la totalitat de connexions existents es troben gestionades i en ús.

Aquest control aconsegueix un **índex de maduresa del 70,0%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però els procediments no s'han formalitzat documentalment.

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

Objectiu de control

Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.

Per què és important aquest control

La finalitat d'aquest control és conéixer i eliminar debilitats tècniques que puguen haver-hi en els sistemes d'informació de l'entitat i reduir la probabilitat que els sistemes siguen vulnerables.

Situació del control

Hem analitzat la gestió de les vulnerabilitats del sistema SEDA i hem observat que s'han implantat mesures per a la seua identificació i resolució, en un procés de gestió manual però efectiu.

No obstant això, encara que hi ha una norma interna que aborda parcialment la gestió de pedaços, no té el detall necessari i no es disposa d'un procediment específic, escrit i formalment aprovat que detalle les accions per a la gestió de riscos i vulnerabilitats del sistema SEDA actualment implantades.

La identificació de vulnerabilitats de l'aplicació la realitza l'adjudicatari del manteniment del sistema i es basa en l'anàlisi de notes i avisos de seguretat emesos pel fabricant del sistema. En cas d'identificar vulnerabilitats que puguen afectar el sistema SEDA, s'informa els responsables funcional i tècnic de l'Ajuntament per a validar i programar les accions pertinents, i es fan accions per a la resolució de totes. Aquest procés és extensiu tant a la aplicació com a les bases de dades i els sistemes operatius que la suporten. La seua gestió és manual però efectiva, i no s'utilitzen eines específiques per a la gestió de vulnerabilitats i de les tasques correctives.

Hem verificat que l'adjudicatari del manteniment del sistema aplica els pedaços que el fabricant recomana per al seu manteniment, com a part del procés de gestió de vulnerabilitats implantat i que es troba recollit i detallat en la documentació contractual que regula el servei de manteniment i suport del sistema SEDA.

Els sistemes físics i de comunicacions de la infraestructura que suporten l'aplicació són mantinguts pel proveïdor del servei *cloud*, incloent-hi la gestió de vulnerabilitats. Disposa de diversos certificats de seguretat que proporcionen una seguretat raonable que les vulnerabilitats d'aquests sistemes són gestionades adequadament i està especificat en les clàusules del contracte.

La valoració global del control dona un **índex de maduresa del 63,8%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però els procediments no s'han formalitzat documentalment.

4. Configuracions segures (CBCS 5)

Objectiu de control

Establir una configuració base segura del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors, i gestionar-la activament, utilitzant un procés de gestió de canvis i configuracions rigorós, per a previndre que els atacants exploten serveis i configuracions vulnerables.

Per què és important aquest control

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

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

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

Situació del control

L'Ajuntament disposa del document "Disseny de seguretat lògica i física", que recull les normes, bones pràctiques, nomenclatures i procediments referents a la seguretat lògica i física. Aquest document detalla aspectes clau per a la configuració segura del sistema SEDA.

Hem verificat determinades configuracions crítiques del sistema i hem confirmat que, en general, s'aplica el que s'especifica en el document de seguretat, incloent-hi l'eliminació de comptes per defecte. No obstant això, hi ha determinades mancances que s'han d'esmenar.

La configuració de seguretat dels diferents entorns és correcta, encara que hi ha possibilitats de millora, tal com s'ha especificat en el control "Desenvolupament d'aplicacions i gestió de canvis".

Per a la configuració dels sistemes operatius que suporten l'aplicació i les bases de dades del sistema, l'adjudicatari del manteniment disposa de guies corporatives que detallen configuracions específiques de seguretat i que s'actualitzen periòdicament.

Hem revisat l'estat de la licitació per a adquisició d'un sistema EDR per a protecció de la xarxa i dispositius finals d'usuari i ens han indicat que no s'han fet avanços respecte a la situació reportada en l'*Informe de seguiment* [en 2022] *de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament de València de l'any 2019*. Ens han indicat que s'han habilitat nous mecanismes dinàmics de contractació i s'ha previst utilitzar-los per al subministrament del sistema EDR, sobre el qual s'han realitzat proves de concepte amb diferents fabricadors i s'han definit requisits per a l'elaboració dels plecs tècnics.

