SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

AUDITORIA DE CIBERSEGURETAT I DELS CONTROLS GENERALS DE TECNOLOGIES DE LA INFORMACIÓ DE L'APLICACIÓ ORION LOGIS

Exercici 2022

RESUM

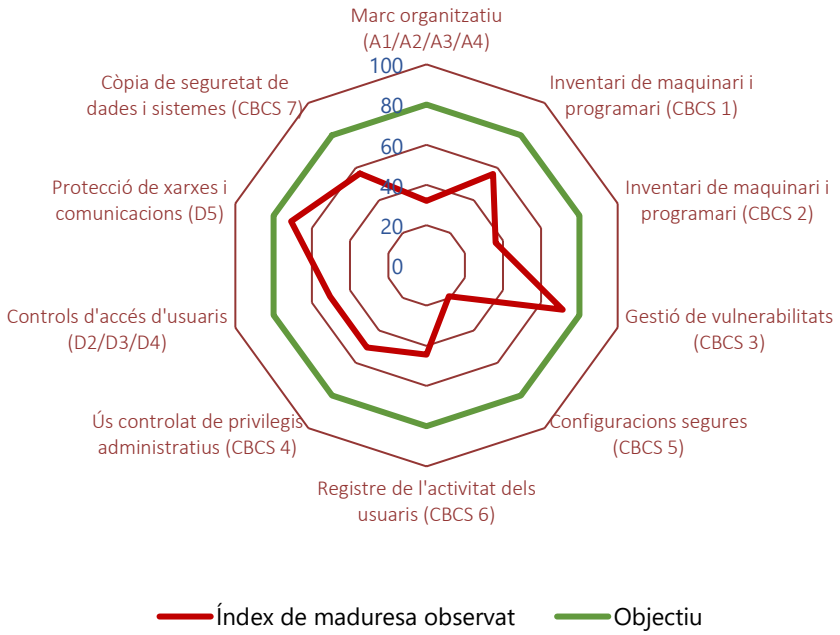
La Sindicatura de Comptes, de manera simultània a la realització de l'**auditoria del control intern i dels sistemes d'informació de les compres sanitàries**, ha dut a terme una auditoria de ciberseguretat i dels controls generals de tecnologies de la informació (CGTI) relacionats amb l'aplicació ORION LOGIS, que proporciona suport als processos de compres de béns i serveis de la Conselleria de Sanitat.

Les principals **conclusions** han sigut:

- L'índex de maduresa dels CGTI relacionats amb ORION LOGIS és molt deficient i no aporta un nivell de confiança raonable per a garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les transaccions i les dades.

  Hem arribat a la conclusió que l'índex de maduresa conjunt d'aquests controls és del 48,7%, inferior al 80% requerit pel Reial Decret 311/2022, pel qual es regula l'Esquema Nacional de Seguretat, que requereix a les administracions amb la categoria de seguretat dels sistemes revisats aquest nivell mínim de maduresa.

  El detall del nivell de maduresa de cada grup de controls es mostra en el gràfic següent.



- La situació dels CGTI representa, per tant, un nivell de risc sobre la seguretat de la informació inacceptable i les deficiències existents no permeten confiar en el bon funcionament dels controls de processament d'informació (CPI), per la qual cosa l'entitat ha d'adoptar mesures per a reconduir la situació.

- La Conselleria de Sanitat no té establida una adequada governança de la ciberseguretat, que és l'element clau per a arribar a l'objectiu de garantir la seguretat i bon funcionament dels sistemes d'informació, i això és responsabilitat dels òrgans superiors de la Conselleria. A més, s'ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

- Les deficiències en els controls assenyalades en l'informe especial de 2016 persisteixen.

La revisió del **compliment normatiu** en matèria de seguretat de la informació ha posat de manifest les incidències següents:

- Encara que hi ha treballs en marxa relacionats amb el compliment de l'ENS, l'índex actual de compliment és molt baix, i hi ha els incompliments significatius que es detallen en el nostre informe.

- No s'ha elaborat el pla d'adequació a l'Esquema Nacional d'Interoperabilitat.

- Hi ha aspectes pendents de compliment de la normativa de protecció de dades personals.

En l'informe realitzem diverses **recomanacions** tendents a esmenar les deficiències observades en matèria de ciberseguretat, entre les quals destaquem las relacionades amb la millora de la capacitat de recuperació dels sistemes davant possibles desastres o ciberatacs per mitjà de sistemes d'alta disponibilitat redundats en diferents ubicacions i una adequada gestió de les còpies de seguretat.

NOTA

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

Auditoria de ciberseguretat i dels controls generals de tecnologies de la informació de l'aplicació ORION LOGIS

Exercici 2022

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. INTRODUCCIÓ

Antecedents

En termes pressupostaris, les obligacions reconegudes en 2022 del capítol 2, "Compres de béns corrents i despeses de funcionament", de la Conselleria de Sanitat Universal i Salut Pública (CSUSP), a partir del 25 de juliol de 2023 denominada Conselleria de Sanitat, ascendeixen a 2.732,4 milions d'euros. És a dir, representen un 74,8% dels 3.655,7 milions d'euros corresponents a aquest capítol en el conjunt del Compte de l'Administració.

La gestió de les compres de la Conselleria es realitza de forma descentralitzada, a través dels centres gestors de compres en els 24 departaments sanitaris en què es divideix el territori de la Comunitat Valenciana, i també en els serveis centrals. Aquesta gestió està suportada per l'aplicació informàtica ORION LOGIS. En l'apèndix 1 es detallen les característiques i funcionalitats d'aquesta aplicació.

Les dades següents relacionades amb l'aplicació ORION LOGIS posen en relleu la seua importància en la gestió de la Conselleria i la seua evolució des dels anteriors informes especials realitzats per la Sindicatura:

Quadre 1. Dades bàsiques d'ORION LOGIS

	2013	2016	2022
Nombre d'usuaris	6.372	7.472	8.737
Nombre de factures	415.011	531.244	730.841
Nombre d'articles	90.635	124.935	170.445
Nombre de proveïdors	4.675	5.595	6.237

La Conselleria de Sanitat i els seus departaments de salut han tramitat en 2022 a través de l'aplicació ORION LOGIS factures corresponents tant a despeses pressupostàries del capítol 2 com a despeses comptabilitzades en els capítols 4, "Transferències corrents", i 6, "Inversions reals".

Per què realitzem aquesta auditoria

Les raons per a realitzar una auditoria sobre l'eficàcia dels controls existents en els sistemes d'informació que suporten la gestió de les compres sanitàries són:

a) Aquestes despeses són una àrea molt significativa en el conjunt del Compte de l'Administració de la Generalitat, ja que representen el 74,8% de les obligacions reconegudes del pressupost del capítol 2.

b) Els controls generals de tecnologies de la informació (**CGTI**) han de garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les dades. A més,

la ineficàcia o mal funcionament impediria confiar en els controls de processament de la informació (**CPI**).

c) Els CPI han de garantir la completesa, exactitud, validesa i legalitat de les transaccions relacionades amb la compra de béns i serveis sanitaris, que es gestionen amb l'aplicació ORION LOGIS. Els resultats de l'auditoria d'aquests controls es recullen en l'informe d'A*uditoria del control intern i dels sistemes d'informació de les compres sanitàries* de l'exercici 2022 de la Sindicatura de Comptes.

d) Els CGTI són molt importants, ja que en els últims anys el sector de la salut s'ha convertit en un objectiu preferent dels ciberdelinqüents, i uns sòlids CGTI representen la defensa més eficaç davant de les ciberamenaces en un entorn que se sustenta en sistemes d'informació intensament interconnectats.[1]

e) Finalment, els controls de seguretat de la informació, bàsicament els CGTI, són de compliment obligat en virtut de diferent normativa, especialment per l'Esquema Nacional de Seguretat (ENS).

Objectius de l'auditoria

L'objectiu d'aquesta auditoria ha sigut verificar el grau d'eficàcia dels CGTI, que garanteixen el correcte funcionament de l'aplicació ORION LOGIS, i ha inclòs les tasques següents:

- Conéixer l'entorn tecnològic dels sistemes que donen suport a ORION LOGIS, identificant els riscos principals relacionats amb la seguretat de la informació i els controls existents per a mitigar-los.

- Revisar i concloure sobre el disseny, implementació i l'eficàcia operativa dels CGTI existents en, o relacionats amb, el sistema ORION LOGIS i si, en conseqüència, aporten un nivell de confiança raonable per a:

  a) garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les transaccions i les dades, i

  b) servir de fonament per al bon funcionament dels CPI.

- Revisar el compliment de la normativa sobre seguretat dels sistemes d'informació.

[1] En un informe recent, ENISA Threat Landscape: Health Sector, de juliol de 2023, de l'European Union Agency for Cybersecurity, es destaca que durant 2021-2022 el sector sanitari europeu ha hagut de d'afrontar un creixent nombre de ciberatacs, generalitzats, i assenyala que Espanya és el segon país d'Europa quant a ciberincidents de seguretat comunicats.

Abast

Aquesta auditoria s'ha centrat en l'anàlisi de la situació dels CGTI relacionats amb l'aplicació ORION LOGIS, que proporciona suport als processos de compres de béns i serveis de la Conselleria de Sanitat.

Encara que molts dels CGTI afecten el conjunt de sistemes d'informació, la revisió s'ha focalitzat en els controls relacionats amb:

1. l'aplicació ORION LOGIS,
2. la base de dades subjacent,
3. els sistemes operatius instal·lats en els sistemes que integren l'aplicació de gestió (servidor web, servidor d'aplicació, servidor de base de dades).

A més, per la seua importància per al bon funcionament dels sistemes d'informació i la ciberseguretat, s'han analitzat els següents tipus d'elements:

4. elements de la xarxa de comunicacions (punt d'accés a xarxa de gestió),
5. elements de seguretat (tallafoc, servidors d'autenticació).

En total hem revisat 51 controls detallats, agrupats en els 10 controls principals assenyalats en el quadre 2, considerats rellevants per al procés de gestió de compres.

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

Metodologia

La metodologia utilitzada en aquesta auditoria està basada en les guies pràctiques de fiscalització GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat", i GPF-OCEX 5330, "Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica", que formen part del *Manual de fiscalització* de la Sindicatura de Comptes i que poden consultar-se en el nostre web.

Avaluem la situació dels controls utilitzant el model de nivell de maduresa dels processos, ja que, a més de ser un sistema àmpliament acceptat, permet establir objectius i realitzar comparacions entre entitats diferents i veure l'evolució al llarg del temps. La metodologia utilitzada està plenament alineada amb el que s'estableix per l'ENS.

Per a major detall sobre la metodologia utilitzada ens remetem a l'apèndix 2.

Confidencialitat

Atés que la informació utilitzada en l'auditoria té un caràcter sensible i pot afectar la seguretat dels sistemes d'informació, els resultats detallats de cada un dels controls revisats

només es comuniquen amb caràcter confidencial als responsables de la Conselleria de Sanitat perquè puguen adoptar les mesures correctores que consideren necessàries. En aquest informe els resultats es mostren de manera sintètica.

2. CONCLUSIONS SOBRE ELS CONTROLS GENERALS DE TECNOLOGIES DE LA INFORMACIÓ

L'índex de maduresa dels CGTI relacionats amb ORION LOGIS és molt deficient i no aporta un nivell de confiança raonable per a garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les transaccions i les dades.

Com a resultat del treball realitzat cal concloure que el grau de control existent en la gestió dels CGTI revisats relacionats amb ORION LOGIS aconsegueix un **índex de maduresa mitjà del 48,7%**, que es correspon amb un nivell de maduresa ***N1, inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la seua gestió no està correctament organitzada.

Aquest resultat està molt allunyat del nivell exigit per l'ENS per als sistemes amb una categoria de seguretat MITJANA,[2] que és el nivell N3 i un índex de maduresa del 80%.

La situació dels CGTI representa, per tant, un nivell de risc sobre la seguretat de la informació inacceptable i les deficiències existents no permeten confiar en el bon funcionament dels CPI, per la qual cosa l'entitat ha d'adoptar mesures per a reconduir la situació.

