SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

AUDITORÍA DE CIBERSEGURIDAD Y DE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA APLICACIÓN ORION LOGIS

Ejercicio 2022

RESUMEN

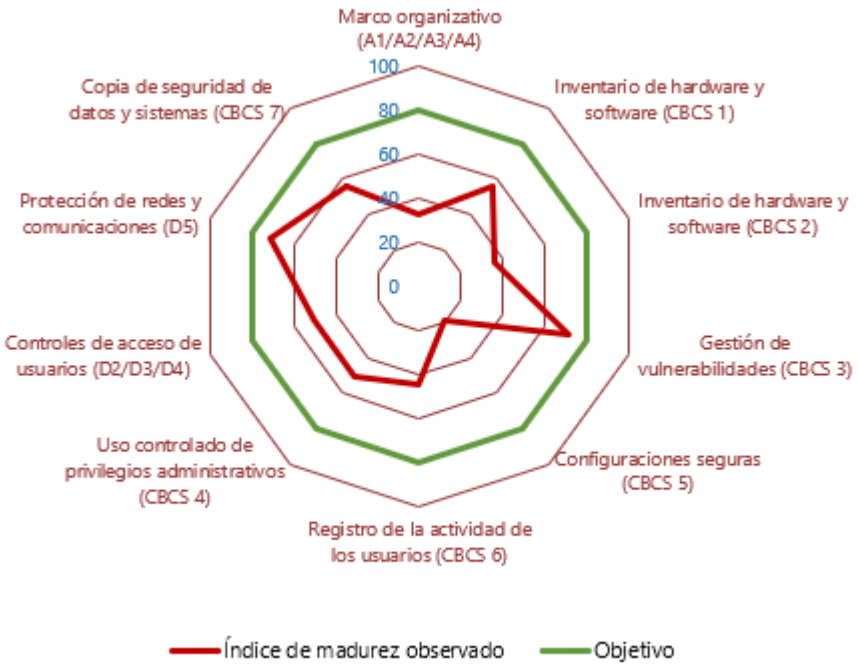
La Sindicatura de Comptes, de forma simultánea a la realización de la **auditoría del control interno y de los sistemas de información de las compras sanitarias**, ha llevado a cabo una auditoría de ciberseguridad y de los controles generales de tecnologías de la información (CGTI) relacionados con la aplicación ORION LOGIS, que proporciona soporte a los procesos de compras de bienes y servicios de la Conselleria de Sanidad.

Las principales **conclusiones** han sido:

- El índice de madurez de los CGTI relacionados con ORION LOGIS es muy deficiente y no aporta un nivel de confianza razonable para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de las transacciones y los datos.

  Hemos llegado a la conclusión de que el índice de madurez conjunto de esos controles es del 48,7%, inferior al 80% requerido por el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, que requiere a las administraciones con la categoría de seguridad de los sistemas revisados ese nivel mínimo de madurez.

  El detalle del nivel de madurez de cada grupo de controles se muestra en el gráfico siguiente.



- 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 controles de procesamiento de información (CPI), por lo que la entidad debe adoptar medidas para reconducir la situación.

- La Conselleria de Sanidad no tiene establecida una adecuada gobernanza de la ciberseguridad, que es el elemento clave para llegar al objetivo de garantizar la seguridad y buen funcionamiento de los sistemas de información, y esto es responsabilidad de los órganos superiores de la Conselleria. Además, se debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

- Las deficiencias en los controles señaladas en el informe especial de 2016 persisten.

La revisión del **cumplimiento normativo** en materia de seguridad de la información ha puesto de manifiesto las siguientes incidencias:

- 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 detallan en nuestro informe.

- No se ha elaborado el plan de adecuación al Esquema Nacional de Interoperabilidad.

- Existen aspectos pendientes de cumplimiento de la normativa de protección de datos personales.

En el informe realizamos varias **recomendaciones** tendentes a subsanar las deficiencias observadas en materia de ciberseguridad. De entre ellas destacamos las relacionadas con mejorar la capacidad de recuperación de los sistemas ante posibles desastres o ciberataques mediante sistemas de alta disponibilidad redundados en diferentes ubicaciones y una adecuada gestión de las copias de seguridad.

NOTA

Este resumen pretende ayudar a comprender los resultados de nuestro informe y facilitar el trabajo a los lectores y a los medios de comunicación. Recomendamos la lectura del informe completo para conocer el verdadero alcance del trabajo realizado.

Auditoría de ciberseguridad y de los controles generales de tecnologías de la información de la aplicación ORION LOGIS

Ejercicio 2022

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Antecedentes

En términos presupuestarios, las obligaciones reconocidas en 2022 del capítulo 2, "Compras de bienes corrientes y gastos de funcionamiento", de la Conselleria de Sanidad Universal y Salud Pública (CSUSP), a partir del 25 de julio de 2023 denominada Conselleria de Sanidad, ascienden a 2.732,4 millones de euros. Es decir, representan un 74,8% de los 3.655,7 millones de euros correspondientes a dicho capítulo en el conjunto de la Cuenta de la Administración.

La gestión de las compras de la Conselleria se realiza de forma descentralizada, a través de los centros gestores de compras en los 24 departamentos sanitarios en que se divide el territorio de la Comunitat Valenciana, y también en los servicios centrales. Esta gestión está soportada por la aplicación informática ORION LOGIS. En el apéndice 1 se detallan las características y funcionalidades de esta aplicación.

Los siguientes datos relacionados con la aplicación ORION LOGIS ponen de relieve su importancia en la gestión de la Conselleria y su evolución desde los anteriores informes especiales realizados por la Sindicatura:

Cuadro 1. Datos básicos de ORION LOGIS

	2013	2016	2022
Número de usuarios	6.372	7.472	8.737
Número de facturas	415.011	531.244	730.841
Número de artículos	90.635	124.935	170.445
Número de proveedores	4.675	5.595	6.237

La Conselleria de Sanidad y sus departamentos de salud han tramitado en 2022 a través de la aplicación ORION LOGIS facturas correspondientes tanto a gastos presupuestarios del capítulo 2 como gastos contabilizados en los capítulos 4, "Transferencias corrientes", y 6, "Inversiones reales".

Por qué realizamos esta auditoría

Las razones para realizar una auditoría sobre la eficacia de los controles existentes en los sistemas de información que soportan la gestión de las compras sanitarias son:

a) Estos gastos son un área muy significativa en el conjunto de la Cuenta de la Administración de la Generalitat, ya que representan el 74,8% de las obligaciones reconocidas del presupuesto del capítulo 2.

b) Los controles generales de tecnologías de la información (**CGTI**) deben garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos. Además, su ineficacia o mal funcionamiento impediría confiar en los controles de procesamiento de la información (**CPI**).

c) Los CPI deben garantizar la completitud, exactitud, validez y legalidad de las transacciones relacionadas con la compra de bienes y servicios sanitarios, que se gestionan con la aplicación ORION LOGIS. Los resultados de la auditoría de estos controles se recogen en el informe de *Auditoría del control interno y de los sistemas de información de las compras sanitarias* del ejercicio 2022 de la Sindicatura de Comptes.

d) Los CGTI son muy importantes, ya que en los últimos años el sector de la salud se ha convertido en un objetivo preferente de los ciberdelincuentes, y unos sólidos CGTI representan la defensa más eficaz frente a las ciberamenazas en un entorno que se sustenta en sistemas de información intensamente interconectados[1].

e) Finalmente, los controles de seguridad de la información, básicamente los CGTI, son de obligado cumplimiento en virtud de distinta normativa, especialmente por el Esquema Nacional de Seguridad (ENS).

Objetivos de la auditoría

El objetivo de esta auditoría ha sido verificar el grado de eficacia de los CGTI, que garantizan el correcto funcionamiento de la aplicación ORION LOGIS, y ha incluido las siguientes tareas:

- Conocer el entorno tecnológico de los sistemas que dan soporte a ORION LOGIS, identificando los riesgos principales relacionados con la seguridad de la información y los controles existentes para mitigarlos.

- Revisar y concluir sobre el diseño, implementación y la eficacia operativa de los CGTI existentes en, o relacionados con, el sistema ORION LOGIS y si, en consecuencia, aportan un nivel de confianza razonable para:

  a) garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de las transacciones y los datos, y

  b) servir de fundamento para el buen funcionamiento de los CPI.

- Revisar el cumplimiento de la normativa sobre seguridad de los sistemas de información.

[1] En el reciente informe ENISA Threat Landscape: Health Sector, de julio de 2023 de la European Union Agency for Cybersecurity, se destaca que durante 2021-2022 el sector sanitario europeo ha debido hacer frente a un creciente número de ciberataques, generalizados, y señala que España es el segundo país de Europa en cuanto a ciberincidentes de seguridad comunicados.

Alcance

La presente auditoría se ha centrado en el análisis de la situación de los CGTI relacionados con la aplicación ORION LOGIS, que proporciona soporte a los procesos de compras de bienes y servicios de la Conselleria de Sanidad.

Aunque muchos de los CGTI afectan al conjunto de sistemas de información, la revisión se ha focalizado en los controles relacionados con:

1. la aplicación ORION LOGIS,

2. la base de datos subyacente,

3. los sistemas operativos instalados en los sistemas que integran la aplicación de gestión (servidor web, servidor de aplicación, servidor de base de datos).

Además, por su importancia para el buen funcionamiento de los sistemas de información y la ciberseguridad, se han analizado los siguientes tipos de elementos:

4. elementos de la red de comunicaciones (punto de acceso a red de gestión),

5. elementos de seguridad (*firewall*, servidores de autenticación).

En total hemos revisado 51 controles detallados, agrupados en los 10 controles principales señalados en el cuadro 2, considerados relevantes para el proceso de gestión de compras.

El periodo revisado ha abarcado desde el 1 de enero de 2022 hasta el 30 de septiembre de 2023, fecha a la que se refiere la situación de los indicadores del índice de madurez.

Metodología

La metodología utilizada en la presente auditoría está basada en las guías prácticas de fiscalización GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad" y GPF-OCEX 5330, "Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica", que forman parte del *Manual de fiscalización* de la Sindicatura de Comptes y que pueden consultarse en nuestra web.

Evaluamos la situación de los controles utilizando el modelo de nivel de madurez de los procesos, ya que, además de ser un sistema ampliamente aceptado, permite establecer objetivos y realizar comparaciones entre entidades distintas y ver la evolución a lo largo del tiempo. La metodología utilizada está plenamente alineada con lo establecido por el ENS.

Para mayor detalle sobre la metodología utilizada nos remitimos al apéndice 2.

Confidencialidad

Dado que la información utilizada en la auditoría tiene un carácter sensible y puede afectar a la seguridad de los sistemas de información, los resultados detallados de cada uno de los controles revisados solo se comunican con carácter confidencial a los responsables de la Conselleria de Sanidad para que puedan adoptar las medidas correctoras que consideren precisas. En el presente informe los resultados se muestran de forma sintética.

2. CONCLUSIONES SOBRE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE LA INFORMACIÓN

El índice de madurez de los CGTI relacionados con ORION LOGIS es muy deficiente y no aporta un nivel de confianza razonable para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de las transacciones y los datos.

Como resultado del trabajo realizado cabe concluir que el grado de control existente en la gestión de los CGTI revisados relacionados con ORION LOGIS alcanza un **índice de madurez medio del 48,7%**, que se corresponde con un nivel de madurez ***N1, inicial/ad hoc***; es decir, el proceso existe, pero no se gestiona o su gestión no está correctamente organizada.

Este resultado está muy alejado del nivel exigido por el ENS para los sistemas con una categoría de seguridad MEDIA[2], que es el nivel N3 y un índice de madurez del 80%.

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.