La valoració global del control dona un **índex de maduresa del 70,0%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits.

5. Registre d'activitat dels usuaris (CBCS 6)

Objectiu de control

Desenvolupar processos i utilitzar eines per a recollir, gestionar i analitzar els registres d'activitat (*logs*) d'esdeveniments que puguen ajudar a detectar, entendre o recuperar-se d'un atac.

Per què és important aquest control

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

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

Situació del control

Encara que el sistema SEDA permet configurar l'emmagatzematge de *logs* d'auditoria i la gestió del període d'emmagatzematge, l'Ajuntament no disposa de cap procediment

aprovat que reculla els paràmetres de recol·lecció de *logs*, que determine el període d'emmagatzematge, ni les anàlisis que s'han de realitzar.

Hem verificat que el *log* d'auditoria es troba habilitat en els servidors de l'aplicació, i que hi ha configuracions per a assegurar un emmagatzematge mínim de 30 dies per als registres d'activitat. A més, aquest període de retenció es troba estés per les còpies de seguretat de dades i sistema que es fan. No obstant això, aquest període no ha sigut formalment definit, ni establit sobre la base de criteris funcionals.

L'Ajuntament no ha implantat un sistema de revisió sobre el *log* d'auditoria amb l'objectiu d'identificar accions no autoritzades realitzades pels usuaris i únicament es fan revisions en cas d'incident.

A més, no s'han integrat els *logs* del sistema SEDA en el SIEM corporatiu ni en un altre sistema de correlació d'esdeveniments, a fi d'identificar comportaments anòmals en la xarxa i sistemes corporatius.

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

6. Ús controlat de privilegis administratius (CBCS 4)

Objectiu de control

Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'assignació i ús de privilegis administratius en els sistemes d'informació.

Per què és important aquest control

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

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

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

Situació del control

L'Ajuntament no disposa d'un inventari formal de gestió de comptes d'administració del sistema SEDA. A més, no existeix un procediment per a la gestió d'aquests comptes.

Hem verificat que els usuaris que disposen de drets d'administració sobre el sistema formen part íntegrament de l'equip d'operadors i desenvolupadors de l'adjudicatari del manteniment. Aquests usuaris no realitzen una explotació funcional de l'aplicació ni es troben implicats en cap dels processos de gestió de l'Ajuntament.

L'autenticació d'usuaris amb privilegis d'administració del sistema SEDA es fa per mitjà de l'ús de contrasenyes associades als comptes d'usuari, de la mateixa manera que es fa per a la resta dels usuaris. Els requisits d'autenticació per mitjà de contrasenya es troben adequadament establits en el procediment de configuració de la seguretat, que està formalment aprovat, i hem verificat que el sistema es troba configurat considerant els criteris establits en aquest document.

Hem identificat al conjunt dels usuaris que disposen de perfils SAP_ALL que proporcionen drets crítics sobre el sistema. El conjunt d'aquests drets proporciona un accés complet a les funcions i dades del sistema i ha de ser restringit a un ús d'emergència, i limitar-ne l'assignació a comptes d'usuaris utilitzats únicament per a la resolució de problemes que ho requerisquen. Durant la fase de posada en operació de l'aplicació, aquest conjunt estava constituït per un total de 29 usuaris; es tracta d'un nombre d'usuaris elevat, i això suposa una deficiència greu de control pels riscos que representa. Aquesta situació s'ha esmenat una vegada superada la fase de posada en operació del sistema.

Sobre l'auditoria i control de les accions dels usuaris amb drets crítics sobre el sistema, encara que hi ha usuaris amb els privilegis adequats per a verificar les entrades al sistema i les transaccions i programes executats, no hem pogut verificar que hi haja un procés establit per a la revisió periòdica de les seues accions.