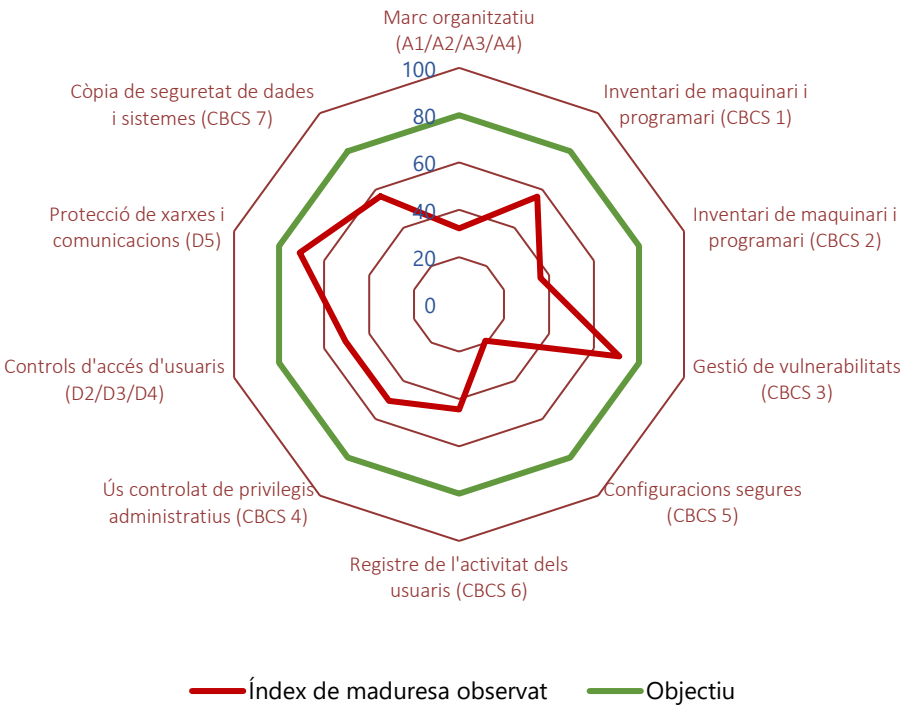
En total hem revisat 51 controls detallats, agrupats en els 10 controls principals que es mostren en el quadre 2 i es visualitzen en el gràfic 1, relacionats amb l'aplicació ORION LOGIS. En aquests estan inclosos els huit controls bàsics de ciberseguretat de la metodologia de la Sindicatura basada en la GPF-OCEX 5313 (vegeu apèndix 2).

[2] Encara que ho exigeix l'ENS, no hem obtingut evidència de la classificació del sistema ORION LOGIS per part de la Conselleria (alt, mitjà o baix). Hem considerat que ha de classificar-se com de categoria de seguretat MITJANA, que és la més habitual en els sistemes que suporten processos de gestió administrativa.

Quadre 2. Índex de maduresa dels CGTI

Àrea		Control	Índex de maduresa	Nivell de maduresa
A. Marc organitzatiu	A1/A2/ A3/A4	Marc organitzatiu i governança de la ciberseguretat (CBCS 8)	32,1%	N1
C. Operacions dels sistemes d'informació	C1H	Inventari de maquinari (CBCS 1)	56,3%	N2
	C1S	Inventari de programari (CBCS 2)	36,2%	N1
	C2	Gestió de vulnerabilitats (CBCS 3)	71,3%	N2
	C3	Configuracions segures (CBCS 5)	19,0%	N1
	C4	Registre de l'activitat dels usuaris (CBCS 6)	44,4%	N1
D. Controls d'accés a dades i programes	D1	Ús controlat de privilegis administratius (CBCS 4)	50,4%	N2
	D2/D3/D4	Controls d'accés a usuaris	50,4%	N2
	D5	Protecció de xarxes i comunicacions	70,8%	N2
E. Continuïtat del servei	E1	Còpia de seguretat de dades i sistemes (CBCS 7)	56,5%	N2
General			48,7%	N1

Gràfic 1. Índex de maduresa dels CGTI revisats



La majoria dels grups de controls tenen un índex de maduresa molt allunyat del requerit per l'ENS (80,0% i N3) i del que s'espera d'un sòlid sistema de control intern, la qual cosa representa un risc significatiu per a la seguretat dels sistemes d'informació de la Conselleria.

Les deficiències significatives en els CGTI observades es comenten amb detall en l'apèndix 3. En l'apartat 6 es realitzen les recomanacions pertinents per a reconduir la situació i aconseguir els nivells exigits per l'ENS per a la protecció dels sistemes d'informació.

El període revisat ha sigut l'exercici 2022 i el treball de camp ha finalitzat al setembre de 2023, data a la qual es refereix la situació dels controls.

La Conselleria de Sanitat no té establida una adequada governança de la ciberseguretat. A més, s'ha de reforçar el suport en forma de recursos humans i pressupostaris dedicats a la seguretat de la informació.

Els òrgans superiors de la Conselleria són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació que garantisca la ciberresiliència de l'entitat.

Si bé hem pogut verificar l'existència d'un cert nivell de compromís i conscienciació amb la ciberseguretat, hi ha mancances rellevants detallades en l'apèndix 3 que impedeixen que la governança puga considerar-se efectiva.

En aquest sentit, considerem que la governança de la ciberseguretat implementada pels òrgans de direcció de la Conselleria és clarament insuficient per a garantir el compliment de la normativa relacionada amb la seguretat de la informació i perquè els controls relacionats amb les TI aconseguisquen els nivells de maduresa requerits per l'ENS.

És necessari, per tant, solucionar de manera urgent les mancances identificades, que tenen un impacte negatiu en el nivell de seguretat de la informació de la Conselleria, i atendre les recomanacions efectuades en aquest informe.

Les deficiències de control intern assenyalades en l'informe especial de 2016 persisteixen.

Atesa la importància que té aquesta àrea en la fiscalització del Compte de l'Administració de la Generalitat, la Sindicatura va realitzar en 2013 i en 2016 sengles informes d'auditoria especials sobre els sistemes d'informació en els quals es va analitzar l'eficàcia dels CGTI del sistema d'informació que suporta ORION LOGIS, que poden consultar-se en la pàgina web de la Sindicatura. En aquest informe s'ha realitzat un seguiment de les deficiències de CGTI incloses en l'últim d'aquests informes.

La primera conclusió general sobre la ineficàcia dels CGTI és bàsicament coincident amb les dels informes de 2013 i 2016. Com es veurà després, la majoria de les recomanacions efectuades en l'informe de 2016 no han sigut ateses.

A causa de l'elevada rellevància de les debilitats de control observades, els òrgans de govern de la Conselleria han de comprometre's de manera clara i decidida a esmenar-les.

No se'ns ha facilitat a temps l'emplenament d'un qüestionari sol·licitat sobre els controls revisats, la qual cosa ha dificultat l'anàlisi de les evidències obtingudes, encara que considerem que no afecta les conclusions del nostre treball. Tampoc se'ns ha facilitat la informació sol·licitada sobre el personal de la Subdirecció General de Sistemes d'Informació per a la Salut.

3. CONCLUSIONS SOBRE EL COMPLIMENT DE LA NORMATIVA EN MATÈRIA DE SEGURETAT DE LA INFORMACIÓ

Encara que hi ha treballs en marxa relacionats amb el compliment de l'ENS, l'índex actual de compliment és molt baix, i hi ha els incompliments significatius que s'assenyalen a continuació.

La Conselleria de Sanitat està subjecta al compliment del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat, substituït en 2022 pel Reial Decret 311/2022, de 8 de maig.

L'Ordre 9/2012, de 10 de juliol, de la Conselleria de Sanitat, estableix l'organització de la seguretat de la informació. D'acord amb aquesta norma, la Conselleria, amb el suport de la Direcció General de les Tecnologies de la Informació i de la Comunicació (DGTIC), és responsable de la seguretat dels seus sistemes d'informació.

La Conselleria es troba treballant en un projecte d'adequació dels diferents departaments de salut a l'ENS. Per mitjà d'un contracte s'han elaborat perfils de compliment específics per a facilitar la implantació de l'ENS en els departaments.

A data d'aquest informe, un dels organismes pertanyents a la Conselleria ja ha obtingut el certificat de conformitat per a categoria "BÀSICA" i es preveu l'aplicació d'aquest perfil de compliment a altres organismes.

La Conselleria ha presentat l'informe sobre l'estat de la seguretat dels sistemes d'informació de 2022 al Centre Criptològic Nacional (CCN), d'acord amb el que es preveu en la Instrucció Tècnica de Seguretat regulada per la Resolució de 7 d'octubre de 2016 de la Secretaria d'Estat d'Administracions Públiques.

Encara que s'han realitzat determinades accions per a donar compliment a l'ENS, durant el treball realitzat s'han posat de manifest els incompliments significatius següents:

- No s'ha nomenat el responsable del servei dels sistemes d'informació previst en l'ENS i en el Decret 130/2012 del Consell.
- El comité de seguretat de la informació de la Conselleria de Sanitat, que és un element essencial de la governança de la ciberseguretat, no té un funcionament efectiu, ja que només s'ha reunit una vegada en 2022.
- Alguns rols de seguretat establits en l'Ordre 9/2012 es defineixen sobre la base de normativa de protecció de dades que ja no es troba en vigor.
- No s'han nomenat tots els rols de seguretat dels elements descentralitzats de l'organització previstos en l'Ordre 9/2012.
- No s'ha aprovat la classificació de seguretat dels seus sistemes d'informació, ni la declaració d'aplicabilitat que requereix l'article 28 de l'ENS.
- No s'han realitzat les auditories previstes en l'article 31 de l'ENS ni, en conseqüència, s'han publicat en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat esmentada abans.

D'altra banda, l'índex de maduresa dels CGTI vist en l'apartat anterior, del 48,7%, reflecteix el baix grau de compliment de les mesures de seguretat establides amb caràcter obligatori per l'ENS. Aquesta norma requereix per als sistemes d'informació de nivell mitjà un índex de maduresa *N3, procés definit*, que exigeix una puntuació mínima del 80,0%.

No s'ha elaborat el pla d'adequació a l'Esquema Nacional d'Interoperabilitat (ENI).

No s'ha elaborat el pla d'adequació a l'ENI que exigeix el Reial Decret 4/2010. ORION LOGIS no està adaptada a la generació d'expedients de conformitat amb l'ENI.

Hi ha aspectes pendents de compliment de la normativa de protecció de dades personals.

La Conselleria té publicada en el seu web la relació d'activitats de tractament.

El delegat de protecció de dades (DPD) nomenat per la Generalitat té competències sobre l'activitat de la Conselleria de Sanitat. No obstant això, no s'ha cobert un lloc de treball existent en el departament del DPD per a atendre les necessitats de la Conselleria de Sanitat.

Durant el treball de camp, hem observat deficiències relacionades amb la protecció de dades personals, com l'enviament d'informació amb aquest tipus de dades sense xifrar i per mitjà de canals no segurs.

No s'han realitzat auditories de protecció de dades personals.

4. RESPONSABILITAT DELS ÒRGANS SUPERIORS I DE DIRECCIÓ DE LA CONSELLERIA DE SANITAT EN RELACIÓ AMB ELS CONTROLS DE SEGURETAT

La gestió de les aplicacions i els sistemes informàtics que suporten la gestió de les compres de béns i serveis per a les institucions sanitàries corresponia en 2022 a la Direcció General de Planificació, Eficiència Tecnològica i Atenció al Pacient, dependent de la Secretaria Autonòmica d'Eficiència i Tecnologia Sanitària, en la qual s'integra la Subdirecció General de Sistemes d'Informació per a la Salut (SDGSIS).

Des del 25 de juliol de 2023, data d'entrada en vigor del Decret 112/2023, de 25 de juliol, del Consell, s'estableix com a òrgan responsable la Direcció General d'Informació Sanitària, Qualitat i Avaluació, enquadrada en la Secretaria Autonòmica de Planificació, Informació i Transformació Digital de la Conselleria de Sanitat.

Els principals responsables en matèria de seguretat de la informació, segons l'ENS i segons l'Ordre 9/2012, de 10 de juliol, de la Conselleria de Sanitat, per la qual estableix l'organització de la seguretat de la informació, són els següents:

- Responsable de la informació: el conseller de Sanitat.
- Comité de Seguretat de la Informació, la composició del qual s'estableix en l'article 10 de l'Ordre 9/2012.
- Responsable del Servei, que no ha sigut formalment nomenat. L'article 12 de l'Ordre 9/2012 atribueix les seues funcions als responsables funcionals. En compres sanitàries corresponia aquesta responsabilitat a la Subdirecció General de Contractació i Central de Compres.
- Responsable de seguretat: la persona responsable de l'Oficina de Seguretat de la Informació nomenada pel conseller.
- Responsable del sistema, que no ha sigut formalment nomenat. L'Ordre 3/2022, de la Conselleria de Sanitat i Salut Pública, per la qual es desplega el Decret 185/2020, del Consell, d'aprovació del Reglament Orgànic i Funcional de la Conselleria, atribuïa les seues funcions al cap del Servei d'Infraestructures de Tecnologies de la Informació i la Comunicació.

5. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

El nostre objectiu és obtindre una seguretat limitada i concloure sobre la situació dels controls generals de tecnologies de la informació revisats de la Conselleria de Sanitat, proporcionant una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a l'esmena de les deficiències observades i a la millora dels procediments de control.

Ens hem centrat, principalment, en l'anàlisi de la situació dels CGTI relacionats amb l'aplicació ORION LOGIS de gestió de compres, si bé hi ha aspectes que són d'aplicació general a tots els sistemes de la Conselleria.

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, recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. En particular, hem seguit la metodologia establida 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". Aquests principis exigeixen que complim els requeriments d'ètica, així com que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CGTI revisats.

Ateses les característiques especials del treball a realitzar sobre els sistemes d'informació, aquest l'ha efectuat la Unitat d'Auditoria de Sistemes d'Informació de la Sindicatura de Comptes (UASI) en coordinació amb l'equip d'auditoria que fiscalitza el Compte de l'Administració de la Generalitat, que ha emés un informe especial sobre el control intern en la gestió de compres sanitàries.