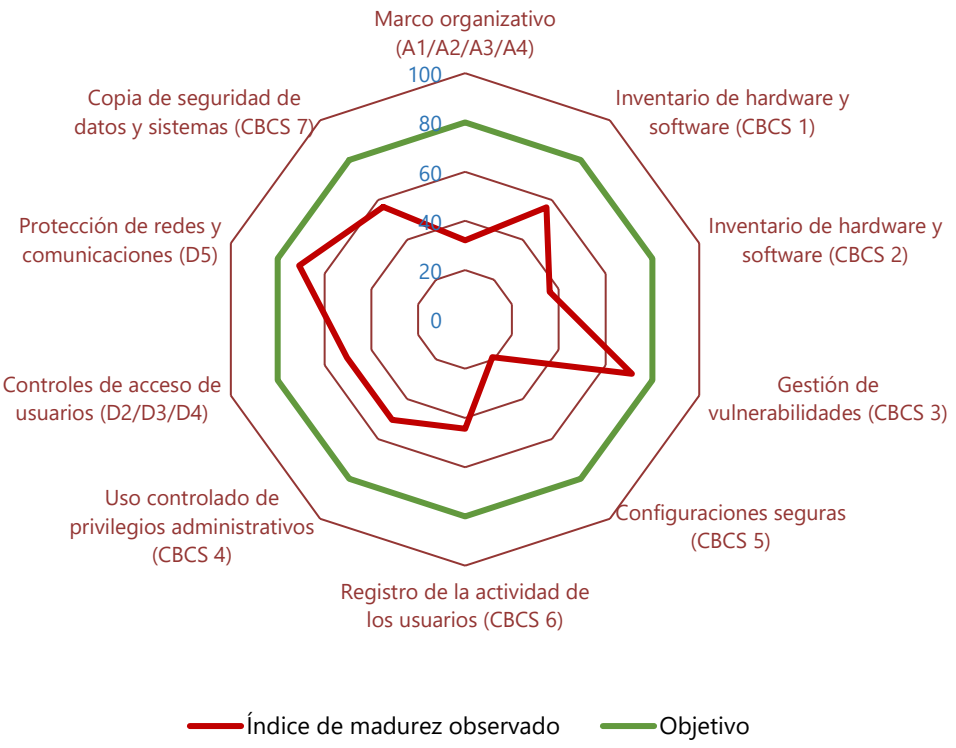
En total hemos revisado 51 controles detallados, agrupados en los 10 controles principales que se muestran en el cuadro 2 y visualizan en el gráfico 1, relacionados con la aplicación ORION LOGIS. En estos están incluidos los ocho controles básicos de ciberseguridad de la metodología de la Sindicatura basada en la GPF-OCEX 5313 (véase apéndice 2).

[2] Aunque lo exige el ENS, no hemos obtenido evidencia de la clasificación del sistema ORION LOGIS por parte de la Conselleria (alto, medio o bajo). Hemos considerado que debe clasificarse como de categoría de seguridad MEDIA, que es la más habitual en los sistemas que soportan procesos de gestión administrativa.

Cuadro 2. Índice de madurez de los CGTI

Área		Control	Índice de madurez	Nivel de madurez
A. Marco organizativo	A1/A2/ A3/A4	Marco organizativo y gobernanza de la ciberseguridad (CBCS 8)	32,1%	N1
C. Operaciones de los sistemas de información	C1H	Inventario de *hardware* (CBCS 1)	56,3%	N2
	C1S	Inventario de *software* (CBCS 2)	36,2%	N1
	C2	Gestión de vulnerabilidades (CBCS 3)	71,3%	N2
	C3	Configuraciones seguras (CBCS 5)	19,0%	N1
	C4	Registro de la actividad de los usuarios (CBCS 6)	44,4%	N1
D. Controles de acceso a datos y programas	D1	Uso controlado de privilegios administrativos (CBCS 4)	50,4%	N2
	D2/D3/D4	Controles de acceso a usuarios	50,4%	N2
	D5	Protección de redes y comunicaciones	70,8%	N2
E. Continuidad del servicio	E1	Copia de seguridad de datos y sistemas (CBCS 7)	56,5%	N2
General			48,7%	N1

Gráfico 1. Índice de madurez de los CGTI revisados



La mayoría de los grupos de controles tienen un índice de madurez muy alejado de lo requerido por el ENS (80,0% y N3) y de lo que se espera de un sólido sistema de control interno, lo que representa un riesgo significativo para la seguridad de los sistemas de información de la Conselleria.

Las deficiencias significativas en los CGTI observadas se comentan con detalle en el apéndice 3. En el apartado 6 se realizan las recomendaciones pertinentes para reconducir la situación y alcanzar los niveles exigidos por el ENS para la protección de los sistemas de información.

El periodo revisado ha sido el ejercicio 2022 y el trabajo de campo ha finalizado en septiembre de 2023, fecha a la que se refiere la situación de los controles.

La Conselleria de Sanidad no tiene establecida una adecuada gobernanza de la ciberseguridad. Además, se debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

Los órganos superiores de la Conselleria son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

Si bien hemos podido verificar la existencia de cierto nivel de compromiso y concienciación con la ciberseguridad, existen carencias relevantes detalladas en el apéndice 3 que impiden que la gobernanza pueda considerarse efectiva.

En este sentido, consideramos que la gobernanza de la ciberseguridad implementada por los órganos de dirección de la Conselleria es claramente insuficiente para garantizar el cumplimiento de la normativa relacionada con la seguridad de la información y para que los controles relacionados con las TI alcancen los niveles de madurez requeridos por el ENS.

Es necesario, por tanto, solventar de forma urgente las carencias identificadas, que tienen un impacto negativo en el nivel de seguridad de la información de la Conselleria, y atender las recomendaciones efectuadas en el presente informe.

Las deficiencias de control interno señaladas en el informe especial de 2016 persisten.

Dada la importancia que tiene esta área en la fiscalización de la Cuenta de la Administración de la Generalitat, la Sindicatura realizó en 2013 y en 2016 sendos informes de auditoría especiales sobre los sistemas de información en los que se analizó la eficacia de los CGTI del sistema de información que soporta ORION LOGIS, que pueden consultarse en la página web de la Sindicatura. En el presente informe se ha realizado un seguimiento de las deficiencias de CGTI incluidas en el último de esos informes.

La primera conclusión general sobre la ineficacia de los CGTI es básicamente coincidente con las de los informes de 2013 y 2016. Como se verá después, la mayoría de las recomendaciones efectuadas en el informe de 2016 no han sido atendidas.

Debido a la elevada significatividad de las debilidades de control observadas, los órganos de gobierno de la Conselleria deben comprometerse de manera clara y decidida a subsanarlas.

No se nos ha facilitado a tiempo la cumplimentación de un cuestionario solicitado sobre los controles revisados, lo que ha dificultado el análisis de las evidencias obtenidas, aunque consideramos que no afecta a las conclusiones de nuestro trabajo. Tampoco se nos ha facilitado la información solicitada sobre el personal de la Subdirección General de Sistemas de Información para la Salud.

3. CONCLUSIONES SOBRE EL CUMPLIMIENTO DE LA NORMATIVA EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

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.

La Conselleria de Sanidad está sujeta al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, sustituido en 2022 por el Real Decreto 311/2022 de 8 de mayo.

La Orden 9/2012, de 10 de julio, de la Conselleria de Sanidad, establece la organización de la seguridad de la información. De acuerdo con esta norma, la Conselleria, con el apoyo de la Dirección General de las Tecnologías de la Información y de la Comunicación (DGTIC), es responsable de la seguridad de sus sistemas de información.

La Conselleria se encuentra trabajando en un proyecto de adecuación de los distintos departamentos de salud al ENS. Mediante un contrato se han elaborado perfiles de cumplimiento específicos para facilitar la implantación del ENS en los departamentos.

A fecha del presente informe, uno de los organismos pertenecientes a la Conselleria ya ha obtenido el certificado de conformidad para categoría "BÁSICA" y se prevé la aplicación de dicho perfil de cumplimiento a otros organismos.

La Conselleria ha presentado el informe sobre el estado de la seguridad de los sistemas de información de 2022 al Centro Criptológico Nacional (CCN), de acuerdo con lo previsto en la Instrucción Técnica de Seguridad regulada por la Resolución de 7 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas.

Aunque se han realizado determinadas acciones para dar cumplimiento al ENS, durante el trabajo realizado se han puesto de manifiesto los siguientes incumplimientos significativos:

- No se ha nombrado al responsable del servicio de los sistemas de información previsto en el ENS y en el Decreto 130/2012 del Consell.
- El comité de seguridad de la información de la Conselleria de Sanidad, que es un elemento esencial de la gobernanza de la ciberseguridad, no tiene un funcionamiento efectivo, ya que solo se ha reunido una vez en 2022.
- Algunos roles de seguridad establecidos en la Orden 9/2012 se definen en base a normativa de protección de datos que ya no se encuentra en vigor.
- No se han nombrado todos los roles de seguridad de los elementos descentralizados de la organización previstos en la Orden 9/2012.
- No se ha aprobado la clasificación de seguridad de sus sistemas de información, ni la declaración de aplicabilidad que requiere el artículo 28 del ENS.
- No se han realizado las auditorías previstas en el artículo 31 del ENS ni, en consecuencia, se han publicado en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la antes citada Instrucción Técnica de Seguridad.

Por otra parte, el índice de madurez de los CGTI visto en el apartado anterior, del 48,7%, refleja el bajo grado de cumplimiento de las medidas de seguridad establecidas con carácter obligatorio por el ENS. Esta norma requiere para los sistemas de información de nivel medio, un índice de madurez *N3, proceso definido*, que exige una puntuación mínima del 80,0%.

No se ha elaborado el plan de adecuación al Esquema Nacional de Interoperabilidad (ENI)

No se ha elaborado el plan de adecuación al ENI que exige el Real Decreto 4/2010. ORION LOGIS no está adaptada a la generación de expedientes de conformidad con el ENI.

Existen aspectos pendientes de cumplimiento de la normativa de protección de datos personales

La Conselleria tiene publicada en su web la relación de actividades de tratamiento.

El delegado de protección de datos (DPD) nombrado por la Generalitat tiene competencias sobre la actividad de la Conselleria de Sanidad. Sin embargo, no se ha cubierto un puesto de trabajo existente en el departamento del DPD para atender las necesidades de la Conselleria de Sanidad.

Durante el trabajo de campo, hemos observado deficiencias relacionadas con la protección de datos personales, como el envío de información con este tipo de datos sin cifrar y por medio de canales no seguros.

No se han realizado auditorías de protección de datos personales.

4. RESPONSABILIDAD DE LOS ÓRGANOS SUPERIORES Y DE DIRECCIÓN DE LA CONSELLERIA DE SANIDAD EN RELACIÓN CON LOS CONTROLES DE SEGURIDAD

La gestión de las aplicaciones y los sistemas informáticos que soportan la gestión de las compras de bienes y servicios para las instituciones sanitarias le correspondía en 2022 a la Dirección General de Planificación, Eficiencia Tecnológica y Atención al Paciente, dependiente de la Secretaría Autonómica de Eficiencia y Tecnología Sanitaria, en la que se integra la Subdirección General de Sistemas de Información para la Salud (SDGSIS).

Desde el 25 de julio de 2023, fecha de entrada en vigor del Decreto 112/2023, de 25 de julio, del Consell, se establece como órgano responsable a la Dirección General de Información Sanitaria, Calidad y Evaluación, encuadrada en la Secretaría Autonómica de Planificación, Información y Transformación Digital de la Conselleria de Sanidad.

Los principales responsables en materia de seguridad de la información, según el ENS y según la Orden 9/2012, de 10 de julio, de la Conselleria de Sanidad, por la que establece la organización de la seguridad de la información, son los siguientes:

- Responsable de la información: el conseller de Sanidad

- Comité de Seguridad de la Información, cuya composición se establece en el artículo 10 de la Orden 9/2012.

- Responsable del Servicio, que no ha sido formalmente nombrado. El artículo 12 de la Orden 9/2012 atribuye sus funciones a los responsables funcionales. En compras sanitarias correspondía esta responsabilidad a la Subdirección General de Contratación y Central de Compras.

- Responsable de seguridad: la persona responsable de la Oficina de Seguridad de la Información nombrada por el conseller.