Quant al control d'accés a la base de dades del sistema, hem verificat que es troba adequadament implementat ja que només els usuaris administradors disposen d'accés privilegiat.

Hem verificat que per als comptes per defecte s'ha modificat la contrasenya o bé no existeixen en tots els entorns, i es considera adequada la seua implementació.

La valoració global del control suposa un **índex de maduresa del 68,0%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però els procediments no s'han formalitzat documentalment.

7. Controls d'accés d'usuaris (D2/D3/D4)

Objectiu de control

Disposar de mecanismes que permeten la identificació segura dels usuaris, gestionar i limitar el seu accés als recursos dels sistemes i gestionar els seus privilegis per a fer una correcta provisió de drets d'accés.

Per què és important aquest control

Establir mecanismes d'identificació a tots els usuaris que accedeixen als sistemes o aplicacions de les entitats és l'única manera de conéixer qui rep determinats drets d'accés o qui ha realitzat accions concretes.

Per a accedir als diferents sistemes o aplicacions, els usuaris han d'utilitzar els seus identificadors singulars i existir, a més, mecanismes que permeten validar la seua identitat.

Sense un procés adequat de gestió de drets d'accés, els sistemes o aplicacions poden albergar usuaris amb majors privilegis dels que requereixen les seues funcions. Una gestió adequada d'altes, baixes i modificació d'usuaris permet a les organitzacions mantindre un inventari actualitzat d'usuaris, de manera que únicament els usuaris actuals accedeixen als sistemes i aplicacions als quals s'ha autoritzat l'accés.

Situació del control

Hem analitzat els controls d'accés dels usuaris al sistema SEDA i hem verificat que existeix un control efectiu, però que aquest control no es troba previst en un procediment formalment aprovat.

La identificació d'usuaris del sistema SEDA es fa per mitjà d'usuaris locals i la seua autenticació per mitjà de l'ús de contrasenyes associades a aquests comptes. Els requisits d'autenticació a través de contrasenya es troben establits en el procediment de configuració de la seguretat, que està formalment aprovat. A més, hem verificat que el sistema es troba configurat considerant els criteris establits en aquest document.

La gestió de drets d'accés dels usuaris als diferents mòduls del sistema es realitza de manera manual, atés que no es disposa d'eines automatitzades. No obstant això, el procés establit, la responsabilitat del qual es troba compartida entre els responsables del sistema a l'Ajuntament i l'empresa adjudicatària del manteniment, es troba adequadament dissenyat i implantat.

Hem verificat que el procés d'assignació de drets d'accessos és efectiu i es troba ben executat. Els privilegis dels usuaris del sistema, aplicats per mitjà de rols i objectes d'autorització, es corresponen amb aquells que han sigut assignats pels responsables, amb una aplicació correcta del principi de mínim privilegi. Els responsables del sistema SEDA a l'Ajuntament han modelitzat els llocs de treball i han establit tipus i subtipus d'usuaris i una descripció detallada de les seues atribucions.

A més, hem fet una revisió dels rols assignats al grup complet d'usuaris del departament de Tresoreria de l'Ajuntament i hem verificat que l'assignació de drets és adequada i es correspon amb la realitzada pels responsables.

La gestió de baixes o modificació d'usuaris és efectiva i s'executa correctament, i la seua gestió és particularment exhaustiva. Es realitza de manera parcialment manual per part dels responsables del sistema a l'Ajuntament, que mantenen una comunicació constant amb els responsables dels diferents serveis, que informen de tots els canvis produïts en els equips de treball. Hem verificat per mitjà de mostreig que, per als usuaris del sistema que cessen o modifiquen les seues funcions a l'Ajuntament, es fan les modificacions necessàries en els seus perfils.

Per al control dels accessos des d'internet, fora de la xarxa de l'Ajuntament, addicionalment a l'ús d'usuari i contrasenya, s'utilitza una connexió VPN corporativa que disposa de doble factor d'autenticació que es troba en fase de desplegament en el moment de realització de l'auditoria.