Considerem que l'evidència d'auditoria obtinguda proporciona una base suficient i adequada per a fonamentar les nostres conclusions sobre l'estat dels CGTI revisats, 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.

També s'ha efectuat un seguiment de les deficiències de control intern i de les recomanacions realitzades en l'informe *Auditoria dels controls generals de tecnologies de la informació de l'aplicació ORION LOGIS* de l'exercici 2016.

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.

6. RECOMANACIONS PER A ESMENAR LES DEFICIÈNCIES EN ELS CGTI I MESURES A ADOPTAR PER AL COMPLIMENT DE LA LEGALITAT

Per a esmenar les deficiències identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 2 anterior, formulem les recomanacions que segueixen. Els òrgans de direcció de la Conselleria de Sanitat hauran de dedicar els esforços i recursos necessaris per a esmenar aquestes deficiències.

També s'assenyalen les mesures que han d'adoptar-se per al compliment de la legalitat.

Recomanacions dirigides a la Secretaria Autonòmica de Planificació, Informació i Transformació Digital

Aquestes recomanacions són aplicables a tots els sistemes d'informació de la Conselleria, no sols a ORION LOGIS.

Sobre l'inventari de maquinari

1. Recomanem actualitzar el procediment existent per a l'inventari de maquinari de manera que, a més de les accions i controls actualment implantats, incloga la identificació del responsable de cada actiu, les altes, baixes i actualitzacions de dispositius en l'inventari, les revisions periòdiques del maquinari i les mesures implantades per a impedir l'accés a la xarxa de dispositius no autoritzats i el seu abast, així com els controls sobre les memòries USB.

Sobre l'inventari de programari

2. Recomanem elaborar i implantar un procediment de gestió de tot el programari instal·lat en els sistemes de la Conselleria. Haurà d'incloure l'autorització de les instal·lacions, la llista del programari autoritzat (llista blanca), les mesures tècniques que impedisquen l'execució del no autoritzat, revisions periòdiques i la manera de documentar aquestes revisions, un pla de manteniment que considere de manera integral el procés de gestió del suport de tot el programari utilitzat i la manera d'identificar i actualitzar tots els sistemes que estan fora del període de suport.

Sobre la gestió de vulnerabilitats

3. Recomanem actualitzar i aprovar formalment el procediment per a la identificació i resolució de vulnerabilitats. Ha d'incloure totes les accions dutes a terme pels diferents departaments de l'SDGSIS. A més, ha de preveure la seua gestió proactiva, incloent-hi tant una anàlisi prèvia a l'entrada en producció dels sistemes com la identificació de vulnerabilitats per mitjà de l'ús d'eines d'escaneig o proves de penetració.

Sobre configuracions segures de maquinari i programari

4. Recomanem aprovar i implantar un procediment de configuració segura o fortificació i la gestió contínua dels sistemes que considere els principis de la seguretat per defecte i mínim privilegi. Aquest procediment ha d'incloure la gestió de canvis en els sistemes i el monitoratge i revisió periòdica dels canvis no autoritzats. També ha d'abordar la utilització de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies de seguretat STIC de les sèries 400, 500 i 600 del CCN.

Sobre registre de l'activitat dels usuaris

5. Recomanem aprovar formalment i implantar un procediment per al tractament dels registres d'auditoria d'activitat dels usuaris que incloga, com a mínim, els sistemes afectats, la informació que s'ha d'emmagatzemar, el període de retenció, els mecanismes de protecció, la gestió de drets d'accés als registres i la revisió d'aquesta activitat. Per a la seua aplicació efectiva, s'hauria d'implantar alguna eina analítica de correlació de registres, que permeta la detecció de comportaments anòmals i detecció d'esdeveniments de seguretat sobre la base de la informació proporcionada pel conjunt de sistemes de la Conselleria.

Sobre l'ús controlat de privilegis administratius

6. Aprovar formalment un procediment de gestió d'usuaris amb privilegis d'administració en tots els sistemes d'informació de la Conselleria, que incloga la seua regulació detallada, i que preveja:

    - l'inventari de comptes administratius i la seua revisió periòdica,
    - la desahabilitació o l'eliminació dels comptes no utilitzats que no siguen necessaris,
    - l'eliminació de tots els usuaris no nominatius i
    - la política d'autenticació amb els reforços previstos en l'ENS.

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

Sobre la gestió dels accessos dels usuaris

7. Elaborar i aprovar un procediment de gestió d'usuaris per a tots els sistemes de la Conselleria en què es regule la tramitació de les altes, baixes i modificació dels usuaris dels sistemes d'informació i el procediment per a aprovar aquests usuaris i per a comunicar-lo a l'SDGSIS. En aquest procediment ha de quedar establit les persones que han d'aprovar les altes, baixes i modificació d'aquests usuaris, així com un procés de revisió periòdic dels usuaris que garantisca el principi d'autorització i mínim privilegi (articles 17 i 20 de l'ENS).

Aquesta revisió ha d'incloure el personal d'empreses subcontractades i la revisió de la vigència dels contractes laborals en aquestes empreses.

El procediment hauria d'incloure l'obligació, per part del departament de personal o dels departaments funcionals, de la comunicació de les baixes de personal o canvis de centre i/o responsabilitats als responsables dels sistemes d'informació encarregats d'aplicar les altes i modificacions d'usuaris.

8. Elaborar i aprovar un procediment de seguretat que regule la forma de creació d'identificadors d'usuaris dels sistemes i els paràmetres d'autenticació per a aquests identificadors en cada sistema.

   El procediment hauria de desenvolupar els paràmetres de seguretat en l'autenticació i aplicar-los a tots els usuaris i sistemes, de manera que les contrasenyes incloguen un bon nivell de complexitat, caducitat, bloquejos davant intents fallits, d'acord amb les bones pràctiques i l'ENS. Per als sistemes de nivell mitjà i alt haurien d'establir-se els reforços en l'autenticació exigits per l'ENS.

Sobre la protecció de les xarxes i comunicacions

9. Aprovar un procediment i enfortir els mecanismes de control de la seguretat en els dispositius que es connecten per VPN i no són gestionats per la Conselleria, de manera que únicament puguen connectar-se si compten amb el nivell de seguretat adequat. També recomanem deshabilitar les connexions VPN innecessàries o no utilitzades durant un període determinat i realitzar un seguiment de la gestió realitzada per part dels departaments de salut sobre eixes connexions no utilitzades.

Sobre les còpies de seguretat i la continuïtat del servei

10. Actualitzar el procediment per a la gestió de còpies de seguretat de dades i sistemes, que preveja tots els requisits exigits per l'ENS.

11. Implementar sistemes d'alta disponibilitat en els sistemes crítics gestionats per la Conselleria amb un nivell addicional de protecció d'aquests sistemes, amb còpies en temps real en diferents ubicacions que estiguen prou separades físicament per a mitigar els riscos en cas de catàstrofes.

12. Recomanem que el pla de continuïtat s'aprove pel màxim nivell directiu de la Conselleria. El pla ha de definir concretament aspectes com les ubicacions o el maquinari alternatiu a utilitzar en cas d'incident greu, així com terminis de recuperació realistes.

Recomanacions sobre la governança de la seguretat de la informació i l'ENS, dirigides als òrgans superiors de la Conselleria

13. Els òrgans superiors de la Conselleria han d'adoptar amb urgència les mesures necessàries per a implantar una adequada governança sobre les tecnologies de la informació i la ciberseguretat, concordes amb el que es disposa per l'ENS i amb la

política de seguretat de la informació de la Generalitat, establida en el Decret 66/2012 del Consell, i resoldre els incompliments assenyalats en l'apartat 3 de l'Informe.

Aquestes mesures han de basar-se en un lideratge efectiu per part dels òrgans superiors de la Conselleria de Sanitat que proporcione les directrius i els recursos econòmics i personals necessaris per a la seua implantació efectiva. Inclourien entre altres qüestions:

- La Conselleria ha d'elaborar un pla d'adequació a l'ENS, implantar les mesures incloses en aquest pla i realitzar les auditories de seguretat legalment obligatòries.

- Actualitzar l'Ordre 9/2012, de 10 de juliol, per la qual s'estableix l'organització de la seguretat de la informació de la Conselleria per a adaptar-la a l'actual ENS, així com eliminar i/o actualitzar les referències a la normativa que ja no estiga en vigor.

- Desenvolupar la política de seguretat de la Generalitat per mitjà de normes i procediments de seguretat degudament aprovats, tal com requereix l'ENS, específics per a l'àmbit de la Conselleria. Aquestes normes i procediments haurien de comunicar-se als responsables d'aplicar-los i estar disponibles en algun repositori actualitzat i accessible per a aquests responsables. Això inclou actualitzar i aprovar els procediments ja existents.

- Elaborar i aprovar un pla estratègic per als sistemes d'informació de la Conselleria que s'integre en la planificació general de les TIC de la Generalitat i que garantisca l'existència d'uns sistemes d'informació orientats a la consecució dels objectius de la Conselleria. Aquesta planificació estratègica ha de concretar-se anualment en plans de projectes que al seu torn han de comptar amb el pressupost anual i/o pluriennal necessari per a dur-los a terme. S'ha d'assegurar la disponibilitat dels mitjans personals necessaris per a executar-los adequadament.

- Desenvolupar i aprovar un pla de formació sobre seguretat de la informació per al personal de la Conselleria, sense perjudici que es puguen aprofitar recursos de la Generalitat per a desenvolupar-lo. La Conselleria ha de realitzar el seguiment del grau d'execució d'aquests plans.

Sobre la normativa de protecció de dades personals, dirigida al responsable de la informació i del seu tractament[3]

14. Recomanem sol·licitar la designació d'un subdelegat del delegat de protecció de dades de la Generalitat per a l'àmbit de la Conselleria de Sanitat, realitzar periòdicament auditories de protecció de dades dels sistemes que manegen informació de caràcter

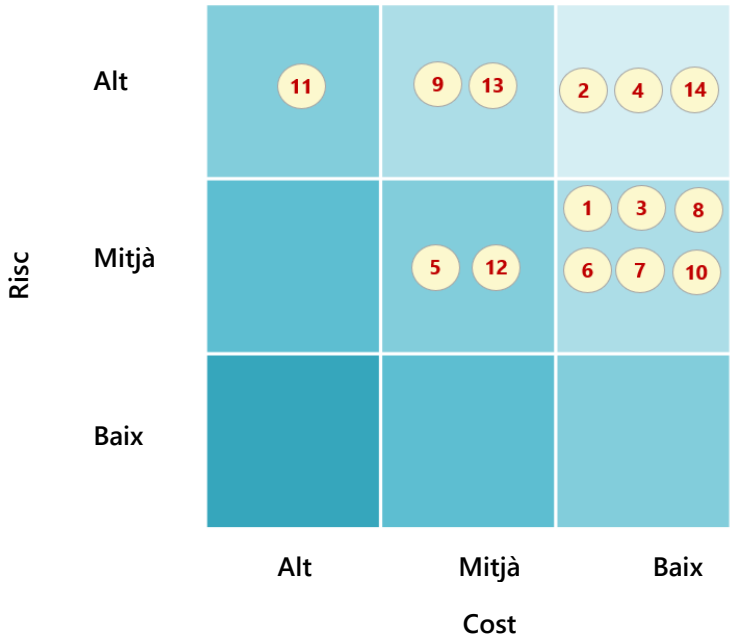
[3] L'article 7 de l'Ordre 9/2012, de 10 de juliol, de la Conselleria de Sanitat, atribueix al conseller les funcions de responsable de la informació i dels tractaments de dades personals, així com el nomenament d'altres responsables (funcionals i de seguretat) que han de participar en la implementació de les mesures de protecció de les dades personals.

personal i arbitrar canals segurs per a la transmissió de dades personals entre els departaments de la Conselleria.

Priorització de les recomanacions

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

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



Seguiment de recomanacions procedents d'informes d'auditoria anteriors

La Conselleria no ha aportat a la Sindicatura la informació sol·licitada de manera reiterada sobre les mesures adoptades en relació amb les recomanacions sobre CGTI incloses en l'informe de l'exercici 2016. La valoració sobre el grau d'implantació d'aquestes recomanacions s'ha realitzat a partir de l'evidència obtinguda de les nostres observacions i converses amb personal de la Conselleria, a la data de la nostra revisió (setembre de 2023).

No s'inclouen en el quadre següent les relatives als controls de processament de la informació l'anàlisi de les quals s'ha realitzat en l'informe especial de compres sanitàries. En aquest quadre, per a cada recomanació, consten els comentaris relatius a la seua situació a final de setembre de 2023 i la categorització corresponent segons la guia pràctica de fiscalització dels òrgans de control extern GPF-OCEX 1735, "Les recomanacions i el seu seguiment" (vegeu apèndix 2), així com els efectes en aquest informe.

Tal com es mostra en el quadre següent, de les 8 recomanacions realitzades en l'informe de 2016, 5 no s'han atés i 3 només s'han atés parcialment.