- Responsable del sistema, que no ha sido formalmente nombrado. La Orden 3/2022, de la Conselleria de Sanidad y Salud Pública, por la que se desarrolla el Decreto 185/2020, del Consell, de aprobación del Reglamento Orgánico y Funcional de la Conselleria, atribuía sus funciones al jefe del Servicio de Infraestructuras de Tecnologías de la Información y la Comunicación.

5. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

Nuestro objetivo es obtener una seguridad limitada y concluir sobre la situación de los controles generales de tecnologías de la información revisados de la Conselleria de Sanidad, proporcionando una evaluación sobre su diseño y eficacia operativa, sobre el cumplimiento de la normativa básica relativa a la seguridad de la información y, en su caso, formular recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control.

Nos hemos centrado, principalmente, en el análisis de la situación de los CGTI relacionados con la aplicación ORION LOGIS de gestión de compras, si bien hay aspectos que son de aplicación general a todos los sistemas de la Conselleria.

Para ello, hemos llevado a cabo el trabajo de conformidad con los *Principios fundamentales de fiscalización de las instituciones públicas de control externo* y con las normas técnicas de fiscalización aprobadas por el Consell de la Sindicatura, recogidas en el *Manual de fiscalización* de la Sindicatura de Comptes. En particular, hemos seguido la metodología establecida en las guías prácticas de fiscalización GPF-OCEX 5330, "Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica", y GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad". Dichos principios exigen que cumplamos los requerimientos de ética, así como que planifiquemos y ejecutemos la auditoría con el fin de obtener una seguridad limitada sobre la situación de los CGTI revisados.

Dadas las especiales características del trabajo a realizar sobre los sistemas de información, este se ha efectuado por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI) en coordinación con el equipo de auditoría que fiscaliza la Cuenta de la Administración de la Generalitat, que ha emitido un informe especial sobre el control interno en la gestión de compras sanitarias.

Consideramos que la evidencia de auditoría obtenida proporciona una base suficiente y adecuada para fundamentar nuestras conclusiones sobre el estado de los CGTI revisados, de acuerdo con el alcance limitado que se ha señalado.

Los procedimientos realizados en una auditoría de seguridad limitada son reducidos en comparación con los que se requieren para obtener una seguridad razonable, pero se espera que el nivel de seguridad sea, conforme al juicio profesional del auditor, significativo para los destinatarios del informe.

Como parte de una auditoría de conformidad con la normativa reguladora de la actividad de los órganos de control externo, aplicamos nuestro juicio profesional y mantenemos una actitud de escepticismo profesional durante toda la auditoría.

Asimismo, ofrecemos propuestas correctoras a las deficiencias encontradas en el curso de la auditoría, para lo que se formulan las pertinentes recomendaciones que contribuyan a incrementar la eficacia del sistema de control interno y la eficiencia de los procesos de gestión.

También se ha efectuado un seguimiento de las deficiencias de control interno y de las recomendaciones realizadas en el informe *Auditoría de los controles generales de tecnologías de la información de la aplicación ORION LOGIS* del ejercicio 2016.

Nos comunicamos con el órgano de gobierno de la entidad en relación con, entre otras cuestiones, el alcance y el momento de realización de la auditoría planificados y los hallazgos significativos de la auditoría, así como cualquier otro aspecto significativo que identificamos en el transcurso de la auditoría.

6. RECOMENDACIONES PARA SUBSANAR LAS DEFICIENCIAS EN LOS CGTI Y MEDIDAS A ADOPTAR PARA EL CUMPLIMIENTO DE LA LEGALIDAD

Para subsanar las deficiencias identificadas por la Sindicatura en la presente auditoría y mejorar los niveles de control señalados en el apartado 2 anterior, formulamos las recomendaciones que siguen. Los órganos de dirección de la Conselleria de Sanidad deberán dedicar los esfuerzos y recursos necesarios para subsanar dichas deficiencias.

También se señalan las medidas que deben adoptarse para el cumplimiento de la legalidad.

Recomendaciones dirigidas a la Secretaría Autonómica de Planificación, Información y Transformación Digital

Estas recomendaciones son aplicables a todos los sistemas de información de la Conselleria, no solo a ORION LOGIS.

Sobre el inventario de *hardware*

1. Recomendamos actualizar el procedimiento existente para el inventariado de *hardware* de manera que, además de las acciones y controles actualmente implantados, contemple la identificación del responsable de cada activo, las altas, bajas y actualizaciones de dispositivos en el inventario, las revisiones periódicas del *hardware* y las medidas implantadas para impedir el acceso a la red de dispositivos no autorizados y su alcance, así como los controles sobre las memorias USB.

Sobre el inventario de *software*

2. Recomendamos elaborar e implantar un procedimiento de gestión de todo el *software* instalado en los sistemas de la Conselleria. Deberá incluir la autorización de las instalaciones, la lista del *software* autorizado (lista blanca), las medidas técnicas que impidan la ejecución del no autorizado, revisiones periódicas y la forma de documentar dichas revisiones, un plan de mantenimiento que considere de manera integral el proceso de gestión del soporte de todo el *software* utilizado y la forma de identificar y actualizar todos los sistemas que están fuera del período de soporte.

Sobre la gestión de vulnerabilidades

3. Recomendamos actualizar y aprobar formalmente el procedimiento para la identificación y resolución de vulnerabilidades. Debe incluir todas las acciones llevadas a cabo por los distintos departamentos de la SDGSIS. Además, debe contemplar su gestión proactiva, incluyendo tanto un análisis previo a la entrada en producción de los sistemas como la identificación de vulnerabilidades mediante el uso herramientas de escaneo o pruebas de penetración.

Sobre configuraciones seguras de *hardware* y *software*

4. Recomendamos aprobar e implantar un procedimiento de configuración segura o bastionado y la gestión continua de los sistemas que considere los principios de la seguridad por defecto y mínimo privilegio. Dicho procedimiento debe contemplar la gestión de cambios en los sistemas y la monitorización y revisión periódica de los cambios no autorizados. También debe contemplar la utilización de guías de instalación específicas por sistemas, basadas en las recomendaciones de los fabricantes y en las recomendaciones de los organismos de referencia, tales como las guías de seguridad STIC de las series 400, 500 y 600 del CCN.

Sobre registro de la actividad de los usuarios

5. Recomendamos aprobar formalmente e implantar un procedimiento para el tratamiento de los registros de auditoría de actividad de los usuarios que contemple, como mínimo, los sistemas afectados, la información que se debe almacenar, el periodo de retención, los mecanismos de protección, la gestión de derechos de acceso a los registros y la revisión de esa actividad. Para su aplicación efectiva, se debería implantar alguna herramienta analítica de correlación de registros, que permita la detección de comportamientos anómalos y detección de eventos de seguridad en base a la información proporcionada por el conjunto de sistemas de la Conselleria.

Sobre el uso controlado de privilegios administrativos

6. Aprobar formalmente un procedimiento de gestión de usuarios con privilegios de administración en todos los sistemas de información de la Conselleria, que incluya su regulación detallada, y contemple:

    - el inventario de cuentas administrativas y su revisión periódica,
    - el deshabilitado o la eliminación de las cuentas no utilizadas que no sean necesarias,
    - la eliminación de todos los usuarios no nominativos y
    - la política de autenticación con los refuerzos previstos en el ENS.

Cuando existan razones de índole técnica que impidan la eliminación de usuarios genéricos, su uso deberá estar controlado de forma que se mantenga el principio de trazabilidad de las acciones en los sistemas.

Sobre la gestión de los accesos de los usuarios

7. Elaborar y aprobar un procedimiento de gestión de usuarios para todos los sistemas de la Conselleria en el que se regule la tramitación de las altas, bajas y modificación de los usuarios de los sistemas de información y el procedimiento para aprobar esos usuarios y para comunicarlo a la SDGSIS. En este procedimiento debe quedar establecido las personas que deben aprobar las altas, bajas y modificación de estos usuarios, así como un proceso de revisión periódico de los usuarios que garantice el principio de autorización y mínimo privilegio (artículos 17 y 20 del ENS). Esta revisión debe incluir al personal de empresas subcontratadas y la revisión de la vigencia de los contratos laborales en esas empresas.

   El procedimiento debería contemplar la obligación, por parte del departamento de personal o de los departamentos funcionales, de la comunicación de las bajas de personal o cambios de centro y/o responsabilidades a los responsables de los sistemas de información encargados de aplicar las altas y modificaciones de usuarios.

8. Elaborar y aprobar un procedimiento de seguridad que regule la forma de creación de identificadores de usuarios de los sistemas y los parámetros de autenticación para esos identificadores en cada sistema.

   El procedimiento debería desarrollar los parámetros de seguridad en la autenticación y aplicarlos a todos los usuarios y sistemas, de manera que las contraseñas incluyan un buen nivel de complejidad, caducidad, bloqueos ante intentos fallidos, de acuerdo con las buenas prácticas y el ENS. Para los sistemas de nivel medio y alto deberían establecerse los refuerzos en la autenticación exigidos por el ENS.

Sobre la protección de las redes y comunicaciones

9. Aprobar un procedimiento y fortalecer los mecanismos de control de la seguridad en los dispositivos que se conectan por VPN y no están gestionados por la Conselleria, de manera que únicamente puedan conectarse si cuentan con el nivel de seguridad adecuado. También recomendamos deshabilitar las conexiones VPN innecesarias o no utilizadas durante un periodo determinado y realizar un seguimiento de la gestión realizada por parte de los departamentos de salud sobre esas conexiones no utilizadas.

Sobre las copias de seguridad y la continuidad del servicio

10. Actualizar el procedimiento para la gestión de copias de seguridad de datos y sistemas, que contemple todos los requisitos exigidos por el ENS.

11. Implementar sistemas de alta disponibilidad en los sistemas críticos gestionados por la Conselleria con un nivel adicional de protección de estos sistemas, con copias en

tiempo real en distintas ubicaciones que estén suficientemente separadas físicamente para mitigar los riesgos en caso de catástrofes.

12. Recomendamos que el plan de continuidad se apruebe por el máximo nivel directivo de la Conselleria. El plan debe definir concretamente aspectos como las ubicaciones o el *hardware* alternativo a utilizar en caso de incidente grave, así como plazos de recuperación realistas.

Recomendaciones sobre la gobernanza de la seguridad de la información y el ENS, dirigidas a los órganos superiores de la Conselleria

13. Los órganos superiores de la Conselleria deben adoptar con urgencia las medidas necesarias para implantar una adecuada gobernanza sobre las tecnologías de la información y la ciberseguridad, acordes con lo dispuesto por el ENS y con la política de seguridad de la información de la Generalitat, establecida en el Decreto 66/2012 del Consell, y resolver los incumplimientos señalados en el apartado 3 del Informe.

    Estas medidas deben basarse en un liderazgo efectivo por parte de los órganos superiores de la Conselleria de Sanidad que proporcione las directrices y los recursos económicos y personales necesarios para su efectiva implantación. Incluirían entre otras cuestiones:

    - La Conselleria debe elaborar un plan de adecuación al ENS, implantar las medidas incluidas en dicho plan y realizar las auditorías de seguridad legalmente obligatorias.

    - Actualizar la Orden 9/2012, de 10 de julio, por la que se establece la organización de la seguridad de la información de la Conselleria para adaptarla al actual ENS, así como eliminar y/o actualizar las referencias a la normativa que ya no esté en vigor.

    - Desarrollar la política de seguridad de la Generalitat mediante normas y procedimientos de seguridad debidamente aprobados, tal como requiere el ENS, específicos para el ámbito de la Conselleria. Estas normas y procedimientos deberían comunicarse a los responsables de su aplicación y estar disponibles en algún repositorio actualizado y accesible para esos responsables. Esto incluye actualizar y aprobar los procedimientos ya existentes.

    - Elaborar y aprobar un Plan estratégico para los sistemas de información de la Conselleria que se integre en la planificación general de las TIC de la Generalitat y que garantice la existencia de unos sistemas de información orientados a la consecución de los objetivos de la Conselleria. Esta planificación estratégica debe concretarse anualmente en planes de proyectos que a su vez deben contar con la presupuestación anual y/o plurianual necesaria para llevarlos a cabo. Se debe asegurar la disponibilidad de los medios personales necesarios para su adecuada ejecución.