En síntesi, la valoració global del control aconsegueix un **índex de maduresa del 70,0%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però els procediments no s'han formalitzat documentalment.

8. Còpia de seguretat de dades i sistemes (CBCS 7)

Objectiu de control

Utilitzar processos i eines per a realitzar còpies de seguretat de la informació crítica amb una metodologia que permeta la seua recuperació en temps oportú.

Per què és important aquest control

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

Els danys de ciberatacs o les conseqüències dels incidents no provocats intencionadament es poden mitigar si es disposa de còpia de seguretat de les dades afectades.

Situació del control

L'Ajuntament ha implantat un procés per a realitzar còpies de seguretat que es troba recollit en el pla de contingència per al sistema SEDA, que està formalment aprovat pels responsables del projecte.

El control té el suport de l'ús de dues eines de còpia, una per a la còpia de l'aplicació i una altra per a la còpia de la base de dades, i les dues eines són administrades i gestionades

per l'adjudicatari del manteniment, que proporciona el servei *cloud* que alberga els equips i sistemes que suporten aquest procés.

Hem verificat que el procés de còpies de seguretat establit està correctament dissenyat i implementat i és efectiu. L'adjudicatari del manteniment reporta sobre el resultat de les còpies realitzades com a part d'un informe d'estat del sistema i del servei que és elaborat i remés diàriament, i revisat pels responsables de l'Ajuntament.

Però no es fan proves de restauració planificades i la seua realització no es troba recollida en el pla de contingència. No obstant això, sí que es fan recuperacions de còpies a causa d'incidències i pèrdues de dades.

Durant la fase de posada en producció del projecte es van realitzar proves de recuperació de les bases de dades que componen el sistema, adequadament planificades, executades i documentades.

Les còpies es troben duplicades en dues ubicacions, la qual cosa proporciona redundància de dades i redueix els riscos de pèrdua d'informació en cas d'incident. La ubicació secundària únicament emmagatzema còpies de seguretat, i no alberga sistemes per a l'execució de l'aplicació.

Les còpies de seguretat únicament són accessibles des de les eines de còpia, que estan instal·lades i operades per l'adjudicatari del manteniment. No és possible accedir a les còpies de seguretat des de les xarxes de l'Ajuntament, la qual cosa impedeix que, en cas d'incident de seguretat, les còpies de seguretat es vegen afectades. A més, les còpies de seguretat de bases de dades es troben xifrades i únicament poden ser recuperades pels sistemes des dels quals es va realitzar la còpia original, la qual cosa evita l'exfiltració de dades en cas d'incident.

La valoració global del control existent sobre les còpies de seguretat és que l'Ajuntament aconsegueix un **índex de maduresa del 73,3%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu;*** és a dir , els controls es realitzen, però hi ha controls parcialment establits.

9. Pla de continuïtat

Objectiu de control

Disposar d'un pla amb mesures que permeten el restabliment dels serveis en cas de pertorbació greu dels sistemes.

Per què és important aquest control

Per a protegir i mantindre en funcionament els serveis que es presten per l'entitat és necessari identificar aquells que són més importants, els sistemes que els suporten i planificar adequadament la seua recuperació en cas d'incident greu que afecte el seu funcionament.

En aquesta planificació s'ha d'incloure la priorització dels serveis a recuperar, els objectius de temps de recuperació i punt de recuperació, així com els mitjans materials i personals a utilitzar en cas de ser necessària aquesta recuperació de sistemes. També és necessari planificar la realització de proves periòdiques d'aquests plans.

Situació del control

L'Ajuntament no disposa d'un pla de continuïtat de l'activitat que siga aplicable a tota l'entitat, ni d'un pla específic per al sistema SEDA.

Encara que aquest requisit únicament és aplicable per a sistemes categoritzats com de nivell alt en l'ENS, i no hem valorat el seu índex de maduresa, l'hem revisat per considerar que l'existència d'un pla de continuïtat és una pràctica recomanable per a organismes amb alt impacte en la ciutadania.