Quadre 3. Seguiment de recomanacions

		Recomanacions d'informes anteriors	Informe de l'exercici	Estat de la recomanació	Conseqüència en l'informe
MARC ORGANITZATIU	1	La Conselleria ha de realitzar la corresponent auditoria de la LOPD amb caràcter biennal, d'acord amb el que s'estableix en l'RLOPD. Addicionalment, a partir del 25 de maig de 2018 serà aplicable el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de dades personals. Aquest reglament inclou diferències significatives respecte a la regulació actual espanyola. Per aquest motiu, es recomana a la Conselleria iniciar un procés d'adequació a aquest reglament a fi de garantir-ne el compliment en els terminis establits.	2013, 2016	**No aplicada** *L'RGPD atribueix el principi de responsabilitat proactiva al responsable del tractament de dades personals i altres obligacions sobre aquests tractaments. Són necessàries actuacions addicionals per al compliment estricte de la normativa de protecció de dades.*	S'actualitza la redacció. (Vegeu recomanació núm. 14)
	2	La Conselleria ha d'elaborar un pla d'adequació a l'ENS, implantar les mesures incloses en aquest pla i realitzar les auditories de seguretat legalment obligatòries.	2013, 2016	**No aplicada** *No s'ha modificat la situació respecte a l'informe anterior.*	Es manté la redacció. (Vegeu recomanació núm. 13)
OPERACIONS	3	La Conselleria ha de preparar i licitar els contractes de suport a totes les aplicacions corporatives de forma planificada i en terminis suficients, de manera que es garantisca el seu adequat manteniment i el compliment de la normativa de contractació.	2016	**No aplicada** *No s'ha modificat la situació respecte a l'informe anterior.*	S'actualitza la redacció. (Vegeu recomanació núm. 2)

		Recomanacions d'informes anteriors	Informe de l'exercici	Estat de la recomanació	Conseqüència en l'informe
CONTROLS D'ACCÉS A DADES I PROGRAMES	**4**	Recomanem que s'aplique el procediment de gestió d'usuaris i de permisos. Així mateix, haurien de realitzar-se revisions periòdiques dels usuaris autoritzats, de manera que es garantisca que només tenen accés a l'aplicació els usuaris que ho necessiten sobre la base de les tasques assignades. Ha de conservar-se la documentació acreditativa de les revisions realitzades, dels resultats i de les accions dutes a terme.	2013, 2016	**Aplicada parcialment** *Hem obtingut evidència que es realitzen revisions periòdiques d'usuaris en ORION LOGIS, però no es realitza un seguiment sobre l'esmena de les incidències resultants de les revisions.*	S'actualitza la redacció. (Vegeu recomanació núm. 7)
	5	Recomanem que es modifiquen les polítiques d'autenticació (contrasenyes) per a tots els sistemes i adaptar-les a paràmetres rigorosos de qualitat i renovació (complexitat mínima, canvi de contrasenyes de 3 a 6 mesos, historial de contrasenyes mínim de 5, bloquejos davant intents fallits, forçar el canvi inicial de contrasenya, etc.), tal com requereix l'ENS.	2013, 2016	**Aplicada parcialment** *S'han millorat els paràmetres d'autenticació en alguns sistemes, però no en tots.*	S'actualitza la redacció anterior. (Vegeu recomanació núm. 8)
	6	Recomanem que s'aprove un procediment que incloga l'obligació que tots els usuaris dels sistemes siguen nominatius, tal com exigeix l'ENS. Quan no siga possible eliminar els usuaris genèrics en els diferents nivells dels sistemes d'informació, s'han de reduir al mínim indispensable i s'han d'incloure controls compensatoris sobre aquests.	2013, 2016	**No aplicada** *Hi ha incidències respecte a la configuració dels identificadors d'usuaris dels sistemes d'informació.*	S'actualitza la redacció. (Vegeu recomanació núm. 8)
	7	Recomanem que es realitze activament una gestió dels drets d'accés a l'aplicació ORION LOGIS que incloga els aspectes següents: - Cada usuari de l'aplicació només disposa dels permisos mínims necessaris d'acord amb les seues funcions. - Atés l'elevat nombre d'usuaris de l'aplicació, han de configurar-se perfils estàndard per als llocs de treball. - Ha de conservar-se la documentació acreditativa de les revisions realitzades, els resultats i les accions dutes a terme. - En cas que es considere necessari que hi haja usuaris que requerisquen un elevat nivell de privilegis i no es puguen evitar els conflictes per falta de segregació de funcions, s'han d'implantar controls compensatoris.	2013, 2016	**No aplicada** *No s'ha modificat la situació respecte a l'informe anterior.*	S'actualitza la redacció. (Vegeu recomanació núm. 7)
CONTINUÏTAT DEL SERVEI	**8**	Recomanem que el màxim nivell directiu elabore i aprove un pla de continuïtat que definisca i documente les accions necessàries per a recuperar i restaurar les activitats crítiques parcialment o totalment interrompudes dins d'un temps predeterminat després d'una interrupció no prevista o desastre.	2013, 2016	**Aplicada parcialment** *S'aporta un document de pla de continuïtat actualitzat però no aprovat per la direcció. No compleix tots els requisits.*	S'actualitza la redacció. (Vegeu recomanació núm. 12)

APÈNDIX 1
L'aplicació ORION LOGIS

ORION LOGIS

ORION LOGIS és l'aplicació corporativa de la Conselleria de Sanitat que integra tota la gestió econòmica i logística dels departaments de salut i altres centres de despesa. Amb aquesta aplicació es gestionen les necessitats de materials, comandes, contractació, recepció de materials o serveis, comprovació de factures i gestió de magatzems.

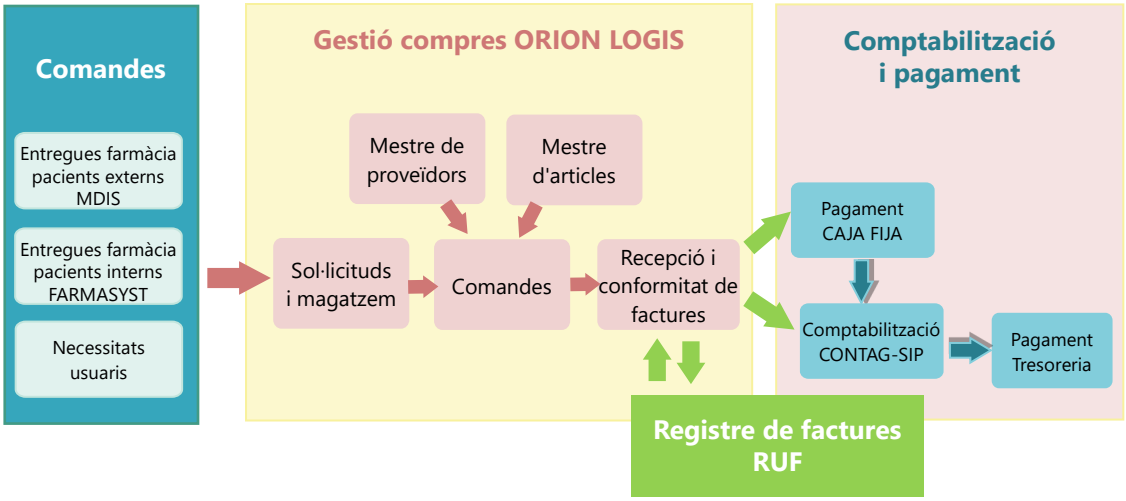
ORION LOGIS es va començar a desenvolupar en 2006 i es va desplegar progressivament en els diferents centres sanitaris a partir de 2008 fins a finalitzar la seua implantació en tots els centres de la Conselleria en 2013.

A més d'ORION LOGIS, les aplicacions més importants que interactuen amb el procés de compres són les següents:

CONTAG-SIP	Comptabilitat pressupostària.
CAJA FIJA	Totes les despeses menors de 5.000 euros previstes en el Decret 25/2017, de 24 de febrer, del Consell.
RUF	Registre de factures de la Generalitat.
MDIS	Programari de gestió de lliuraments de medicaments a pacients externs.
FARMASYST	Programari de gestió de lliuraments de medicaments a pacients interns.

El conjunt d'aquest procés de gestió es pot representar esquemàticament de la manera següent:

Gràfic 3. Mapa de processos de la gestió de compres



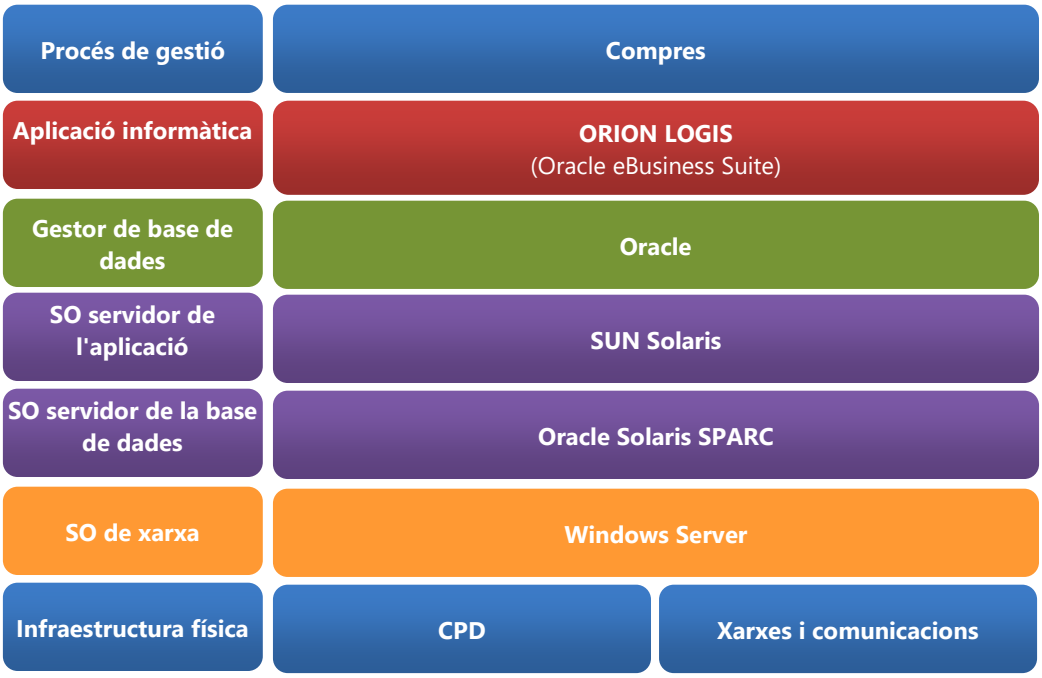
Les principals interfícies entre les aplicacions són:

RUF>ORION	RUF aboca les factures rebudes que es gestionaran en els departaments de salut a ORION LOGIS (estat: enviades).
ORION>RUF	ORION aboca les factures revisades a RUF (estat: disponible).
ORION>CAJA FIJA	Les factures verificades en ORION LOGIS s'aboquen a Caja Fija.
ORION>CONTAG-SIP	Informa manualment de les factures verificades per a la seua comptabilització en CONTAG-SIP.
MDIS>ORION	Aboca les eixides de farmàcia entregades a pacients externs a ORION LOGIS.
FARMASYST>ORION	Aboca els lliuraments de productes farmacèutics a planta de l'hospital.

Entorn tecnològic

L'entorn tecnològic d'ORION LOGIS es pot representar esquemàticament en el gràfic següent.

Gràfic 4. Esquema de l'entorn tecnològic de la gestió de compres sanitàries



APÈNDIX 2
Metodologia de l'auditoria

1. Què és un sistema de control intern

A l'efecte d'aquest informe, entenem com a sistema de control intern de la Conselleria de Sanitat **el sistema dissenyat, implementat i mantingut pels òrgans superiors (responsables del govern de l'entitat), la direcció i altre personal, amb la finalitat de proporcionar una seguretat raonable sobre la consecució dels objectius de l'entitat** relatius a:[4]

a) l'eficàcia i eficiència de les operacions,

b) la fiabilitat de la informació financera, i

c) el compliment de les disposicions legals i reglamentàries aplicables.

Un sistema de control intern efectiu proporciona una seguretat raonable respecte a la consecució dels objectius de l'entitat i redueix a un nivell acceptable el risc de no aconseguir un objectiu de l'entitat.[5]

A aquest efecte, un sistema de control intern comprén cinc components interrelacionats:

a) l'entorn de control (que inclou la governança sobre les tecnologies de la informació i sobre la ciberseguretat),

b) el procés de valoració del risc per l'entitat,

c) el procés de l'entitat per al seguiment del sistema de control intern,

d) el sistema d'informació i comunicació, i

e) les activitats de control (controls generals de tecnologies de la informació CGTI i controls de processament de la informació CPI).

El component "activitats de control" inclou els controls, és a dir, les polítiques o procediments que estableix una entitat per a aconseguir els objectius de control de la direcció o dels responsables del govern de l'entitat. Bàsicament els controls es divideixen en dos tipus: els CGTI i els CPI.