- Desarrollar y aprobar un plan de formación sobre seguridad de la información para el personal de la Conselleria, sin perjuicio de que se puedan aprovechar recursos de la Generalitat para desarrollarlos. La Conselleria debe realizar el seguimiento del grado de ejecución de estos planes.

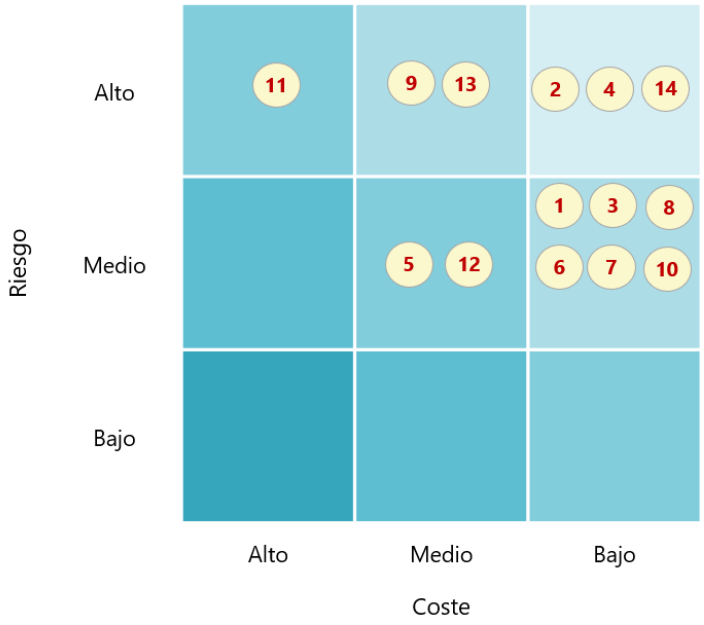
Sobre la normativa de protección de datos personales, dirigida al responsable de la información y de su tratamiento[3]

14. Recomendamos solicitar la designación de un subdelegado del Delegado de Protección de Datos de la Generalitat para el ámbito de la Conselleria de Sanidad, realizar periódicamente auditorías de protección de datos de los sistemas que manejan información de carácter personal y arbitrar canales seguros para la transmisión de datos personales entre los departamentos de la Conselleria.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico 2 se muestra la clasificación de las recomendaciones relativas a los CGTI, según los criterios combinados de riesgo potencial a mitigar y coste de su implantación.

Gráfico 2. Riesgos que se atienden y coste de implantación de las recomendaciones referidas a los CGTI



[3] El artículo 7 de la Orden 9/2012, de 10 de julio, de la Conselleria de Sanidad, atribuye al conseller las funciones de responsable de la información y de los tratamientos de datos personales, así como el nombramiento de otros responsables (funcionales y de seguridad) que deben participar en la implementación de las medidas de protección de los datos personales.

Seguimiento de recomendaciones procedentes de informes de auditoría anteriores

La Conselleria no ha aportado a la Sindicatura la información solicitada de forma reiterada sobre las medidas adoptadas en relación con las recomendaciones sobre CGTI incluidas en el informe del ejercicio 2016. La valoración sobre el grado de implantación de esas recomendaciones se ha realizado a partir de la evidencia obtenida de nuestras observaciones y conversaciones con personal de la Conselleria, a la fecha de nuestra revisión (septiembre de 2023).

No se incluyen en el siguiente cuadro las relativas a los controles de procesamiento de la información cuyo análisis se ha realizado en el informe especial de compras sanitarias. En este cuadro, para cada recomendación, constan los comentarios relativos a su situación a finales de septiembre de 2023 y su correspondiente categorización según la guía práctica de fiscalización de los órganos de control externo GPF-OCEX 1735, "Las recomendaciones y su seguimiento" (véase apéndice 2), así como los efectos en el presente informe.

Tal como se muestra en el siguiente cuadro, de las 8 recomendaciones realizadas en el informe de 2016, 5 no se han atendido y 3 lo han sido solo parcialmente.

Cuadro 3. Seguimiento de recomendaciones

		Recomendaciones de informes anteriores	Informe del ejercicio	Estado de la recomendación	Consecuencia en el informe
MARCO ORGANIZATIVO	1	La Conselleria debe realizar la correspondiente auditoría de la LOPD con carácter bienal, de acuerdo con lo establecido en el RLOPD. Adicionalmente, a partir del 25 de mayo de 2018 será aplicable el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos personales. Este reglamento incluye diferencias significativas respecto a la regulación actual española. Por este motivo, se recomienda a la Conselleria iniciar un proceso de adecuación a dicho reglamento a fin de garantizar su cumplimiento en los plazos establecidos.	2013, 2016	**No aplicada** *El RGPD atribuye el principio de responsabilidad proactiva al responsable del tratamiento de datos personales y otras obligaciones sobre esos tratamientos. Son necesarias actuaciones adicionales para el cumplimiento estricto de la normativa de protección de datos.*	Se actualiza la redacción. (Véase recomendación nº 14)
	2	La Conselleria debe elaborar un plan de adecuación al ENS, implantar las medidas incluidas en dicho plan, y realizar las auditorías de seguridad legalmente obligatorias.	2013, 2016	**No aplicada** *No se ha modificado la situación respecto al informe anterior.*	Se mantiene la redacción. (Véase recomendación nº 13)
OPERACIONES	3	La Conselleria debe preparar y licitar los contratos de soporte a todas las aplicaciones corporativas de forma planificada y en plazos suficientes, de forma que se garantice su adecuado mantenimiento y el cumplimiento de la normativa de contratación.	2016	**No aplicada** *No se ha modificado la situación respecto al informe anterior.*	Se actualiza la redacción. (Véase recomendación nº 2)

		Recomendaciones de informes anteriores	Informe del ejercicio	Estado de la recomendación	Consecuencia en el informe
CONTROLES DE ACCESO A DATOS Y PROGRAMAS	4	Recomendamos que se aplique el procedimiento de gestión de usuarios y de permisos. Asimismo, deberían realizarse revisiones periódicas de los usuarios autorizados, de forma que se garantice que solo tienen acceso a la aplicación los usuarios que lo necesitan en base a las tareas asignadas. Debe conservarse la documentación acreditativa de las revisiones realizadas, de los resultados y de las acciones llevadas a cabo.	2013, 2016	**Aplicada parcialmente** *Hemos obtenido evidencia de que se realizan revisiones periódicas de usuarios en ORION LOGIS, pero no se realiza un seguimiento sobre la subsanación de las incidencias resultantes de las revisiones.*	Se actualiza la redacción. (Véase recomendación nº 7)
	5	Recomendamos se modifiquen las políticas de autenticación (contraseñas) para todos los sistemas y adaptarlas a parámetros rigurosos de calidad y renovación (complejidad mínima, cambio de contraseñas de 3 a 6 meses, historial de contraseñas mínimo de 5, bloqueos ante intentos fallidos, forzar el cambio inicial de contraseña, etc.), tal como requiere el ENS.	2013, 2016	**Aplicada parcialmente** *Se han mejorado los parámetros de autenticación en algunos sistemas, pero no en todos.*	Se actualiza la redacción anterior. (Véase recomendación nº 8)
	6	Recomendamos se apruebe un procedimiento que contemple la obligación de que todos los usuarios de los sistemas sean nominativos, tal como exige el ENS. Cuando no sea posible eliminar los usuarios genéricos en los distintos niveles de los sistemas de información, se deben reducir al mínimo indispensable y se deben contemplar controles compensatorios sobre ellos.	2013, 2016	**No aplicada** *Existen incidencias respecto a la configuración de los identificadores de usuarios de los sistemas de información.*	Se actualiza la redacción. (Véase recomendación nº 8)
	7	Recomendamos que se realice activamente una gestión de los derechos de acceso a la aplicación ORION LOGIS que contemple los siguientes aspectos: - Cada usuario de la aplicación solo dispone de los permisos mínimos necesarios de acuerdo con sus funciones. - Dado el elevado número de usuarios de la aplicación, deben configurarse perfiles estándar para los puestos de trabajo. - Debe conservarse la documentación acreditativa de las revisiones realizadas, los resultados y las acciones llevadas a cabo. - En caso de que se considere necesario que haya usuarios que requieran un elevado nivel de privilegios y no se puedan evitar los conflictos por falta de segregación de funciones, se deben implantar controles compensatorios.	2013, 2016	**No aplicada** *No se ha modificado la situación respecto al informe anterior.*	Se actualiza la redacción. (Véase recomendación nº 7)
CONTINUIDAD DEL SERVICIO	8	Recomendamos que el máximo nivel directivo elabore y apruebe un plan de continuidad que defina y documente las acciones necesarias para recuperar y restaurar las actividades críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado tras una interrupción no prevista o desastre.	2013, 2016	**Aplicada parcialmente** *Se aporta un documento de plan de continuidad actualizado pero no aprobado por la dirección. No reúne todos los requisitos.*	Se actualiza la redacción. (Véase recomendación nº 12)

APÉNDICE 1
La aplicación ORION LOGIS

ORION LOGIS

ORION LOGIS es la aplicación corporativa de la Conselleria de Sanidad que integra toda la gestión económica y logística de los departamentos de salud y demás centros de gasto. Con ella se gestionan las necesidades de materiales, pedidos, contratación, recepción de materiales o servicios, comprobación de facturas y gestión de almacenes.

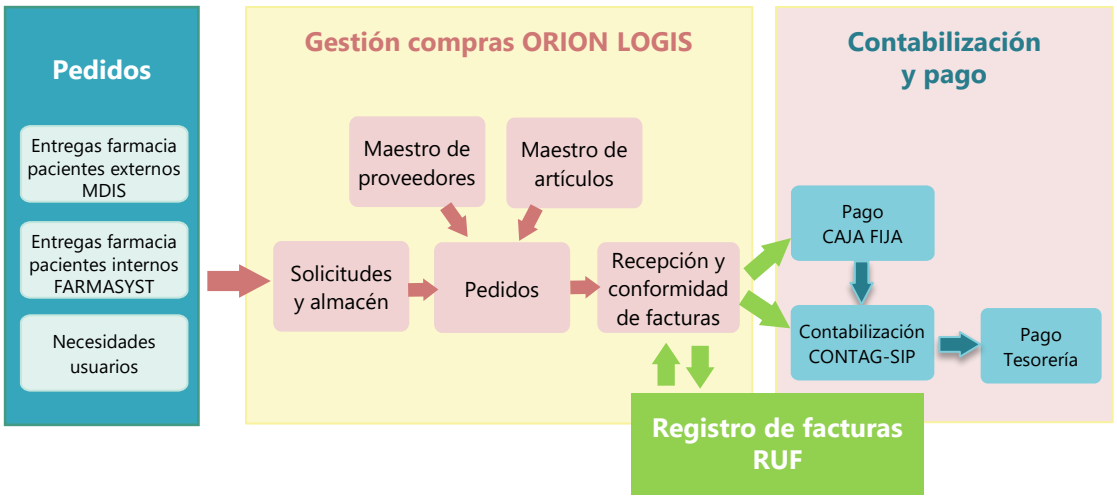
ORION LOGIS se empezó a desarrollar en 2006 y se desplegó progresivamente en los distintos centros sanitarios a partir de 2008 hasta finalizar su implantación en todos los centros de la Conselleria en 2013.

Además de ORION LOGIS, las aplicaciones más importantes que interactúan con el proceso de compras son las siguientes:

CONTAG-SIP	Contabilidad presupuestaria.
CAJA FIJA	Todos los gastos menores de 5.000 euros contemplados en el Decreto 25/2017, de 24 de febrero, del Consell.
RUF	Registro de facturas de la Generalitat.
MDIS	*Software* de gestión de entregas de medicamentos a pacientes externos.
FARMASYST	*Software* de gestión de entregas de medicamentos a pacientes internos.