Sí que es disposa d'un document d'anàlisi d'impacte en el negoci, element clau en l'elaboració d'un pla de continuïtat de l'activitat. Aquest document identifica els serveis crítics de l'entitat i la seua relació amb els sistemes i actius físics que suporten aquests serveis. I detalla, per a cada un dels sistemes que suporten els serveis essencials, els requisits quant a disponibilitat dels sistemes, incloent-hi els temps RTO (objectiu de temps de recuperació) i RPO (objectiu de punt de recuperació) per a cada un.

A més, tal com s'ha indicat anteriorment, es disposa d'un pla de contingència per al sistema SEDA, que és una part fonamental per a l'elaboració del pla de continuïtat de l'activitat. Aquest pla de contingència detalla la solució d'alta disponibilitat desplegada per a bases de dades HANA, la solució d'alta disponibilitat en la capa de virtualització per als servidors d'aplicació i la configuració de còpies de seguretat per al sistema SEDA.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

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

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

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

Ciberseguretat: Totes les activitats necessàries per a la protecció de les xarxes i sistemes d'informació, dels usuaris d'aquests sistemes i d'altres persones afectades per les ciberamenaces (Reglament (UE) 2019/881).

EDR:[7] Un sistema EDR, sigla en anglés d'*endpoint detection and response*, és un sistema de protecció dels equips i infraestructures de l'empresa. Combina l'antivirus tradicional juntament amb eines de monitoratge i intel·ligència artificial per a oferir una resposta ràpida i eficient davant dels riscos i les amenaces més complexes.

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

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i han de descriure *a*) l'ús correcte d'equips, serveis i instal·lacions; *b*) el que es considerarà ús indegut, i *c*) la

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

responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat ha d'estar a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, ha d'estar disponible en la intranet corporativa de l'entitat a través d'una adreça URL. La normativa de seguretat de cada entitat deriva i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desenvolupament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

Pla de contingència: Definició d'accions a realitzar, recursos a utilitzar i personal a ocupar en cas de produir-se un esdeveniment intencionat o accidental que inutilitze o degrade els recursos informàtics o de transmissió de dades d'una organització.

Pla de continuïtat: Pla l'objectiu del qual és mantindre la funcionalitat d'una organització a un nivell mínim acceptable durant una contingència. Defineix els passos que es requereixen per al restabliment dels processos de negoci després d'una interrupció.

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

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

RPO: L'objectiu de punt de recuperació (*recovery point objective*, RPO) és la quantitat màxima d'informació que es pot perdre quan el servei és restaurat després d'una interrupció. L'RPO s'expressa com una longitud de temps abans de la fallada.

RTO: L'objectiu de temps de recuperació (*recovery time objective*, RTO) és la màxima quantitat de temps tolerable que un ordinador, sistema, xarxa o aplicació pot estar inactiu després d'una fallada o un desastre. L'RTO es mesura en segons, minuts, hores o dies, i és una consideració important en la planificació de recuperació en cas de desastre.

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir amb la interventora de Comptabilitat i Pressupostos, amb la cap del Servei de Comptabilitat i amb el cap del Servei de Tecnologies de la Informació i Comunicacions, perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*c* del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'informe d'auditoria corresponent a 2023, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

Transcorregut aquest termini no s'han rebut al·legacions.

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*h* del seu Reglament de Règim Interior i del Programa Anual d'Actuació de 2023 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 22 de novembre de 2023, va aprovar aquest informe d'auditoria.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Auditoria ciberseguretat SEDA_val - SEFYCU 4633123

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

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

Codi Segur de Verificació (CSV): KUAC HZX4 YEDN QAMQ 3YKH

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

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

Empremta del document per a la persona firmant	Text de la firma	Dades addicionals de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrònica - ACCV - 29/11/2023 8:53 VICENT CUCARELLA TORMO