2. Què són els controls generals de tecnologies de la informació

Com a part del sistema de control intern d'una entitat, els controls generals de tecnologies de la informació (CGTI) estableixen un marc general de confiança respecte del funcionament dels controls en els processos i aplicacions de gestió.

[4] NIA-ES 315R/GPF-OCEX 1315R.

[5] Control intern-Marc integrat, Resum executiu, COSO, maig 2013.

D'acord amb l'ENS, els CGTI han de dissenyar-se per a proporcionar una garantia raonable que les dades, la informació i els actius dels sistemes d'informació de l'entitat compleixen les següents propietats o dimensions de la seguretat de la informació:

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

- **Integritat**, és la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, assegurant que no se n'ha produït l'alteració, pèrdua o destrucció, ja siga de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.

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

- **Autenticitat**, és la propietat o característica segons la qual una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.

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

Des del punt de vista de la Sindicatura els CGTI compleixen una doble funció:

a) Els CGTI són importants com a protecció davant de les ciberamenaces. En els últims anys el sector de la salut s'ha convertit en un objectiu preferent dels ciberdelinqüents, i uns sòlids CGTI representen la defensa més eficaç davant de les ciberamenaces en un entorn que se sustenta en sistemes d'informació intensament interconnectats.

b) A més, aquests controls són importants, ja que estableixen un marc general de confiança respecte del funcionament dels CPI. La ineficàcia o mal funcionament dels CGTI impediria confiar en els controls de processament de la informació. Per tant, la seua auditoria proporciona confiança respecte de si els CGTI compleixen o no aquest objectiu.

Els auditors han de revisar el sistema de control intern i obtindre evidència d'auditoria per a aconseguir un determinat grau de seguretat sobre l'eficàcia dels CGTI i comprovar si garanteixen raonablement les cinc propietats o dimensions de la seguretat.

Finalment, els controls de seguretat de la informació, bàsicament els CGTI, són de compliment obligat en virtut de diferent normativa, especialment per l'ENS.

3. Metodologia de l'auditoria

Aquesta auditoria està basada en les guies pràctiques de fiscalització GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat", i GPF-OCEX 5330, "Revisió dels controls generals de tecnologies d'informació en un entorn d'administració electrònica", que formen part del *Manual de fiscalització* de la Sindicatura de Comptes i que poden consultar-se en

el nostre web. Per a major 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 d'obligat compliment 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 són exigits per l'ENS.

La metodologia establida en les guies esmentades inclou la revisió de nombrosos controls. Hem seleccionat per a aquesta auditoria, per considerar-los els més importants per al procés de compres sanitàries, els següents:

Quadre 4. Controls generals de tecnologies de la informació

Àrea		Control
A. Marc organitzatiu	A1/A2/ A3/A4	Marc organitzatiu i governança de la ciberseguretat (CBCS 8)
C. Operacions dels sistemes d'informació	C1H	Inventari de maquinari (CBCS 1)
	C1S	Inventari de programari (CBCS 2)
	C2	Gestió de vulnerabilitats (CBCS 3)
	C3	Configuracions segures (CBCS 5)
	C4	Registre de l'activitat dels usuaris (CBCS 6)
D. Controls d'accés a dades i programes	D1	Ús controlat de privilegis administratius (CBCS 4)
	D2/D3/D4	Controls d'accés a usuaris
	D5	Protecció de xarxes i comunicacions
E. Continuïtat del servei	E1	Còpia de seguretat de dades i sistemes (CBCS 7)

4. Criteris d'avaluació dels controls

Els CBCS i els CGTI són controls globals formats per diversos subcontrols detallats. Totes les nostres comprovacions tenen per finalitat contrastar-ne la situació real en l'entitat amb les bones pràctiques recollides en les GPF-OCEX 5313 i 5330, en les quals s'especifiquen amb el màxim detall els aspectes comprovats en cada control.

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

Avaluació dels subcontrols

Els CBCS i els CGTI són controls globals compostos per diversos controls detallats o subcontrols, dels quals hem revisat el disseny i l'eficàcia operativa.

El treball d'auditoria ha consistit bàsicament a avaluar cada un dels 51 subcontrols revisats en funció bé dels resultats de les proves realitzades i les evidències obtingudes o bé de la informació proporcionada en l'informe d'auditoria de l'ENS, si existeix i si hi confiem. Cada subcontrol s'avalua segons l'escala que mostra el quadre següent:

Quadre 5. Avaluació dels subcontrols

Avaluació	Descripció
Control efectiu	Cobreix al 100% l'objectiu de control i: El procediment està formalitzat (documentat i aprovat) i actualitzat. El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	En línies generals, compleix l'objectiu de control, si bé hi pot haver certs aspectes no coberts al 100% i: - Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.). - Les proves realitzades per a verificar la implementació són satisfactòries. - S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	Cobreix de forma molt limitada l'objectiu de control i: - Se segueix un procediment, encara que aquest pot no estar formalitzat. - El resultat de les proves d'implementació i d'eficàcia no és satisfactori. Cobreix en línies generals l'objectiu de control, però: - No se segueix un procediment clar. - Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	No cobreix l'objectiu de control. El disseny cobreix l'objectiu de control, però el resultat de la revisió realitzada posa de manifest que la implementació o l'eficàcia operativa del control no són satisfactòries (s'han detectat incompliments significatius i generalitzats).

Nivell de maduresa dels controls

Per a determinar la situació global de cada control hem utilitzat el model de nivell de maduresa dels processos de control d'acord amb el que s'estableix en les GPF-OCEX 5313 i GPF-OCEX 5330, que al seu torn estan basades en la *Guía de seguridad CCN-STIC 804* del CCN, usant una escala, segons es resumeix en el quadre següent. Les descripcions són les establides en l'annex II de l'RD 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

Quadre 6. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	No existeix un procés que done suport al servei requerit.
N1 Inicial / *ad hoc*	10	Les organitzacions en aquest nivell no disposen d'un ambient estable per a la prestació del servei requerit. Encara que s'utilitzen tècniques correctes d'enginyeria, els esforços es veuen minats per falta de planificació. L'èxit dels projectes es basa la majoria de les vegades en l'esforç personal, encara que sovint es produeixen fracassos i quasi sempre retards i sobrecostos. El resultat és impredictible. Sovint les solucions s'implementen de manera reactiva als incidents. Els procediments de treball, quan n'hi ha, són informals, incomplets i no s'apliquen de manera sistemàtica.
N2 Repetible, però intuïtiu	50	En aquest nivell les organitzacions disposen d'unes pràctiques institucionalitzades de gestió, hi ha unes mètriques bàsiques i un seguiment raonable de la qualitat. Hi ha procediments de treball, però no estan prou documentats o no cobreixen tots els aspectes requerits.
N3 Procés definit	80	A més d'una bona gestió, a aquest nivell les organitzacions disposen de normativa i procediments detallats i documentats de coordinació entre grups, formació del personal, tècniques d'enginyeria, etc.
N4 Gestionat i mesurable	90	Es caracteritza perquè les organitzacions disposen d'un conjunt de mètriques d'efectivitat i eficiència, que s'usen de manera sistemàtica per a la presa de decisions i la gestió de riscos. El servei resultant és d'alta qualitat.
N5 Optimitzat	100	L'organització completa està abocada en la millora contínua dels processos. Es fa ús intensiu de les mètriques i es gestiona el procés d'innovació.

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

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

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

Indicador global

A l'efecte de l'ENS, la guia CCN-STIC-824 inclou una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics. En particular l'**índex de maduresa general** sintetitza, en tant per cent, el nivell de maduresa aconseguit per un organisme respecte del conjunt de controls de ciberseguretat.

5. Classificació de les deficiències de control a l'efecte de l'auditoria

En avaluar les deficiències de control intern detectades s'ha de considerar la rellevància i es classifiquen en tres nivells d'importància relativa:

- Una **deficiència de control intern** existeix quan el disseny o el funcionament d'un control no permet al personal de l'entitat o a la seua direcció, en el curs ordinari de les operacions, previndre o detectar errors o irregularitats en un termini raonable.

  Poden ser una deficiència de disseny del control (quan un control necessari per a aconseguir l'objectiu de control no existeix o no està adequadament dissenyat) o deficiències de funcionament (quan un control adequadament dissenyat no opera tal com va ser dissenyat o la persona que l'executa no el realitza eficaçment).

  No es pot qualificar de deficiència significativa ni debilitat material, ja que el seu impacte potencial no s'espera que siga significatiu. L'esmena pot aportar millores en el procés examinat.

- Una **deficiència significativa** és una deficiència en el control intern, o una combinació de deficiències, que afecten adversament la capacitat de l'entitat per a iniciar, autoritzar, registrar, processar o reportar informació financera o pressupostària de manera fiable, de conformitat amb els principis o normes comptables i/o pressupostàries aplicables, i existeix una probabilitat, que és més que remota, que una manifestació errònia en els comptes anuals, o un incompliment, que no és clarament trivial, no es previnga o es detecte en termini oportú.

- Una **debilitat material** és una deficiència significativa en el control intern, o una combinació d'aquestes, respecte de les quals existeix una raonable possibilitat que una incorrecció material en els comptes anuals, incloent-hi un incompliment de caràcter greu, no es previnga o detecte i corregisca en termini oportú.

  Tractant-se d'un CGTI, a més, seran aquelles que no són capaces de previndre un incident que puga causar una pertorbació o impacte significatiu en la seguretat de la informació manejada o en els serveis prestats. A aquest efecte, es considerarà que tenen un impacte significatiu els nivells "Alt", "Molt alt" i "Crític" recollits en la taula de "Criteris de determinació del nivell d'impacte" de la guia CCN-STIC 817.

Algunes deficiències de control poden ser considerades no significatives individualment, però considerades juntament amb d'altres de similars, l'efecte combinat pot ser més significatiu.

L'auditor informàtic determinarà si les deficiències de control són, individualment o en conjunt, debilitats materials o deficiències significatives per al funcionament adequat dels sistemes d'informació.

Si les deficiències de control constitueixen debilitats materials, l'auditor financer, sobre la base del treball de l'auditor informàtic, conclourà que els controls interns no són eficaços i haurà de replantejar-se la seua estratègia d'auditoria, és a dir, la combinació adequada de

proves de compliment i de proves substantives, i donar major èmfasi a aquestes últimes per a intentar minimitzar el risc final d'auditoria.

6. Recomanacions i el seu seguiment

Si s'efectuen **recomanacions**, hi haurà una relació directa entre el tipus de deficiència de control (segons la seua importància relativa), el risc d'auditoria que representa i la prioritat que es concedisca a cada recomanació.

La prioritat també estarà matisada per consideracions cost/benefici.

En el quadre següent es resumeix la relació existent entre els tres tipus de deficiències de control segons la seua rellevància o importància relativa, el risc que representen i la prioritat de les recomanacions corresponents:

Quadre 7. Categoria de les deficiències de control i recomanacions

Tipus de deficiència segons la seua importància relativa	Risc	Prioritat d'una recomanació
Debilitat material	**Alt**	**Alta** — Es requereix atenció urgent de la direcció per a implantar controls/procediments que mitiguen els riscos identificats.
Deficiència significativa	**Mitjà**	**Mitjana** — La direcció hauria d'establir un pla d'acció concret per a resoldre la deficiència observada en un termini raonable.
Deficiència de control intern	**Baix**	**Baixa**

Les debilitats materials han de ser incloses en l'informe d'auditoria com una excepció o com una conclusió, segons el tipus d'informe.

Seguiment de les recomanacions d'informes anteriors

En la valoració de la situació actual, s'ha seguit la GPF-OCEX 1735, "Les recomanacions i el seu seguiment", que proposa la categorització següent:

Quadre 8. Situació de les recomanacions

Totalment o substancialment aplicada	Si l'ens auditat ha adoptat les mesures correctores, raonables i proporcionades en l'esfera de les seues competències, que permeten considerar que la recomanació ha produït efectes i no ha quedat pendent de resolució cap qüestió d'importància significativa. En aquests casos s'entendrà que la recomanació s'ha complit raonablement. A més, s'ha obtingut evidència suficient que acredita les mesures adoptades.
Aplicada parcialment	Si l'ens auditat ha pres en consideració les recomanacions i ha realitzat actuacions encaminades a corregir les deficiències, debilitats o insuficiències que s'han posat de manifest, però solament en un estat incipient, en una part d'aquestes o en alguns aspectes, la qual cosa no permet considerar que la recomanació s'ha complit raonablement.
No aplicada	Si l'ens auditat no ha realitzat les actuacions encaminades a corregir les deficiències, debilitats o insuficiències que s'han posat de manifest o bé ho ha fet insuficientment o inadequadament, de manera que la recomanació segueix sense aplicar-se.
Sense validesa en el marc actual	S'hi inclouen les recomanacions que, encara que vàlides i pertinents quan es va emetre l'informe i per a l'exercici fiscalitzat, i tot i ser acceptades i reconegudes per l'ens auditat, no poden aplicar-se en el context actual, perquè no es donen les circumstàncies que ho permeten o la mateixa casuística que llavors, és a dir, no es donen en el moment actual els supòsits dels fets en funció dels quals es va efectuar la recomanació en el passat. La recomanació ha esdevingut inaplicable.
No verificada	S'inclouen en aquesta categoria les recomanacions que, encara que acceptades o fins i tot aplicades i corregides per l'ens auditat, necessitarien obligatòriament alguna prova addicional per a contrastar el que ha manifestat l'ens auditat que excedeixen l'abast previst en el treball.