El conjunto de este proceso de gestión se puede representar esquemáticamente de la siguiente forma:

Gráfico 3. Mapa de procesos de la gestión de compras



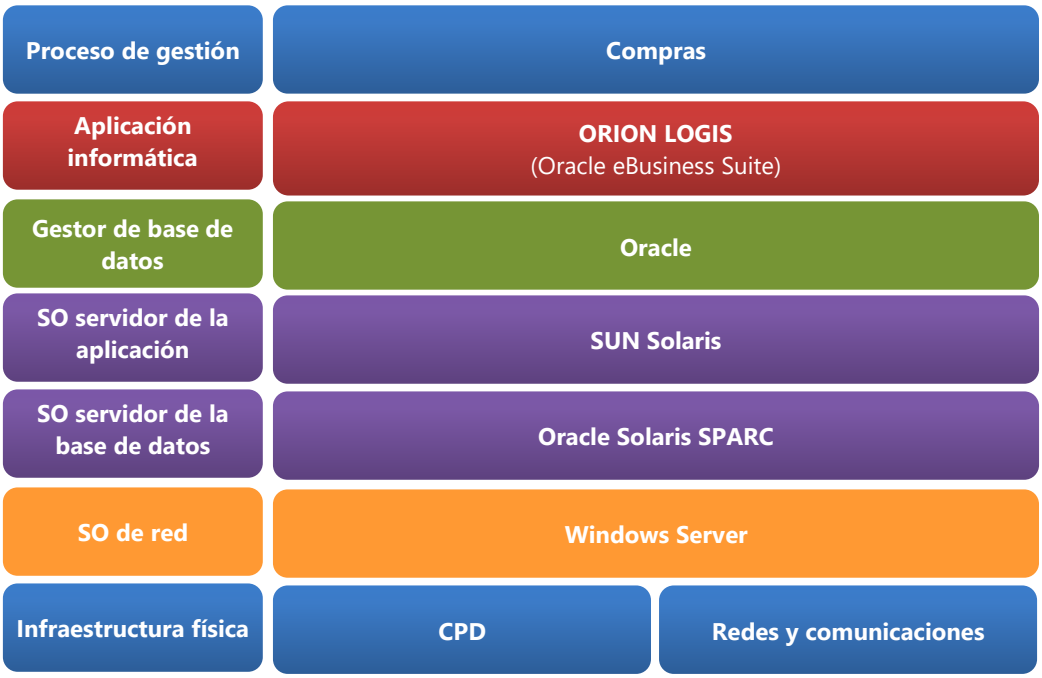
Las principales interfaces entre las aplicaciones son:

RUF>ORION	RUF vuelca las facturas recibidas que se van a gestionar en los departamentos de salud a ORION LOGIS (estado: enviadas).
ORION>RUF	ORION vuelca las facturas revisadas a RUF (estado: disponible).
ORION>CAJA FIJA	Las facturas verificadas en ORION LOGIS se vuelcan a Caja Fija.
ORION>CONTAG-SIP	Informa manualmente de las facturas verificadas para su contabilización en CONTAG-SIP.
MDIS>ORION	Vuelca las salidas de farmacia entregadas a pacientes externos a ORION LOGIS.
FARMASYST>ORION	Vuelca las entregas de productos farmacéuticos a planta del hospital.

Entorno tecnológico

El entorno tecnológico de ORION LOGIS se puede representar esquemáticamente en el siguiente gráfico.

Gráfico 4. Esquema del entorno tecnológico de la gestión de compras sanitarias



APÉNDICE 2
Metodología de la auditoría

1. Qué es un sistema de control interno

A los efectos de este informe, entendemos como sistema de control interno de la Conselleria de Sanidad **el sistema diseñado, implementado y mantenido por los órganos superiores (responsables del gobierno de la entidad), la dirección y otro personal, con la finalidad de proporcionar una seguridad razonable sobre la consecución de los objetivos de la entidad** relativos a[4]:

a) la eficacia y eficiencia de las operaciones,

b) la fiabilidad de la información financiera, y

c) el cumplimiento de las disposiciones legales y reglamentarias aplicables.

Un sistema de control interno efectivo proporciona una seguridad razonable respecto a la consecución de los objetivos de la entidad y reduce a un nivel aceptable el riesgo de no alcanzar un objetivo de la entidad. [5]

A estos efectos, un sistema de control interno comprende cinco componentes interrelacionados:

a) el entorno de control (que incluye la gobernanza sobre las tecnologías de la información y sobre la ciberseguridad),

b) el proceso de valoración del riesgo por la entidad,

c) el proceso de la entidad para el seguimiento del sistema de control interno,

d) el sistema de información y comunicación, y

e) las actividades de control (controles generales de tecnologías de la información CGTI y controles de procesamiento de la información CPI).

El componente "actividades de control" incluye los controles, es decir, las políticas o procedimientos que establece una entidad para alcanzar los objetivos de control de la dirección o de los responsables del gobierno de la entidad. Básicamente los controles se dividen en dos tipos: los CGTI y los CPI.

2. Qué son los controles generales de tecnologías de la información

Como parte del sistema de control interno de una entidad, los controles generales de tecnologías de la información (CGTI) establecen un marco general de confianza respecto del funcionamiento de los controles en los procesos y aplicaciones de gestión.

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

[5] Control interno-Marco integrado, Resumen ejecutivo, COSO, mayo 2013.

De acuerdo con el ENS, los CGTI deben diseñarse para proporcionar una garantía razonable de que los datos, la información y los activos de los sistemas de información de la entidad cumplen las siguientes propiedades o dimensiones de la seguridad de la información:

- **Confidencialidad**, es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

- **Integridad**, es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales.

- **Disponibilidad**, se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por usuarios o procesos autorizados cuando lo requieran.

- **Autenticidad**, es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

- **Trazabilidad**, es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Desde el punto de vista de la Sindicatura los CGTI cumplen una doble función:

a) Los CGTI son importantes como protección frente a las ciberamenazas. En los últimos años el sector de la salud se ha convertido en un objetivo preferente de los ciberdelincuentes, y unos sólidos CGTI representan la defensa más eficaz frente a las ciberamenazas en un entorno que se sustenta en sistemas de información intensamente interconectados.

b) Además, estos controles son importantes, ya que establecen un marco general de confianza respecto del funcionamiento de los CPI. La ineficacia o mal funcionamiento de los CGTI impediría confiar en los controles de procesamiento de la información. Por tanto, su auditoría proporciona confianza respecto de si los CGTI cumplen o no este objetivo.

Los auditores deben revisar el sistema de control interno y obtener evidencia de auditoría para obtener un determinado grado de seguridad sobre la eficacia de los CGTI y comprobar si garantizan razonablemente las cinco propiedades o dimensiones de la seguridad.

Finalmente, los controles de seguridad de la información, básicamente los CGTI, son de obligado cumplimiento en virtud de distinta normativa, especialmente por el ENS.

3. Metodología de la auditoría

La presente auditoría está basada en las guías prácticas de fiscalización GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad", y GPF-OCEX 5330, "Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica", que forman parte del *Manual de fiscalización* de la Sindicatura de Comptes y

que pueden consultarse en nuestra web. Para mayor detalle sobre la metodología utilizada nos remitimos a esas guías.

El contenido de ambas guías, fundamentalmente relacionado con la auditoría de la seguridad de los sistemas de información, es coherente con los postulados del ENS, que es de obligado cumplimiento para todos los entes públicos. Esta alineación facilita la realización de las auditorías de ciberseguridad por parte de la Sindicatura y coadyuva a la implantación del ENS en los entes auditados, ya que prácticamente todos los subcontroles o controles detallados que verifica la Sindicatura están exigidos por el ENS.

La metodología establecida en las citadas guías incluye la revisión de numerosos controles. Hemos seleccionado para esta auditoría, por considerarlos los más importantes para el proceso de compras sanitarias, los siguientes:

Cuadro 4. Controles generales de tecnologías de la información

Área		Control
A. Marco organizativo	A1/A2/ A3/A4	Marco organizativo y gobernanza de la ciberseguridad (CBCS 8)
C. Operaciones de los sistemas de información	C1H	Inventario de *hardware* (CBCS 1)
	C1S	Inventario de *software* (CBCS 2)
	C2	Gestión de vulnerabilidades (CBCS 3)
	C3	Configuraciones seguras (CBCS 5)
	C4	Registro de la actividad de los usuarios (CBCS 6)
D. Controles de acceso a datos y programas	D1	Uso controlado de privilegios administrativos (CBCS 4)
	D2/D3/D4	Controles de acceso a usuarios
	D5	Protección de redes y comunicaciones
E. Continuidad del servicio	E1	Copia de seguridad de datos y sistemas (CBCS 7)

4. Criterios de evaluación de los controles

Los CBCS y los CGTI son controles globales formados por varios subcontroles detallados. Todas nuestras comprobaciones tienen por finalidad contrastar su situación real en la entidad con las buenas prácticas recogidas en las GPF-OCEX 5313 y 5330, en las que se especifican con el máximo detalle los aspectos comprobados en cada control.

Los resultados del trabajo se analizan y evalúan a dos niveles: subcontroles y controles.

Evaluación de los subcontroles

Los CBCS y los CGTI son controles globales compuestos por varios controles detallados o subcontroles, de los que hemos revisado su diseño y eficacia operativa.

El trabajo de auditoría ha consistido básicamente en evaluar cada uno de los 51 subcontroles revisados en función, bien de los resultados de las pruebas realizadas y las evidencias obtenidas, o bien de la información proporcionada en el informe de auditoría del ENS, si existe y si confiamos en él. Cada subcontrol se evalúa según la escala mostrada en el siguiente cuadro:

Cuadro 5. Evaluación de los subcontroles

Evaluación	Descripción
Control efectivo	Cubre al 100% el objetivo de control y: El procedimiento está formalizado (documentado y aprobado) y actualizado. El resultado de las pruebas realizadas para verificar su implementación y eficacia operativa ha sido satisfactorio.
Control bastante efectivo	En líneas generales, cumple con el objetivo de control, si bien puede haber ciertos aspectos no cubiertos al 100% y: - Se sigue un procedimiento formalizado, aunque puede presentar aspectos de mejora (detalle, nivel de actualización, nivel de aprobación, etc.). - Las pruebas realizadas para verificar la implementación son satisfactorias. - Se han detectado incumplimientos en las pruebas realizadas para verificar la eficacia operativa, pero no son ni significativos ni generalizados.
Control poco efectivo	Cubre de forma muy limitada el objetivo de control y: - Se sigue un procedimiento, aunque este puede no estar formalizado. - El resultado de las pruebas de implementación y de eficacia no es satisfactorio. Cubre en líneas generales el objetivo de control, pero: - No se sigue un procedimiento claro. - Las pruebas realizadas para verificar la implementación o la eficacia operativa no son satisfactorias (se han detectado incumplimientos significativos, aunque no están generalizados).
Control no efectivo o no implantado	No cubre el objetivo de control. El diseño cubre el objetivo de control, pero el resultado de la revisión realizada pone de manifiesto que la implementación o la eficacia operativa del control no son satisfactorias (se han detectado incumplimientos significativos y generalizados).

Nivel de madurez de los controles

Para determinar la situación global de cada control hemos utilizado el modelo de nivel de madurez de los procesos de control de acuerdo con lo establecido en las GPF-OCEX 5313 y GPF-OCEX 5330, que a su vez están basadas en la *Guía de seguridad CCN-STIC 804* del CCN, usando una escala, según se resume en el siguiente cuadro. Las descripciones son las establecidas en el anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Cuadro 6. Niveles de madurez

Nivel	Índice	Descripción
N0 Inexistente	0	No existe un proceso que soporte el servicio requerido.
N1 Inicial / *ad hoc*	10	Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes. Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.
N2 Repetible, pero intuitivo	50	En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad. Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.
N3 Proceso definido	80	Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.
N4 Gestionado y medible	90	Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.
N5 Optimizado	100	La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

La evaluación que realizamos sobre el nivel de madurez no se ha basado únicamente en los procesos teóricos o en los procedimientos aprobados, sino también en la verificación de su aplicación práctica.