APÈNDIX 3
Situació dels controls auditats

1. Introducció

Hem revisat un total de 51 subcontrols relacionats amb el procés de gestió de les compres sanitàries, agrupats en els 10 controls principals assenyalats en el quadre 2, i hem avaluat el seu nivell de maduresa.

Encara que la classificació dels sistemes d'informació és una exigència establida per l'ENS, no hem obtingut evidència que el sistema ORION LOGIS haja sigut classificat per part de la Conselleria d'acord amb l'ENS (categoria alta, mitjana o baixa), per la qual cosa l'hem considerat de categoria de seguretat MITJANA, que és la més habitual en els sistemes que suporten processos de gestió administrativa. El nivell de maduresa requerit per l'ENS per a aquest tipus de sistemes és *N3, procés definit* i els sistemes han d'aconseguir un índex de maduresa del 80%.

Els resultats obtinguts per a cada un dels CGTI revisats es mostren en el quadre 2. En l'apartat 2 d'aquest informe s'han inclòs les deficiències més rellevants dels CGTI, en l'apartat 3 s'inclouen també les observacions més importants sobre compliment de la normativa i en l'apartat 6, les recomanacions que es deriven de la revisió realitzada. A continuació, es detallen les observacions i deficiències de control detallades obtingudes en la nostra auditoria.

2. Marc organitzatiu i governança de la ciberseguretat

Per què són importants aquests controls

Amb la inclusió dels controls A1, A2, A3 i A4 es pretén assegurar que es compleixen diverses normes rellevants per a mantindre un control adequat sobre la seguretat dels sistemes d'informació i les comunicacions, i la privacitat de la informació.

És molt important donar el compliment degut al que es disposa en l'Esquema Nacional de Seguretat, ja que la seua finalitat és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeta als ciutadans i a les administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans.

La gestió de la ciberseguretat, com a tasca clau per a la prevenció proactiva, requereix l'establiment d'un marc de governança, en el qual es designe els organismes o unitats responsables d'aquesta gestió i es definisquen clarament les seues competències en aquest àmbit, que hauran de ser conegudes per tota l'organització.

La importància de la governança en la gestió de la ciberseguretat ha sigut objecte de diversos documents i guies del Centre Criptològic Nacional (CCN), entre els quals destaquen *Aproximación al marco de gobernanza de la ciberseguridad. Año 2022*, la *Guía de seguridad de las TIC CCN-STIC 201. Organización y gestión para la seguridad de las TIC* i la *Guía de seguridad de las TIC CCN-STIC 801. Esquema Nacional de Seguridad. Responsabilidades y funciones*.

https://ens.ccn.cni.es/ca/

L'existència d'un conjunt eficaç de processos de gestió de la ciberseguretat i de responsabilitats definides proporciona a les entitats múltiples avantatges respecte a les entitats sense un marc de governança adequadament definit, independentment de l'existència de recursos tècnics i de les mesures de seguretat aplicades.

2.1. Compliment normatiu i governança de la ciberseguretat (A1-CBCS 8)

Objectiu del control

Assegurar el compliment de la normativa bàsica en matèria de seguretat de la informació, la qual cosa inclou l'establiment d'una adequada governança de ciberseguretat.

Situació del control

Compliment de l'ENS

L'organització de la seguretat de la informació en la Conselleria s'estableix en l'Ordre 9/2012, de 10 de juliol de 2012, en què es configuren i estableixen els òrgans responsables de la seguretat, tant pel que fa a la Conselleria com als departaments de salut que en depenen.

Aquesta ordre ha d'actualitzar-se, ja que conté referència a responsabilitats de seguretat i normativa de protecció de dades que ja no està vigent i les seues previsions han d'adequar-se al que s'exigeix en el Reial Decret 311/2022, de 3 de maig, pel qual s'aprova l'Esquema Nacional de Seguretat (ENS).

Alguns dels òrgans de seguretat previstos en l'ENS i en l'Ordre 9/2012 no s'han nomenat formalment ni al nivell de la Conselleria ni al nivell descentralitzat per als departaments de salut. D'acord amb el que es preveu en l'article 13 de l'ENS, aquests responsables han d'estar identificats de manera inequívoca. Alguns responsables, com el responsable del servei, no s'identifiquen inequívocament.

No s'ha establit formalment la categoria (alta, mitjana o baixa) del sistema ORION LOGIS, tal com exigeix l'ENS.

La Conselleria ha presentat l'informe INES al CCN d'acord amb el que es preveu en l'ENS.

No s'han realitzat les auditories previstes en l'article 31 de l'ENS ni, en conseqüència, s'han publicat en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS aprovada per mitjà de la Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques.

Governança de la ciberseguretat

La Conselleria no té establida una adequada governança de la seguretat de la informació que preveja un lideratge eficaç de l'alta direcció per a promoure i implantar, al llarg de tota l'organització, els controls exigits per la normativa de seguretat de la informació i protecció de dades personals que li és aplicable, bàsicament ENS i LOPDP.[6]

Encara que existeix un alt nivell de compromís i conscienciació amb la ciberseguretat per part dels membres de la Subdirecció General de Sistemes d'Informació per a la Salut (SDGSIS) i, en particular, de l'Oficina de Seguretat de la Informació, aquest compromís no es visualitza en els òrgans superiors de la Conselleria, la qual cosa s'observa en aspectes com:

- La Conselleria disposa d'una ordre que regula l'organització de la seguretat, que es completa amb un marc normatiu i procedimental, però aquesta documentació no està completa ni està aprovada formalment i no ens consta que es comunique formalment a tots els responsables encarregats d'aplicar-la. A més, com ja s'ha indicat, aquesta ordre és de 2012 i es troba desactualitzada.

- No hem pogut avaluar si l'SDGSIS disposa de suficients recursos econòmics i humans dedicats a la seguretat de la informació atés que no se'ns ha facilitat la informació sol·licitada sobre el seu personal, projectes i dotacions pressupostàries.

Addicionalment, determinades circumstàncies indiquen que la governança no pot considerar-se efectiva. Basem aquesta afirmació en les mancances rellevants següents:

- La falta de lideratge en matèria de ciberseguretat dels òrgans superiors de la Conselleria.

  L'organització no disposa de plans ni estratègies elaborades i aprovades pels òrgans superiors en relació amb la seguretat de la informació, ni impulsa les mesures de seguretat necessàries, incloent-hi la formació i conscienciació dels seus treballadors. Són els membres del departament TIC, per pròpia iniciativa i sense el suport del comité de seguretat de la informació, els qui implanten mesures relacionades amb la ciberseguretat i impulsen el compliment de la normativa en aquesta matèria.

[6] Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals.

El compromís amb la ciberseguretat ha de partir dels òrgans superiors de la Conselleria perquè puga arribar a la resta de l'organització i es facilite la seua aplicació pràctica.

- El Comité de Seguretat de la Informació (CSI) únicament s'ha reunit una vegada en 2022, encara que l'acta d'aquesta reunió no està signada. És necessari que el CSI funcione de manera efectiva, com a òrgan imprescindible per a coordinar la seguretat de la informació entre les diferents àrees de l'organització.

  És en el CSI on s'han de prendre les decisions concretes en matèria de seguretat de la informació, aprovant les normes de seguretat pertinents i impulsant les accions a dur a terme. Encara que aquest òrgan està establit en una ordre aprovada per la Conselleria, no exerceix les seues funcions de manera efectiva. El Comité ha de reunir-se periòdicament i, en una entitat de la grandària de la Conselleria i atesa la complexitat dels seus sistemes, recomanem que ho faça almenys mensualment.

- Alguns dels rols en matèria de seguretat de la informació no estan correctament definits i altres no s'han nomenat formalment.

  El rol de responsable del servei no es troba formalment definit i altres rols de seguretat es defineixen sobre la base de la normativa de protecció de dades anterior. No s'han nomenat tots els rols de seguretat dels elements descentralitzats de l'organització previstos en l'Ordre 9/2012 de la Conselleria.

Els òrgans superiors de la Conselleria són els responsables que hi haja uns controls de seguretat adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació que garantisca la ciberresiliència de l'entitat.

És necessari solucionar de manera urgent les mancances identificades, atés que afecten de manera negativa el nivell de seguretat de la informació de la Conselleria.

Compliment del Reial Decret 4/2010 (ENI)

No s'ha elaborat el pla d'adequació a l'ENI que exigeix el Reial Decret 4/2010 de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica. ORION LOGIS no està adaptat a la generació d'expedients ENI.

La Conselleria ha d'elaborar un pla d'adaptació a l'ENI d'acord amb el que s'exigeix en la mateixa norma. El pla ha d'incloure l'adaptació d'ORION LOGIS per a la generació de documents i expedients ENI.

Compliment de la LOPDP

Quant al compliment en matèria de protecció de dades personals, la revisió realitzada ha posat de manifest que hi ha algunes mesures en relació amb el compliment de la LOPDP que es troben implementades: nomenament d'un delegat de protecció de dades (DPD) per

a la Generalitat, elaboració de la relació d'activitats de tractament, que inclou la referent a compres sanitàries, previsió d'òrgans encarregats de protecció de dades, etc.

No obstant això, tenint en compte el tipus de dades personals que es tracten en la Conselleria i els seus departaments, haurien de fer-se esforços addicionals: realitzar auditories de protecció de dades i nomenar el subdelegat de protecció de dades per a sanitat previst en l'organització del DPD de la Generalitat.

2.2. Estratègia de TI (A2)

Objectiu del control

Assegurar una planificació estratègica dels sistemes d'informació de manera que aquests estiguen sempre orientats a la consecució dels objectius de l'organització.

Situació del control

La Conselleria basa la seua planificació estratègica en relació amb els sistemes d'informació en el Pla Estratègic de Transformació Digital de l'Administració de la Generalitat 2020-2025. No obstant això, no hem identificat una planificació quant a projectes de la Conselleria que concrete i desenvolupe anualment els objectius previstos en aquesta planificació estratègica. Tampoc hem pogut obtindre evidències que els projectes de TI disposen de pressupost adequat perquè es puguen dur a terme.

2.3. Organització i personal de TI (A3)

Objectiu del control

Assegurar la independència funcional del departament TIC de manera que li permeta fer les seues tasques per tal d'arribar a tota l'organització, assegurar que existeix segregació de funcions incompatibles entre els components del departament, garantir la formació en matèria de seguretat de la informació i utilitzar indicadors per a valorar el nivell de prestació dels serveis TIC a la resta de l'organització.

Situació del control

Durant el període auditat, la Subdirecció General de Sistemes de la Informació per a la Salut (SDGSIS) depén de la Direcció General de Planificació, Eficiència Tecnològica i Atenció al Pacient i s'estructura en tres serveis que al seu torn es divideixen en unitats funcionals no reconegudes formalment en el ROF de la Conselleria.

No hem identificat situacions que comprometen la independència de l'SDGSIS quant a la dedicació dels recursos necessaris TIC a les altres direccions generals i unitats. No obstant això, la seua ubicació en l'organigrama de la Conselleria la situa com a dependent d'una direcció general amb múltiples missions.

L'Ordre 4/2023, de 13 d'octubre, de la Conselleria de Sanitat, per la qual es desplega el Decret 135/2023, de 10 d'agost, del Consell, d'aprovació del Reglament Orgànic i Funcional de la Conselleria de Sanitat, modifica la denominació del departament, que passa a ser la Subdirecció General de Tecnologies de la Informació i les Comunicacions per a la Salut, el situa sota la dependència directa de la Secretaria Autonòmica de Planificació, Informació i Transformació Digital i la dota d'un quart servei.

No hem pogut obtindre evidència de l'existència d'un pla de formació sobre seguretat de la informació en la Conselleria.

D'acord amb la informació facilitada no existeix un seguiment d'indicadors dels serveis prestats per l'SDGSIS a la resta d'unitats de la Conselleria.

2.4. Marc normatiu i procedimental de seguretat (A4)

Objectiu del control

Aprovar una normativa interna de seguretat de la informació i comunicar els procediments associats als responsables de la seua aplicació.

Situació del control

La Conselleria aplica la política de seguretat de la Generalitat. L'SDGSIS ha desenvolupat alguns procediments de seguretat no aprovats formalment. A més, no consta que s'hagen comunicat adequadament a tots els responsables d'aplicar-los ni que existisca un repositori actualitzat disponible per a aquests responsables.

Hi ha aspectes importants per a la seguretat de la informació que no compten amb un procediment detallat, aprovat i comunicat formalment als interessats com la gestió d'inventaris de programari i maquinari, gestió d'usuaris, control dels usuaris administradors dels sistemes o assignació de responsabilitats en els sistemes d'informació.

3. Operacions dels sistemes d'informació

Apartat eliminat en la fase d'al·legacions.