Para evaluar el nivel de madurez de cada control se han tenido en cuenta los resultados obtenidos en la revisión de los subcontroles que lo forman y considerando la ponderación o importancia relativa que les asignamos para el cumplimiento del objetivo de control.

Este modelo proporciona una base sólida para formarse una idea general de la situación en la entidad revisada en relación con los controles de ciberseguridad y el cumplimiento de la legalidad en esta materia. También permite comparar resultados entre distintos entes y entre distintos periodos.

Indicador global

A efectos del ENS, la guía CCN-STIC-824 contempla una serie de indicadores agregados capaces de aportar información resumida sobre el estado de la seguridad en los organismos públicos. En particular el **índice de madurez general** sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de controles de ciberseguridad.

5. Clasificación de las deficiencias de control a efectos de la auditoría

Al evaluar las deficiencias de control interno detectadas se debe considerar su significatividad y se clasifican en tres niveles de importancia relativa:

- Una **deficiencia de control interno** existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable.

  Pueden ser una deficiencia de diseño del control (cuando un control necesario para alcanzar el objetivo de control no existe o no está adecuadamente diseñado) o deficiencias de funcionamiento (cuando un control adecuadamente diseñado no opera tal como fue diseñado o la persona que lo ejecuta no lo realiza eficazmente).

  No se puede calificar como deficiencia significativa ni debilidad material, ya que su impacto potencial no se espera que sea significativo. Su subsanación puede aportar mejoras en el proceso examinado.

- Una **deficiencia significativa** es una deficiencia en el control interno, o una combinación de deficiencias, que afectan adversamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera o presupuestaria de forma fiable, de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad, que es más que remota, de que una manifestación errónea en las cuentas anuales, o un incumplimiento, que no es claramente trivial, no sea prevenida o detectada en plazo oportuno.

- Una **debilidad material** es una deficiencia significativa en el control interno, o una combinación de ellas, respecto de las que existe una razonable posibilidad de que una incorrección material en las cuentas anuales, incluyendo un incumplimiento de carácter grave, no sea prevenida o detectada y corregida en plazo oportuno.

  Tratándose de un CGTI, además, serán aquellas que no son capaces de prevenir un incidente que pueda causar una perturbación o impacto significativo en la seguridad de la información manejada o en los servicios prestados. A estos efectos, se considerará que tienen un impacto significativo los niveles "Alto", "Muy alto" y "Crítico" recogidos en la tabla de "Criterios de determinación del nivel de impacto" de la guía CCN-STIC 817.

Algunas deficiencias de control pueden ser consideradas no significativas individualmente, pero consideradas juntamente con otras similares, el efecto combinado puede ser más significativo.

El auditor informático determinará si las deficiencias de control son, individualmente o en conjunto, debilidades materiales o deficiencias significativas para el adecuado funcionamiento de los sistemas de información.

Si las deficiencias de control constituyen debilidades materiales, el auditor financiero, en base al trabajo del auditor informático, concluirá que los controles internos no son eficaces y deberá replantearse su estrategia de auditoría, es decir, la combinación adecuada de pruebas de cumplimiento y de pruebas sustantivas, dando mayor énfasis a estas últimas para intentar minimizar el riesgo final de auditoría.

6. Recomendaciones y su seguimiento

Si se efectúan **recomendaciones**, existirá una relación directa entre el tipo de deficiencia de control (según su importancia relativa), el riesgo de auditoría que representa y la prioridad que se conceda a cada recomendación.

La prioridad también estará matizada por consideraciones coste/beneficio.

En el cuadro siguiente se resume la relación existente entre los tres tipos de deficiencias de control según su significatividad o importancia relativa, el riesgo que representan y la prioridad de las recomendaciones correspondientes:

Cuadro 7. Categoría de las deficiencias de control y recomendaciones

Tipo de deficiencia según su importancia relativa	Riesgo		Prioridad de una recomendación
Debilidad material	**Alto**	**Alta**	Se requiere atención urgente de la dirección para implantar controles/procedimientos que mitiguen los riesgos identificados.
Deficiencia significativa	**Medio**	**Media**	La dirección debería establecer un plan de acción concreto para resolver la deficiencia observada en un plazo razonable.
Deficiencia de control interno	**Bajo**	**Baja**	

Las debilidades materiales deben ser incluidas en el informe de auditoría como una salvedad o como una conclusión, según el tipo de informe.

Seguimiento de las recomendaciones de informes anteriores

En la valoración de la situación actual, se ha seguido la GPF-OCEX 1735, "Las recomendaciones y su seguimiento", que propone la siguiente categorización:

Cuadro 8. Situación de las recomendaciones

Total o sustancialmente aplicada	Si el ente auditado ha adoptado las medidas correctoras, razonables y proporcionadas en la esfera de sus competencias, que permiten considerar que la recomendación ha surtido sus efectos y no ha quedado pendiente de resolución ninguna cuestión de importancia significativa. En estos casos se entenderá que la recomendación se ha cumplido razonablemente. Además, se ha obtenido evidencia suficiente que acredita las medidas adoptadas.
Aplicada parcialmente	Si el ente auditado ha tomado en consideración las recomendaciones y ha realizado actuaciones encaminadas a corregir las deficiencias, debilidades o insuficiencias que se han puesto de manifiesto, pero solamente en un estado incipiente, en una parte de ellas o en algunos aspectos, lo que no permite considerar que la recomendación se ha cumplido razonablemente.
No aplicada	Si el ente auditado no ha realizado las actuaciones encaminadas a corregir las deficiencias, debilidades o insuficiencias que se han puesto de manifiesto o bien lo ha hecho insuficiente o inadecuadamente, de forma que la recomendación sigue sin aplicarse.
Sin validez en el marco actual	Se incluyen aquellas recomendaciones que, aunque válidas y pertinentes cuando se emitió el informe y para el ejercicio fiscalizado, y aun siendo aceptadas y reconocidas por el ente auditado, no pueden aplicarse en el contexto actual, al no darse las circunstancias que lo permitan o la misma casuística que entonces, es decir, no se dan en el momento actual los supuestos de los hechos en función de los cuales se efectuó la recomendación en el pasado. La recomendación ha devenido inaplicable.
No verificada	Se incluyen en esta categoría las recomendaciones que, aunque aceptadas o incluso aplicadas y corregidas por el ente auditado, necesitarían obligatoriamente de alguna prueba adicional para contrastar lo manifestado por el ente auditado que exceden el alcance previsto en el trabajo.

APÉNDICE 3
Situación de los controles auditados

1. Introducción

Hemos revisado un total de 51 subcontroles relacionados con el proceso de gestión de las compras sanitarias, agrupados en los 10 controles principales señalados en el cuadro 2, y evaluado su nivel de madurez.

Aunque la clasificación de los sistemas de información es una exigencia establecida por el ENS, no hemos obtenido evidencia de que el sistema ORION LOGIS haya sido clasificado por parte de la Conselleria de acuerdo con el ENS (categoría alta, media o baja), por lo que lo hemos considerado de categoría de seguridad MEDIA que es la más habitual en los sistemas que soportan procesos de gestión administrativa. El nivel de madurez requerido por el ENS para este tipo de sistemas es el *N3, proceso definido* y los sistemas deben alcanzar un índice de madurez del 80%.

Los resultados obtenidos para cada uno de los CGTI revisados se muestran en el cuadro 2. En el apartado 2 de este informe se han incluido las deficiencias más relevantes de los CGTI, en el apartado 3 se incluyen también las observaciones más importantes sobre cumplimiento de la normativa y en el apartado 6, las recomendaciones que se derivan de la revisión realizada. A continuación, se detallan las observaciones y deficiencias de control detalladas obtenidas en nuestra auditoría.

2. Marco organizativo y gobernanza de la ciberseguridad

Por qué son importantes estos controles

Con la inclusión de los controles A1, A2, A3 y A4 se pretende asegurar que se cumplen diversas normas relevantes para mantener un adecuado control sobre la seguridad de los sistemas de información y las comunicaciones, y la privacidad de la información.

Es muy importante dar el debido cumplimiento a lo dispuesto por el Esquema Nacional de Seguridad, ya que su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza, en el que se designe a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.

La importancia de la gobernanza en la gestión de la ciberseguridad ha sido objeto de diversos documentos y guías del Centro Criptológico Nacional (CCN), entre los que destacan *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* y la *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*.

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

La existencia de un conjunto eficaz de procesos de gestión de la ciberseguridad y de responsabilidades definidas proporciona a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

2.1. Cumplimiento normativo y gobernanza de la ciberseguridad (A1-CBCS 8)

Objetivo del control

Asegurar el cumplimiento de la normativa básica en materia de seguridad de la información, lo que incluye el establecimiento de una adecuada gobernanza de ciberseguridad.

Situación del control

Cumplimiento del ENS

La organización de la seguridad de la información en la Conselleria viene establecida en la Orden 9/2012, de 10 de julio de 2012. En ella se configuran y establecen los órganos responsables de la seguridad, tanto al nivel de la Conselleria como de los departamentos de salud que dependen de ella.

Esta orden debe actualizarse, ya que contiene referencia a responsabilidades de seguridad y normativa de protección de datos que ya no está vigente y sus previsiones deben adecuarse a lo exigido en el Real Decreto 311/2022, de 3 de mayo, por el que se aprueba el Esquema Nacional de Seguridad (ENS).

Algunos de los órganos de seguridad previstos en el ENS y en la Orden 9/2012 no se han nombrado formalmente ni a nivel de la Conselleria ni al nivel descentralizado para los departamentos de salud. De acuerdo con lo previsto en el artículo 13 del ENS, estos responsables deben estar identificados de forma inequívoca. Algunos responsables, como el responsable del servicio, no se identifican inequívocamente.

No se ha establecido formalmente la categoría (alta, media o baja) del sistema ORION LOGIS, tal y como exige el ENS.

La Conselleria ha presentado el informe INES al CCN de acuerdo con lo previsto en el ENS.

No se han realizado las auditorías previstas en el artículo 31 del ENS ni, en consecuencia, se han publicado en la sede electrónica las declaraciones de conformidad y los distintivos correspondientes, de acuerdo con la Instrucción Técnica de Seguridad de conformidad con el ENS aprobada por Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas.

Gobernanza de la ciberseguridad

La Conselleria no tiene establecida una adecuada gobernanza de la seguridad de la información que contemple un liderazgo eficaz de la alta dirección para promover e implantar, a lo largo de toda la organización, los controles exigidos por la normativa de seguridad de la información y protección de datos personales que le es de aplicación, básicamente ENS y LOPDP[6].

Aunque existe un alto nivel de compromiso y concienciación con la ciberseguridad por parte de los miembros de la Subdirección General de Sistemas de Información para la Salud (SDGSIS) y, en particular, de la Oficina de Seguridad de la Información, este compromiso no se visualiza en los órganos superiores de la Conselleria, lo que se observa en aspectos como:

- La Conselleria dispone de una Orden que regula la organización de la seguridad, que se completa con un marco normativo y procedimental, pero esta documentación no es completa ni está aprobada formalmente y no nos consta que se comunique formalmente a todos los responsables encargados de aplicarla. Además, como ya se ha indicado, esa Orden es de 2012 y se encuentra desactualizada.

- No hemos podido evaluar si la SDGSIS dispone de suficientes recursos económicos y humanos dedicados a la seguridad de la información dado que no se nos ha facilitado la información solicitada sobre su personal, proyectos y dotaciones presupuestarias.

Adicionalmente, determinadas circunstancias indican que la gobernanza no puede considerarse efectiva. Basamos esta afirmación en las siguientes carencias relevantes:

- La falta de liderazgo en materia de ciberseguridad de los órganos superiores de la Conselleria.

  La organización no dispone de planes ni estrategias elaboradas y aprobadas por los órganos superiores en relación con la seguridad de la información, ni impulsa las medidas de seguridad necesarias, incluyendo la formación y concienciación de sus trabajadores. Son los miembros del departamento TIC, por propia iniciativa y sin el

[6] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

respaldo del comité de seguridad de la información, quienes implantan medidas relacionadas con la ciberseguridad e impulsan el cumplimiento de la normativa en esta materia.

El compromiso con la ciberseguridad debe partir desde los órganos superiores de la Conselleria para que pueda alcanzar al resto de la organización y se facilite su aplicación práctica.

- El Comité de Seguridad de la Información (CSI) únicamente se ha reunido una vez en 2022, aunque el acta de esta reunión no está firmada. Es necesario que el CSI funcione de forma efectiva, como órgano imprescindible para coordinar la seguridad de la información entre las distintas áreas de la organización.

  Es en el CSI donde deben tomarse las decisiones concretas en materia de seguridad de la información, aprobando las normas de seguridad pertinentes e impulsando las acciones a llevar a cabo. Aunque este órgano está establecido en una Orden aprobada por la Conselleria, no ejerce sus funciones de manera efectiva. El Comité debe reunirse periódicamente y, en una entidad del tamaño de la Conselleria y dada la complejidad de sus sistemas, recomendamos que lo haga al menos mensualmente.

- Algunos de los roles en materia de seguridad de la información no están correctamente definidos y otros no se han nombrado formalmente.

  El rol de responsable del servicio no se encuentra formalmente definido y otros roles de seguridad se definen en base a la anterior normativa de protección de datos. No se han nombrado todos los roles de seguridad de los elementos descentralizados de la organización previstos en la Orden 9/2012 de la Conselleria.

Los órganos superiores de la Conselleria son los responsables de que existan unos controles de seguridad adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

Es necesario solventar de forma urgente las carencias identificadas, dado que afectan de manera negativa al nivel de seguridad de la información de la Conselleria.

Cumplimiento del Real Decreto 4/2010 (ENI)

No se ha elaborado el plan de adecuación al ENI que exige el Real Decreto 4/2010 de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica. ORION LOGIS no está adaptado a la generación de expedientes ENI.

La Conselleria debe elaborar un plan de adaptación al ENI de acuerdo con lo exigido en la propia norma. El plan debe incluir la adaptación de ORION LOGIS para la generación de documentos y expedientes ENI.

Cumplimiento de la LOPDP

En cuanto al cumplimiento en materia de protección de datos personales, la revisión realizada ha puesto de manifiesto que existen algunas medidas en relación con el cumplimiento de la LOPDP que se encuentran implementadas: nombramiento de un delegado de protección de datos (DPD) para la Generalitat, elaboración de la relación de actividades de tratamiento, que incluye la referente a compras sanitarias, previsión de órganos encargados de protección de datos, etc.

Sin embargo, habida cuenta del tipo de datos personales que se tratan en la Conselleria y sus departamentos, deberían realizarse esfuerzos adicionales: realizar auditorías de protección de datos y nombrar al subdelegado de protección de datos para sanidad previsto en la organización del DPD de la Generalitat.

2.2. Estrategia de TI (A2)

Objetivo del control

Asegurar una planificación estratégica de los sistemas de información de forma que estos estén siempre orientados a la consecución de los objetivos de la organización.

Situación del control

La Conselleria basa su planificación estratégica en relación con los sistemas de información en el Plan Estratégico de Transformación Digital de la Administración de la Generalitat 2020-2025. Sin embargo, no hemos identificado una planificación a nivel de proyectos de la Conselleria que concrete y desarrolle anualmente los objetivos previstos en esa planificación estratégica. Tampoco hemos podido obtener evidencias de que los proyectos de TI cuenten con presupuesto adecuado para que se puedan llevar a cabo.

2.3. Organización y personal de TI (A3)

Objetivo del control

Asegurar la independencia funcional del departamento TIC de forma que le permita realizar sus tareas de manera que abarquen a toda la organización, asegurar que existe segregación de funciones incompatibles entre los componentes del departamento, garantizar la formación en materia de seguridad de la información y utilizar indicadores para valorar el nivel de prestación de los servicios TIC al resto de la organización.

Situación del control

Durante el periodo auditado, la Subdirección General de Sistemas de la Información para la Salud (SDGSIS) depende de la Dirección General de Planificación, Eficiencia Tecnológica y Atención al Paciente y se estructura en tres servicios que a su vez se dividen en unidades funcionales no reconocidas formalmente en el ROF de la Conselleria.

No hemos identificado situaciones que comprometan la independencia de la SDGSIS en cuanto a la dedicación de los recursos necesarios TIC a las otras direcciones generales y unidades. Sin embargo, su ubicación en el organigrama de la Conselleria la sitúa como dependiente de una dirección general con múltiples misiones.

La Orden 4/2023, de 13 de octubre, de la Conselleria de Sanidad, por la que se desarrolla el Decreto 135/2023, de 10 de agosto, del Consell, de aprobación del Reglamento orgánico y funcional de la Conselleria de Sanidad, modifica la denominación del departamento, que pasa a ser la Subdirección General de Tecnologías de la Información y las Comunicaciones para la Salud, lo sitúa bajo la dependencia directa de la Secretaría Autonómica de Planificación, Información y Transformación Digital y la dota de un cuarto servicio.

No hemos podido obtener evidencia de la existencia de un plan de formación sobre seguridad de la información en la Conselleria.

De acuerdo con la información facilitada no existe un seguimiento de indicadores de los servicios prestados por la SDGSIS al resto de unidades de la Conselleria.

2.4. Marco normativo y procedimental de seguridad (A4)

Objetivo del control

Aprobar una normativa interna de seguridad de la información y comunicar los procedimientos asociados a los responsables de su aplicación.

Situación del control

La Conselleria aplica la política de seguridad de la Generalitat. La SDGSIS ha desarrollado algunos procedimientos de seguridad no aprobados formalmente. Además, no consta que se hayan comunicado adecuadamente a todos los responsables de aplicarlos ni que exista un repositorio actualizado disponible para esos responsables.

Existen aspectos importantes para la seguridad de la información que no cuentan con un procedimiento detallado, aprobado y comunicado formalmente a los interesados como la gestión de inventarios de *software* y *hardware,* gestión de usuarios, control de los usuarios administradores de los sistemas o asignación de responsabilidades en los sistemas de información.

3. Operaciones de los sistemas de información

Apartado eliminado en la fase de alegaciones.

4. Controles de acceso a datos y programas

Apartado eliminado en la fase de alegaciones.

Dada la sensibilidad de los sistemas de información sanitarios y de la información tratada, y con objeto de reducir a cero el riesgo adicional en la seguridad en dichos sistemas, derivado de un posible mal uso de nuestro informe, los resultados detallados que se incluían en los apartados 3 y 4 del apéndice 3 se han eliminado en la fase de alegaciones y se comunican con carácter confidencial a los responsables de la conselleria para que puedan adoptar las medidas correctoras precisas.

5. Continuidad del servicio

5.1. Copias de seguridad de datos y sistemas (E1-CBCS 7)

Objetivo del control

Utilizar procesos y herramientas para realizar copias de seguridad de la información crítica con una metodología que permita la recuperación de la información en tiempo oportuno.

Por qué es importante este control

Cuando los atacantes comprometen los sistemas, a menudo realizan cambios significativos de las configuraciones y el *software*. En ocasiones, los atacantes también realizan alteraciones sutiles de los datos almacenados en los sistemas comprometidos, lo que puede poner en peligro la eficacia de la organización con información contaminada. Otras veces simplemente destruyen o invalidan todos o parte de los datos y *software* de una entidad.

Los daños de ciberataques pueden ser mitigados si se dispone de copia de seguridad de los datos afectados.

Situación del control

La Conselleria dispone de varios controles y procedimientos asociados a la gestión de los distintos niveles de copia de seguridad de los datos y sistemas, que no detallamos por razones de seguridad.

Existe un proceso de revisión de las copias de seguridad llevado a cabo por los técnicos responsables, que garantiza la revisión del estado de las copias mediante tiques en la herramienta de gestión de incidencias que quedan pendientes hasta que se resuelven.

Durante la auditoría hemos observado que se realizan restauraciones de datos y sistemas desde la copia de seguridad que, aunque no son pruebas planificadas de restauración, se

llevan a cabo con éxito y se registran en forma de tiques en la herramienta de gestión de incidencias.

Aunque existe cierto nivel de control sobre las copias, hemos observado carencias que impiden alcanzar un nivel de madurez superior en este control, como son:

- El procedimiento de políticas de copias de seguridad ha sido actualizado recientemente. Aunque actualmente prevé pruebas de recuperación cada 6 meses, no especifica sobre qué sistemas ni prevé la forma de documentar las pruebas.

- Los responsables funcionales de los datos no participan en la definición de los datos a copiar ni en los periodos de retención de las copias. Los datos incluidos en la copia son los decididos por los técnicos de sistemas de la SGSIS según su propio criterio, salvo peticiones expresas de los responsables funcionales del sistema a través de la herramienta de gestión de incidencias.

- La Conselleria dispone de un único CPD, lo que conlleva varios tipos de riesgo en caso de incidente: pérdida de disponibilidad o continuidad de servicios, pérdida de los datos de copia, etc.

- Aunque existen copias desconectadas almacenadas en una ubicación diferente al CPD, estas no se extraen con una periodicidad suficiente para impedir la pérdida de datos en caso de requerir respaldos desde estas copias.

Este sistema de copias de seguridad, aunque es útil y hasta ahora ha sido suficiente para recuperaciones de incidentes de seguridad leves, no garantiza la recuperación de los sistemas críticos de la Conselleria en unos plazos razonables ante un incidente grave que afecte a su CPD.

GLOSARIO

Alta dirección: A los efectos de este trabajo, nos referimos a los órganos superiores de la Conselleria, conseller/a, secretarías autonómicas, direcciones generales y subsecretarías. Son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, así como una adecuada gobernanza de ciberseguridad.

Alta disponibilidad: Es la capacidad que tiene un sistema para asegurar la continuidad de los servicios, incluso en situaciones donde ocurran incidentes a nivel de *hardware*, *software*, cortes de energía, de comunicaciones o de otro tipo.

Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se clasifica un sistema de información a fin de seleccionar las medidas de seguridad necesarias para este. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Ciberamenazas: Eventos con origen en internet que pueden desencadenar un incidente en la organización y producir daños materiales, pérdidas inmateriales en sus activos o la interrupción de un servicio.

Ciberhigiene: Conjunto de prácticas y acciones básicas que una organización debe implantar para hacer frente a los riesgos de ciberseguridad más comunes y generalizados a los que se enfrenta hoy en día. A los efectos de este trabajo, dicho conjunto de prácticas y acciones básicas son los CBCS.

Ciberresiliencia: Es la capacidad de un proceso, negocio, organización o nación para anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos cibernéticos que necesitan para funcionar. En el ámbito concreto del sector público, es la capacidad de un ente público para evitar o resistir y recuperarse de un ataque y continuar prestando sus servicios en un tiempo razonable.

Ciberseguridad: Todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas (Reglamento (UE) 2019/881).

Dirección: Son los responsables de la ejecución de las actividades establecidas por la alta dirección en materia TIC y de ciberseguridad, es la dirección ejecutiva. En este grupo, a los efectos de este informe, se incluye a los miembros de la alta dirección con responsabilidades específicas sobre las TIC, al responsable de seguridad, al responsable de los sistemas de información y las comunicaciones, a los funcionarios directores del departamento TIC y los subdirectores o jefes de servicio.

Gobernanza de ciberseguridad: Según el Tribunal de Cuentas Europeo, la gobernanza de la seguridad de la información consiste en la creación de estructuras y políticas para garantizar la confidencialidad, integridad y disponibilidad de los datos. Es más que una mera cuestión técnica, por lo que exige un liderazgo efectivo, procesos sólidos y estrategias

en consonancia con los objetivos de la organización. A los efectos de este informe le damos el mismo significado que a *gobernanza de la seguridad de la información*.