4. Controls d'accés a dades i programes

Apartat eliminat en la fase d'al·legacions.

Atesa la sensibilitat dels sistemes d'informació sanitaris i de la informació tractada, i a fi de reduir a zero el risc addicional en la seguretat d'aquests sistemes, derivat d'un possible mal ús del nostre informe, els resultats detallats que s'incloïen en els apartats 3 i 4 de l'apèndix 3 s'han eliminat en la fase d'al·legacions i es comuniquen amb caràcter confidencial als responsables de la Conselleria perquè puguen adoptar les mesures correctores necessàries.

5. Continuïtat del servei

5.1. Còpies de seguretat de dades i sistemes (E1-CBCS 7)

Objectiu del control

Utilitzar processos i eines per a realitzar còpies de seguretat de la informació crítica amb una metodologia que permeta la recuperació de la informació 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 totes o part de les dades i programari d'una entitat.

Els danys de ciberatacs es poden mitigar si es disposa de còpia de seguretat de les dades afectades.

Situació del control

La Conselleria disposa de diversos controls i procediments associats a la gestió dels diferents nivells de còpia de seguretat de les dades i sistemes, que no detallem per raons de seguretat.

Hi ha un procés de revisió de les còpies de seguretat dut a terme pels tècnics responsables, que garanteix la revisió de l'estat de les còpies per mitjà de *tickets* en l'eina de gestió d'incidències que queden pendents fins que es resolen.

Durant l'auditoria hem observat que es realitzen restauracions de dades i sistemes des de la còpia de seguretat que, encara que no són proves planificades de restauració, es duen a terme amb èxit i es registren en forma de *tickets* en l'eina de gestió d'incidències.

Encara que hi ha un cert nivell de control sobre les còpies, hem observat mancances que impedeixen aconseguir un nivell de maduresa superior en aquest control, com ara:

- El procediment de polítiques de còpies de seguretat s'ha actualitzat recentment. Encara que actualment preveu proves de recuperació cada 6 mesos, no especifica sobre quins sistemes ni preveu la manera de documentar les proves.

- Els responsables funcionals de les dades no participen en la definició de les dades a copiar ni en els períodes de retenció de les còpies. Les dades incloses en la còpia són les que decideixen els tècnics de sistemes de l'SGSIS segons el seu criteri, excepte peticions expresses dels responsables funcionals del sistema a través de l'eina de gestió d'incidències.

- La Conselleria disposa d'un únic CPD, la qual cosa comporta diversos tipus de risc en cas d'incident: pèrdua de disponibilitat o continuïtat de serveis, pèrdua de les dades de còpia, etc.

- Encara que hi ha còpies desconnectades emmagatzemades en una ubicació diferent del CPD, aquestes no s'extrauen amb una periodicitat suficient per a impedir la pèrdua de dades en cas de requerir suports des d'aquestes còpies.

Aquest sistema de còpies de seguretat , encara que és útil i fins ara ha sigut suficient per a recuperacions d'incidents de seguretat lleus, no garanteix la recuperació dels sistemes crítics de la Conselleria en uns terminis raonables davant un incident greu que afecte el seu CPD.

GLOSSARI

Alta direcció: A l'efecte d'aquest treball, ens referim als òrgans superiors de la Conselleria, conseller/a, secretaries autonòmiques, direccions generals i sotssecretaries. Són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions, així com una adequada governança de ciberseguretat.

Alta disponibilitat: És la capacitat que té un sistema per a assegurar la continuïtat dels serveis, fins i tot en situacions en què ocórreguen incidents de maquinari, programari, talls d'energia, de comunicacions o d'un altre tipus.

Categoria de seguretat d'un sistema: és un grau, dins de l'escala Bàsica-Mitjana-Alta, amb què es classifica un sistema d'informació a fi de seleccionar les mesures de seguretat necessàries per a aquest. La categoria de seguretat del sistema recull la visió holística del conjunt d'actius com un tot harmònic, orientat a la prestació d'uns serveis.

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 als quals s'enfronta hui dia. A l'efecte 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 de tals sistemes i d'altres persones afectades per les ciberamenaces (Reglament (UE) 2019/881).

Direcció: Són els responsables de l'execució de les activitats establides per l'alta direcció en matèria TIC i de ciberseguretat, és la direcció executiva. En aquest grup, a l'efecte d'aquest informe, s'inclou els membres de l'alta direcció amb responsabilitats específiques sobre les TIC, el responsable de seguretat, el responsable dels sistemes d'informació i les comunicacions, els funcionaris directors del departament TIC i els subdirectors o caps de servei.

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*.

Informe INES: És un informe-declaració que han de realitzar les administracions públiques anualment per a presentar-lo al Centre Criptològic Nacional (CCN) amb l'eina del mateix nom. Aquesta eina és una solució desenvolupada pel CCN per a la governança de la ciberseguretat, que permet avaluar regularment l'estat de la seguretat dels sistemes TIC de les entitats i la seua adequació a l'Esquema Nacional de Seguretat (ENS) adaptant-se a altres estàndards o normes reguladores en cas necessari.

Interfície: És una connexió entre dos dispositius, aplicacions o sistemes d'origen i destinació, per mitjà de la qual s'intercanvia 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 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 dels preceptes de l'ENS, en primera instància, i del desenvolupament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

Política de seguretat de la informació: La política de seguretat de la informació és el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta, d'acord amb l'article 12 del Reial Decret 311/2022 (ENS). Ha de ser aprovada pels alts òrgans de direcció de l'entitat i 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 el que cal fer, pas a pas. Detallen de manera clara i precisa: *a*) com dur a terme les tasques habituals; *b*) qui ha de fer cada tasca, i *c*) com identificar i reportar comportaments anòmals.

Procés: Conjunt organitzat d'activitats que es duen a terme per a produir un producte o prestar un servei, que té un principi i fi delimitats, que implica recursos i dona lloc a un resultat.

ABREVIACIONS

CBCS: Controls bàsics de ciberseguretat (formen part dels CGTI).

CGTI: Controls generals de tecnologies de la informació.

CPD: Centre de processament de dades.

CPI: Controls de procés de gestió de la informació.

DGTIC: Direcció General de Tecnologies de la Informació i les Comunicacions.

DPD: Delegat de protecció de dades personals.

EDR: Eina de detecció i resposta davant amenaces cibernètiques (per les seues sigles en anglés: *endpoint detection and response*).

ENI: RD 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.

ENS: RD 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

GETEC: Unitat de gestió de tecnologia (servidors lògics) de l'SDGSIS.

LAN: Xarxa d'àrea local (*local area network*).

LOPDP: Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals.

ODM: Oficina de dades mestres de la Conselleria que controla i autoritza les altes d'articles i proveïdors en ORION LOGIS.

OSI: Oficina de Seguretat de la Informació de la Conselleria.

RGPD: Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.

ROF: Reglament orgànic i funcional.

RUF: Aplicació amb la qual es gestiona el registre de factures de la Generalitat Valenciana.

SDGSIS: Subdirecció General de Sistemes de la Informació per a la Salut.

TIC: Tecnologies de la informació i les comunicacions.

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que es preveu en la secció 1220 del *Manual de fiscalització* de la Sindicatura, l'esborrany previ de l'Informe d'auditoria es va discutir amb responsables TIC de la Conselleria de Sanitat 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 l'exercici 2022, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

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

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

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

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

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

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, 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 13 de desembre de 2023, va aprovar aquest informe d'auditoria.

ANNEX I

Al·legacions presentades

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

PAA2022/26 - AUDITORIA DE SISTEMAS DE INFORMACIÓN DEL CONTROL INTERNO DE LA GESTIÓN DE COMPRAS SANITARIAS

C/ Sant Vicent, 4
46002 València

Código: 2078631

Interesado nº 1

Doc. identidad: [redacted]
Nombre: BARRACHINA VALERO M CARMEN
Notificación: Electrónica
Idioma: Castellano
Correo-e: [redacted]

Acepta la interoperabilidad entre Administraciones (*)

Representante

Contenido de la Instancia

PAA2022/26 - Auditoria de Sistemas de Información del control interno de la gestión de compras sanitarias

Ver contenido en ficheros adjuntos

Ficheros adjuntos

Nombre:	Huella digital SHA-256	Tamaño
Selección entidad		95,0 KB
5_SC22_Aleg_Orion Logis_Resp a SC_fdo	[redacted]	833,9 KB
SC22_Aleg_Orion Logis_resp_C Sanidad	[redacted]	374,5 KB

Aceptación de condiciones:

☑ El solicitante conoce que sus datos personales solamente serán utilizados para gestionar su solicitud, facilitar al interesado la cumplimentación de futuras instancias y recibir comunicaciones en expedientes en los que pudiera resultar afectado. Dichos datos no se cederán a terceros, salvo obligación legal. Manifestando su consentimiento en los términos del artículo 6 del Reglamento General de Protección de Datos al que ha tenido acceso artículo 6.1.a) del RGPD. Diario oficial UE 4/5/2016.

☑ Igualmente manifiesta conocer sus derechos a solicitar el acceso a sus datos personales, a solicitar su rectificación o supresión, a solicitar la limitación de su tratamiento, a oponerse al tratamiento y el derecho a la portabilidad de los datos. Todo ello mediante la correspondiente instancia dirigida a:

Organismo: SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA - CIF S9600001C
Sede Electrónica: https://sindicom sedipualba.es/
Delegado Protección de Datos: dpd@sindicom.es
Dirección postal: C/ Sant Vicent, 4 - 46002 València

(*) La interoperabilidad entre Administraciones permite que la Administración actuante pueda consultar o recabar datos y documentos de cualquier Administración. En caso de oposición, deberá aportar con la solicitud la documentación acreditativa correspondiente (art. 28.2 Ley 39/2015. Redactado por la disposición final 12 de la Ley Orgánica 3/2018, de 5 de diciembre.)

GENERALITAT VALENCIANA
Conselleria de Hacienda, Economía y Administración Pública

INTERVENCIÓN GENERAL
Ciudad Administrativa 9 de Octubre
Calle de la Democracia, 77, Edificio B2
46018 Valencia
Tel.: 961248112

Ref: *IGL/DGI/AALl-gpb*
Asunto: *Sindicatura de Comptes. PAA2022/26. Borrador Informe de auditoría de ciberseguridad y de los controles generales de tecnologías de la información de la aplicación ORION LOGIS, ejercicio 2022.*

En contestación a su escrito de fecha 3 de noviembre del corriente al que adjuntaba el borrador del "*Informe de auditoría de ciberseguridad y de los controles generales de tecnologías de la información de la aplicación ORION LOGIS, ejercicio 2022"*, se ha procedido al envío telemático de las alegaciones efectuadas por la Conselleria de Sanidad para su consideración y efectos oportunos así como copia del presente escrito.

La Interventora General

Firmado por Amparo Adam Llagües el
24/11/2023 14:05:50

Excmo. Sr. D. Vicent Cucarella Tormo. Síndic Major de la Sindicatura de Comptes
C/ San Vicente, 4
46002 Valencia

CSV [redacted] URL de validación [redacted]

GENERALITAT VALENCIANA
Conselleria de Sanitat

SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA LA SALUD

Alegaciones al borrador de informe de auditoría de ciberseguridad y de controles generales de tecnologías de la información de la aplicación Orión-Logis, del ejercicio 2022

1. Alegación

Referencia

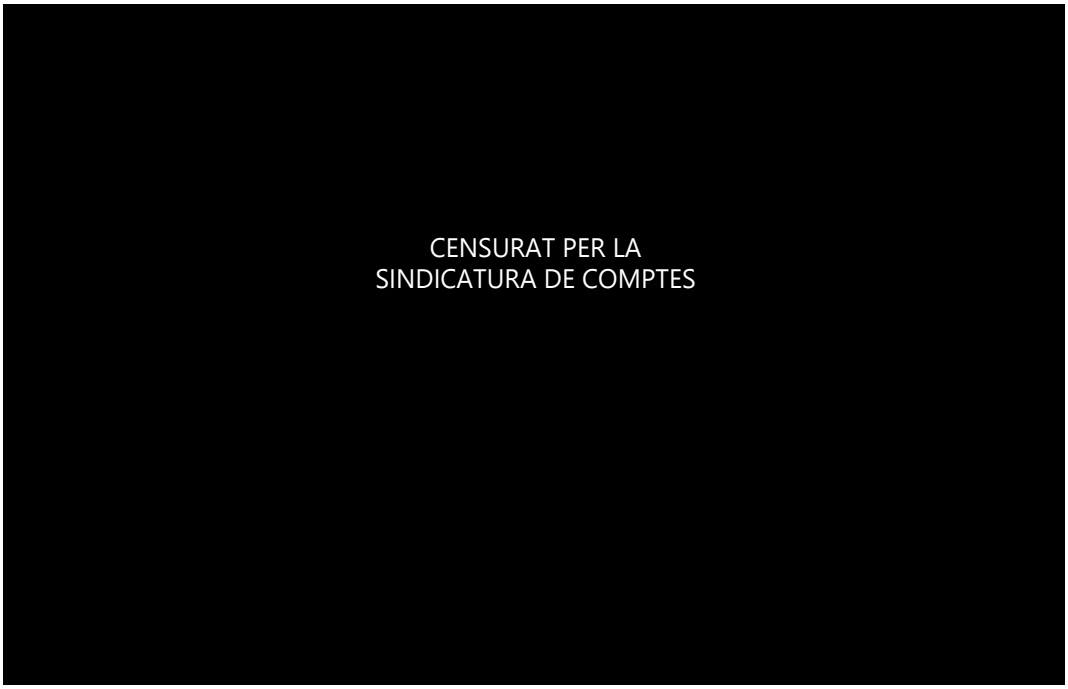
Apartado Conclusiones generales de TI, página 6:

> La situación de los CGTI representa, por tanto, un nivel de riesgo sobre la seguridad de la información inaceptable y las deficiencias existentes no permiten confiar en el buen funcionamiento de los CPI, por lo que la entidad debe adoptar medidas para reconducir la situación

Contenido

Entre otras actuaciones para corregir esta situación, la Conselleria tiene previsto invertir 4.5M€ en cinco proyectos financiados por la UE que gestiona el Ministerio de Sanidad (Fondos NextGeneration MRR). Las actuaciones están destinadas a mejorar la ciberseguridad en los sistemas de Atención Primaria (CiberAP) y se desarrollan en colaboración con los demás sistemas públicos de salud.

Los proyectos en que participa esta Conselleria están destinados a mejorar la seguridad de los puestos de trabajo (EDR para endpoints), y de los dispositivos de electromedicina, parcheado virtual de puestos de trabajo y servidores, control de acceso a cuentas privilegiadas (PAM), y herramienta GRC (gobierno, riesgo y cumplimiento). Las condiciones para hacer uso de estos fondos incluyen la finalización de las actuaciones antes de final de junio de 2026, aunque las previsiones de esta Conselleria pasan por finalizar su implantación en 2024, salvo de los equipos médicos, pendiente de los resultados de unas pruebas piloto, que lo estaría en el tercer trimestre de 2025.



Además de la captura de esta captura de imagen, tienen a su disposición abundante documentación oficial relativa al seguimiento de estos proyectos.

2. Alegación

Referencia

Apartado Conclusiones generales de TI, página 9, párrafo 5:

> Aunque existen trabajos en marcha relacionados con el cumplimiento del ENS, el índice actual de cumplimiento es muy bajo, existiendo los incumplimientos significativos que se señalan a continuación.

Contenido

Los valores de los indicadores son inferiores a los que resultan de las autoevaluaciones que realiza anualmente esta Conselleria siguiendo el formato de las encuestas para el informe INES, si bien es cierto que en ambos casos siguen sin alcanzar los niveles exigibles. Por eso el gran salto cualitativo que se espera de los planes de adecuación al ENS que ha emprendido la Conselleria, con una inversión prevista de .1.200.000€

La adecuación al ENS de los sistemas de una organización tan grande y compleja como esta Conselleria no es tarea fácil. Gran parte de los trabajos realizados hasta la fecha han servido para preparar (desarrollar y pilotar) una hoja de ruta viable. Para recorrer ese camino, la Conselleria ha preparado tres expedientes de contratación. Uno para la adecuación de los hospitales HACLE, en el que se utilizará el perfil de cumplimiento específico que ya pusimos a prueba en el Instituto de Investigaciones Sanitarias del Hospital La Fe. El segundo, para los departamentos de salud, en el que se utilizará el perfil de cumplimiento específico puesto a prueba en el ´departamento de salud Clínico-Malvarrosa. El tercer expediente, para los sistemas ubicados en el Centro de Informática de la Conselleria, que necesitará un cuarto expediente para la contratación de la

correspondiente certificación. La finalización de los tres primeros contratos está prevista para 2024. La metodología empleada en los dos primeros (perfiles de cumplimiento específicos) se ha desarrollado y puesto a punto en esta Conselleria con la colaboración del CCN y de los servicios públicos de salud de otras comunidades autónomas. En el V Encuentro del ENS organizado por el CCN en Madrid, en junio de este mismo año, tuvo lugar la presentación de esta metodología (véase la grabación aportada como evidencia).

Documentación justificativa

Grabación de la presentación de dos perfiles de cumplimiento específicos para facilitar la adecuación al ENS en el sector salud: https://www.youtube.com/watch?v=t4r_zN_GCgA

Los tres primeros expedientes de contratación indicados están en tramitación. El de los HACLE ya ha salido publicado y los otros dos lo serán de forma inminente. El cuarto, lógicamente, tendrá que esperar unos meses.

3. Alegación

Referencia

Apartado 3.2 Inventario de software, página 41

> Los sistemas operativos que soportan ORION LOGIS se encuentran dentro del periodo de soporte del fabricante. Sin embargo, el soporte de las bases de datos vence en un plazo breve, por lo que se debe planificar su actualización

Contenido

Las bases de datos del sistema Orión-Logis están en proceso de actualización a la última versión. Actualmente ya se han actualizado los entornos de BD de TEST, FOR y PRE y la BD de producción (PRO) está planificada su actualización el próximo 7 de diciembre del año en curso.

Documentación justificativa

Mensaje del servicio de atención a usuarios de la Conselleria de Sanitat (CATS) emitido con ocasión del anuncio de la próxima parada de servicio para la actualización de la BD

[redacted]
CENSURAT PER LA
SINDICATURA DE COMPTES

4. Alegación

Referencia

Apartado 4.1 Uso controlado de privilegios administrativos (D1-CBCS 4), pág 46,

> ORION LOGIS cuenta con distintos perfiles de usuarios en los distintos niveles de funcionalidades de administración requeridos. Existen 76 usuarios relacionados directamente con la administración del sistema, 29 de ellos no nominativos, lo que disminuye la trazabilidad de las acciones de estos usuarios

Contenido

Los usuarios no nominativos con capacidades de administración de Orión-Logis son usuarios internos del sistema, necesarios para la realización de funciones del núcleo de ejecución del programa. Cabe recordar que Orión-Logis es el nombre con el que se designa a la parametrización y personalización para la Conselleria de Sanitat de una suite de software ERP (Enterprise Resource Planning) comercial.

La problemática de dichos usuarios no nominativos ya se clarificó a través de las sucesivas reuniones mantenidas entre el equipo técnico de Orión-Logis y los auditores.

Documentación justificativa

La obtenida durante las citadas reuniones.

Consideración final

Sobre el conflicto entre transparencia y seguridad

Reconociendo la transparencia como una parte esencial del buen gobierno, así como el importante papel y la independencia de la Sindicatura de Comptes, dar publicidad a los aspectos donde esta Conselleria es vulnerable aumenta su superficie de exposición al riesgo y, en lugar de contribuir a mejorar la situación, la empeora gravemente. En este sentido, a pesar de lo indicado en el apartado Confidencialidad (pág. 3), consideramos excesivo el nivel de detalle del informe.

Por tanto, rogamos limiten el nivel de detalle en el informe público, evitando dar pistas a los posibles atacantes sobre las debilidades de control detectadas. Por otro lado, una mayor concreción es de agradecer en el informe interno en la media en que pueda servir para mejorar la situación.

Firmado electrónicamente por
JUAN MIGUEL SIGNES ANDREU - [redacted]
Oficina de Seguridad de la Información
24/11/2023 12:23:25

ANNEX II

Informe sobre les al·legacions presentades

ANÀLISI DE LES AL·LEGACIONS EFECTUADES A L'ESBORRANY DE L'INFORME D'AUDITORIA DE CIBERSEGURETAT I DELS CONTROLS GENERALS DE TECNOLOGIES DE LA INFORMACIÓ DE L'APLICACIÓ ORION LOGIS. EXERCICI 2022

S'han analitzat les al·legacions rebudes el 27 de novembre de 2023, respecte de les quals s'informa del que segueix:

Primera al·legació

Conclusió del paràgraf 4t de l'apartat 2, "CONCLUSIONS SOBRE ELS CONTROLS GENERALS DE TECNOLOGIES DE LA INFORMACIÓ"

Comentaris

La conclusió de l'informe assenyala:

> "La situació dels CGTI representa, per tant, un nivell de risc sobre la seguretat de la informació inacceptable i les deficiències existents no permeten confiar en el bon funcionament dels CPI, per la qual cosa l'entitat ha d'adoptar mesures per a reconduir la situació."

La Conselleria de Sanitat al·lega que té previst executar en un futur pròxim 4,5 milions d'euros en projectes per a millorar la ciberseguretat finançats pel Mecanisme de Recuperació i Resiliència de la Unió Europea amb l'objectiu de desenvolupar-los i finalitzar-los, en la major part dels casos, en 2024.

Les inversions en ciberseguretat milloraran els nivells de maduresa de la Conselleria, per la qual cosa considerem que la iniciativa va en la direcció correcta per a implantar les recomanacions incloses en l'Informe. L'al·legació no altera les nostres conclusions.

Conseqüències en l'Informe

No es modifica l'esborrany de l'Informe.

Segona al·legació

Primer paràgraf de l'apartat 3, "CONCLUSIONS SOBRE EL COMPLIMENT DE LA NORMATIVA EN MATÈRIA DE SEGURETAT DE LA INFORMACIÓ"

Comentaris

El paràgraf de l'Informe sobre el qual s'al·lega és el següent:

> "Encara que hi ha treballs en marxa relacionats amb el compliment de l'ENS, l'índex actual de compliment és molt baix, i hi ha els incompliments significatius que s'assenyalen a continuació."

La Conselleria de Sanitat al·lega que es produirà un salt qualitatiu quan s'executen els contractes previstos en acabar les actuacions que actualment continuen en marxa en aquesta matèria.

Durant el treball de camp hem observat (i inclòs en el nostre informe) les actuacions iniciades per a donar compliment a la normativa en matèria de seguretat de la informació. Considerem que la finalització d'aquestes accions juntament amb l'execució de les contractacions previstes va en la direcció correcta per a complir la normativa. L'al·legació no altera les nostres conclusions.

Conseqüències en l'Informe

No es modifica l'esborrany del Informe.

Tercera al·legació

Apèndix 3, últim paràgraf de l'apartat "3.2. Inventari de programari (C1-CBCS 2)"

Comentaris

S'ha eliminat tot l'apartat. Vegeu la cinquena al·legació.

Quarta al·legació

Apèndix 3, apartat "4.1. Ús controlat de privilegis administratius (D1-CBCS 4)"

Comentaris

S'ha eliminat tot l'apartat. Vegeu la cinquena al·legació.

Cinquena al·legació

Consideració final afegida per la Conselleria en les seues al·legacions

La Conselleria de Sanitat ha afegit al seu informe d'al·legacions l'observació següent: "donar publicitat als aspectes en què aquesta conselleria és vulnerable augmenta la seua superfície d'exposició al risc i, en lloc de contribuir a millorar la situació, l'empitjora greument". A més, sol·liciten limitar "el nivell de detall en l'informe públic per a evitar donar pistes als possibles atacants sobre les debilitats de control detectades" i "una major concreció en l'informe intern".

Comentaris

La informació tractada durant les auditories de ciberseguretat està relacionada amb la seguretat dels sistemes d'informació de les entitats, per la qual cosa la Sindicatura de

Comptes, conscient de la sensibilitat d'aquesta informació, revisa sempre exhaustivament que la informació publicada en els informes no supose un risc addicional per a l'entitat fiscalitzada.

Hem revisat novament l'esborrany d'informe i no hem trobat informació concreta que puga ser utilitzada per a vulnerar cap dels sistemes auditats, tenint en compte que no inclou informació detallada dels sistemes ni de les mesures de seguretat implantades en ORION LOGIS.

No obstant això, atesa la sensibilitat dels sistemes d'informació sanitaris i a fi de reduir el risc addicional a zero, els resultats detallats que s'incloïen en els apartats 3 i 4 de l'apèndix 3 s'eliminen de l'Informe i es comuniquen amb caràcter confidencial als responsables de la Conselleria perquè puguen adoptar les mesures correctores necessàries.

Conseqüències en l'Informe

S'elimina el contingut dels apartats 3 i 4 de l'apèndix 3 i s'afegeix un comentari, i queden redactats així:

> **"3. Operacions dels sistemes d'informació**
>
> Apartat eliminat en la fase d'al·legacions.
>
> **4. Controls d'accés a dades i programes**
>
> Apartat eliminat en la fase d'al·legacions.
>
> Atesa la sensibilitat dels sistemes d'informació sanitaris i de la informació tractada, i a fi de reduir a zero el risc addicional en la seguretat d'aquests sistemes, derivat d'un possible mal ús del nostre informe, els resultats detallats que s'incloïen en els apartats 3 i 4 de l'apèndix 3 s'han eliminat en la fase d'al·legacions i es comuniquen amb caràcter confidencial als responsables de la Conselleria perquè puguen adoptar les mesures correctores necessàries."

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Auditoria ciberseguretat ORION LOGIS_2022_val - SEFYCU 4681416

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 JLQ7 4V2K AFLQ RQYH

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 - 18/12/2023 8:02 VICENT CUCARELLA TORMO