Informe INES: Es un informe-declaración que deben realizar las Administraciones públicas anualmente para presentarlo al Centro Criptológico Nacional (CCN) con la herramienta del mismo nombre. Esta herramienta es una solución desarrollada por el CCN para la gobernanza de la ciberseguridad, que permite evaluar regularmente el estado de la seguridad de los sistemas TIC de las entidades y su adecuación al Esquema Nacional de Seguridad (ENS) adaptándose a otros estándares o normas reguladoras en caso necesario.

Interfaz: Es una conexión entre dos dispositivos, aplicaciones o sistemas de origen y destino, mediante la que se intercambia información.

Normas de seguridad: Uniforman el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio y describirán: a) el uso correcto de equipos, servicios e instalaciones; b) lo que se considerará uso indebido, y c) la responsabilidad del personal con respecto al cumplimiento o violación de estas normas. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones; como regla general, estará disponible en la intranet corporativa de la entidad a través de una dirección URL. La normativa de seguridad de cada entidad trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y del desarrollo normativo de la política de seguridad de la entidad en cuestión, en segunda instancia.

Política de seguridad de la información: La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta, de acuerdo con el artículo 12 del Real Decreto 311/2022 (ENS). Debe ser aprobada por los altos órganos de dirección de la entidad y debe estar accesible para todos los miembros de la organización y redactada de forma sencilla, precisa y comprensible. Conviene que sea breve, y que deje los detalles técnicos para otros documentos más precisos que ayuden a llevar a cabo lo propuesto: normas de seguridad y procedimientos de seguridad.

Procedimientos de seguridad: Abordan tareas concretas, indicando lo que hay que hacer, paso a paso. Detallan de forma clara y precisa: a) cómo llevar a cabo las tareas habituales; b) quién debe hacer cada tarea y, c) cómo identificar y reportar comportamientos anómalos.

Proceso: Conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.

ABREVIACIONES

CBCS: Controles básicos de ciberseguridad (forman parte de los CGTI).

CGTI: Controles generales de tecnologías de la información.

CPD: Centro de proceso de datos.

CPI: Controles de proceso de gestión de la información.

DGTIC: Dirección General de Tecnologías de la Información y las Comunicaciones.

DPD: Delegado de protección de datos personales.

EDR: Herramienta de detección y respuesta ante amenazas cibernéticas (por sus siglas en inglés: *endpoint detection and response*).

ENI: RD 4/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Interoperabilidad.

ENS: RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

GETEC: Unidad de gestión de tecnología (servidores lógicos) de la SDGSIS.

LAN: Red de área local (*local area network*).

LOPDP: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

ODM: Oficina de datos maestros de la Conselleria que controla y autoriza las altas de artículos y proveedores en ORION LOGIS.

OSI: Oficina de Seguridad de la Información de la Conselleria.

RGPD: Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

ROF: Reglamento orgánico y funcional

RUF: Aplicación con la que se gestiona el registro de facturas de la Generalitat Valenciana.

SDGSIS: Subdirección General de Sistemas de la Información para la Salud.

TIC: Tecnologías de la información y las comunicaciones.

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, el borrador previo del Informe de auditoría se discutió con responsables TIC de la Conselleria de Sanidad para su conocimiento y para que, en su caso, efectuaran las observaciones que estimaran pertinentes.

Posteriormente, en cumplimiento del artículo 16 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, y del artículo 55.1.c) del Reglamento de Régimen Interior de la Sindicatura de Comptes, así como del acuerdo del Consell de esta institución por el que tuvo conocimiento del borrador del Informe de auditoría correspondiente al ejercicio 2022, este se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Dentro del plazo concedido, la entidad ha formulado las alegaciones que ha considerado pertinentes.

En relación con el contenido de las alegaciones y su tratamiento, es preciso señalar lo siguiente:

1) Todas las alegaciones han sido analizadas detenidamente.

2) Las alegaciones admitidas se han incorporado al contenido del Informe.

El texto de las alegaciones formuladas, así como el informe motivado que se ha emitido sobre estas, que ha servido de antecedente para su estimación o desestimación por esta Sindicatura, se incorporan en los anexos I y II.

APROBACIÓN DEL INFORME

En cumplimiento del artículo 19.j) de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, del artículo 55.1.h) de su Reglamento de Régimen Interior y del Programa Anual de Actuación de 2023 de esta institución, el Consell de la Sindicatura de Comptes, en reunión del día 13 de diciembre de 2023, aprobó este informe de auditoría.

ANEXO I

Alegaciones presentadas

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

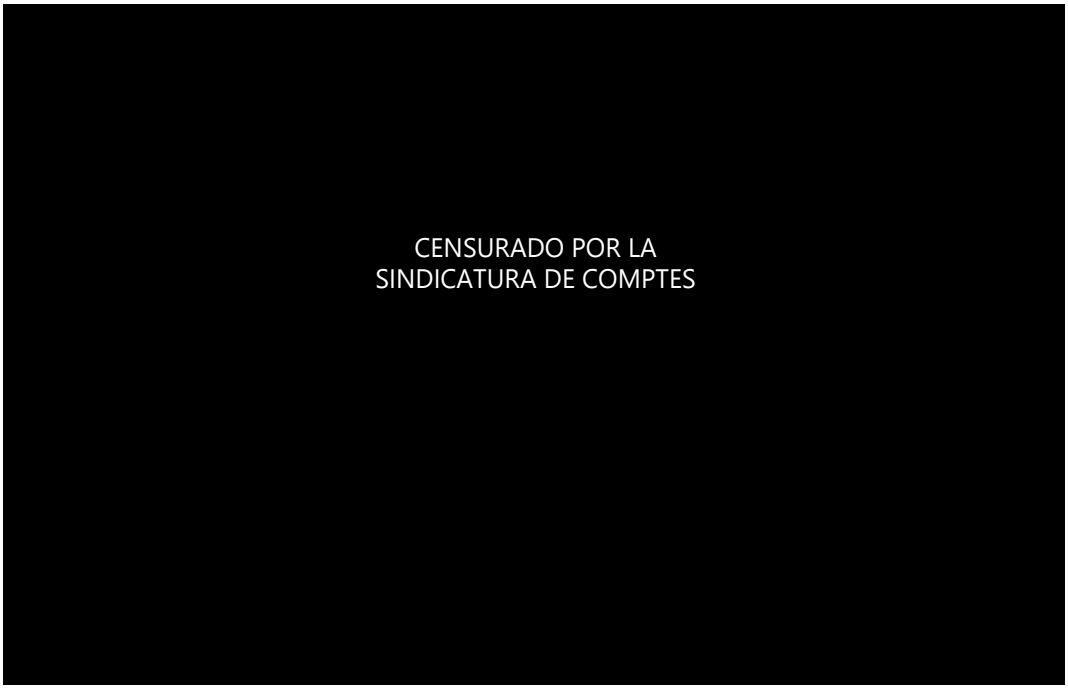
Apartado Conclusiones generales de TI, página 6:

> 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]
CENSURADO POR 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

ANEXO II

Informe sobre las alegaciones presentadas

ANÁLISIS DE LAS ALEGACIONES EFECTUADAS AL 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 han analizado las alegaciones recibidas el 27 de noviembre de 2023 y con respecto a estas se informa lo siguiente:

Primera alegación

Conclusión del párrafo 4º del apartado 2, "CONCLUSIONES SOBRE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE LA INFORMACIÓN"

Comentarios

La conclusión del informe señala que:

> "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."

La Conselleria de Sanidad alega que tiene previsto ejecutar en un futuro próximo 4,5 millones de euros en proyectos para mejorar la ciberseguridad financiados por el Mecanismo de Recuperación y Resiliencia de la Unión Europea con el objetivo de desarrollarlos y finalizarlos, en la mayor parte de los casos, en 2024.

Las inversiones en ciberseguridad mejorarán los niveles de madurez de la Conselleria, por lo que consideramos que la iniciativa va en la dirección correcta para implantar las recomendaciones incluidas en el Informe. La alegación no altera nuestras conclusiones.

Consecuencias en el Informe

No se modifica el borrador del Informe.

Segunda alegación

Primer párrafo del apartado 3, "CONCLUSIONES SOBRE EL CUMPLIMIENTO DE LA NORMATIVA EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN"

Comentarios

El párrafo alegado del Informe es el siguiente:

> "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."

La Conselleria de Sanidad alega que se producirá un salto cualitativo al ejecutar los contratos previstos al finalizar las actuaciones que actualmente siguen en marcha en esta materia.

Durante el trabajo de campo hemos observado (e incluido en nuestro informe) las actuaciones iniciadas para dar cumplimiento a la normativa en materia de seguridad de la información. Consideramos que la finalización de dichas acciones junto a la ejecución de las contrataciones previstas va en la dirección correcta para cumplir con la normativa. La alegación no altera nuestras conclusiones.

Consecuencias en el Informe

No se modifica el borrador del Informe.

Tercera alegación

Apéndice 3, último párrafo del apartado "3.2. Inventario de *software* (C1-CBCS 2)"

Comentarios

Se ha eliminado todo el apartado. Véase la quinta alegación.

Cuarta alegación

Apéndice 3, apartado "4.1. Uso controlado de privilegios administrativos (D1-CBCS 4)"

Comentarios

Se ha eliminado todo el apartado. Véase la quinta alegación.

Quinta alegación

Consideración final añadida por la Conselleria en sus alegaciones

La Conselleria de Sanidad ha añadido a su informe de alegaciones la siguiente observación: "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". Además, solicitan limitar "el nivel de detalle en el informe público, evitando dar pistas a los posibles atacantes sobre las debilidades de control detectadas" y "una mayor concreción en el informe interno".

Comentarios

La información tratada durante las auditorías de ciberseguridad está relacionada con la seguridad de los sistemas de información de las entidades, por lo que la Sindicatura de Comptes, consciente de la sensibilidad de esta información, revisa siempre exhaustivamente que la información publicada en los informes no suponga un riesgo adicional para la entidad fiscalizada.

Hemos revisado nuevamente el borrador de informe y no hemos encontrado información concreta que pueda ser utilizada para vulnerar ninguno de los sistemas auditados, teniendo en cuenta que no incluye información detallada de los sistemas ni de las medidas de seguridad implantadas en ORION LOGIS.

No obstante, dada la sensibilidad de los sistemas de información sanitarios y con objeto de reducir el riesgo adicional a cero, los resultados detallados que se incluían en los apartados 3 y 4 del apéndice 3 se eliminan del Informe y se comunican con carácter confidencial a los responsables de la conselleria para que puedan adoptar las medidas correctoras precisas.

Consecuencias en el Informe

Se elimina el contenido de los apartados 3 y 4 del apéndice 3 y se añade un comentario, quedando redactados así:

> **"3. Operaciones de los sistemas de información**
>
> Apartado eliminado en la fase de alegaciones.
>
> **4. Controles de acceso a datos y programas**
>
> Apartado eliminado en la fase de alegaciones.
>
> Dada la sensibilidad de los sistemas de información sanitarios y de la información tratada, y con objeto de reducir a cero el riesgo adicional en la seguridad en dichos sistemas, derivado de un posible mal uso de nuestro informe, los resultados detallados que se incluían en los apartados 3 y 4 del apéndice 3 se han eliminado en la fase de alegaciones y se comunican con carácter confidencial a los responsables de la conselleria para que puedan adoptar las medidas correctoras precisas."

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Auditoría ciberseguridad ORION LOGIS_2022_cas - SEFYCU 4681414

Puede acceder a este documento en formato PDF - PAdES y comprobar su autenticidad en la Sede Electrónica usando el código CSV siguiente:

URL (dirección en Internet) de la Sede Electrónica: https://sindicom.sedipualba.es/

Código Seguro de Verificación (CSV): KUAC JLQ7 RDNC 4MYZ W9HM

En dicha dirección puede obtener más información técnica sobre el proceso de firma, así como descargar las firmas y sellos en formato XAdES correspondientes.

Resumen de firmas y/o sellos electrónicos de este documento

Huella del documento para el firmante	Texto de la firma	Datos adicionales de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrónica - ACCV - 18/12/2023 8:02 VICENT CUCARELLA TORMO