SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

AUDITORÍA DE CIBERSEGURIDAD Y DE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE LA INFORMACIÓN DEL NUEVO SISTEMA SEDA DEL AYUNTAMIENTO DE VALÈNCIA

Situación al 30 de septiembre de 2023

RESUMEN

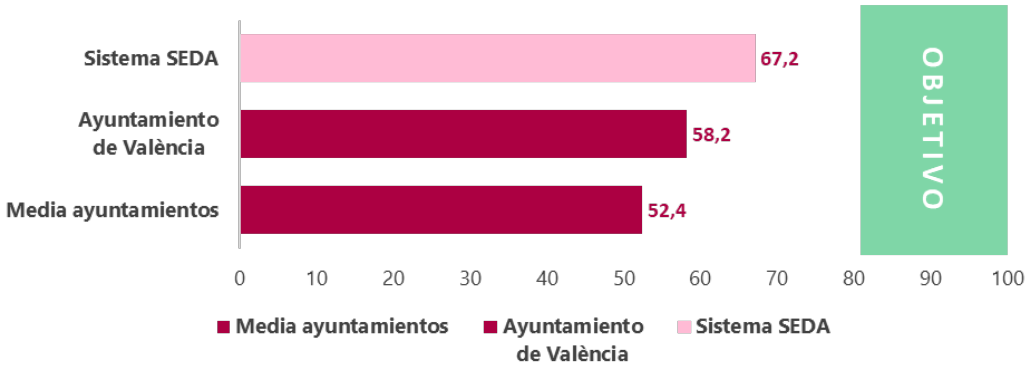
El sistema de información para la gestión de la información municipal de carácter económico-financiero y contable del Ayuntamiento de València ha sido sustituido en 2022 por la aplicación SEDA. El sistema SEDA es la versión más actual del *software ERP* de la compañía SAP.

Este cambio ha tenido como objeto la simplificación de los procesos mediante la unificación en un sistema de diversas aplicaciones municipales, el aumento de la eficacia y eficiencia en el cumplimiento de las obligaciones legales y garantizar la fiabilidad de la información económica municipal.

En sintonía con los objetivos estratégicos de la Sindicatura de Comptes, se ha realizado un trabajo de auditoría de ciberseguridad específica sobre el sistema SEDA. Este informe complementa los resultados del *Informe de seguimiento de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València del año 2019* aprobado en 2022.

Como resultado de la revisión efectuada de 44 controles detallados, cabe concluir que el grado de control existente en la gestión de los controles generales de tecnologías de la información relacionados con la ciberseguridad del sistema SEDA alcanza un índice de madurez del 67,2%. Todos los controles analizados deben mejorar para alcanzar el objetivo del 80% establecido por el Esquema Nacional de Seguridad y existen claras posibilidades de mejora para la protección de los sistemas de información.

Contextualizando los resultados obtenidos en la presente auditoría en el marco del *Informe de síntesis de las auditorías de ciberseguridad de los quince mayores ayuntamientos y de las tres diputaciones de la Comunitat Valenciana del ejercicio 2021*, podemos constatar la posición relativa del nivel de madurez general de los controles de ciberseguridad del sistema SEDA con respecto a la media de los controles básicos de ciberseguridad de los 15 ayuntamientos analizados y con el Ayuntamiento de València.



Asimismo, durante nuestra revisión hemos observado, como parte del proceso de obtención de conocimiento del sistema SEDA, que el sistema cumple con los requisitos funcionales y satisface las necesidades operativas de los usuarios, y que se ha realizado una

adecuada gestión del desarrollo y despliegue del sistema SEDA por parte de los responsables del proyecto en el Ayuntamiento y por parte de los adjudicatarios del proyecto y de su dirección.

También hemos realizado una serie de recomendaciones con el propósito de contribuir a subsanar las deficiencias observadas y mejorar la gestión de la ciberseguridad del sistema SEDA. Entre ellas aconsejamos mejorar la configuración de seguridad de los distintos entornos del sistema, finalizar la licitación para la adquisición de un sistema EDR para la protección de los dispositivos finales de usuario del Ayuntamiento, y ampliar el Plan de Contingencia para el sistema SEDA de manera que recoja y formalice la realización periódica de pruebas de recuperación planificadas para todos los tipos de copia existentes.

Con carácter general siguen vigentes las conclusiones y las recomendaciones realizadas en el informe antes citado, la más importante de las cuales se refiere a la necesaria actualización y aprobación de la Política de Seguridad de la Información del Ayuntamiento.

NOTA

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

Auditoría de ciberseguridad y de los controles generales de tecnologías de la información del nuevo sistema SEDA del Ayuntamiento de València

Situación al 30 de septiembre de 2023

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDICE (con hipervínculos)

1. INTRODUCCIÓN

Qué es el sistema SEDA

La información municipal de carácter económico-financiero y contable del Ayuntamiento de València se ha gestionado hasta 2021 a través de diferentes sistemas de información y aplicaciones informáticas, principalmente mediante el Sistema de Información Económico Municipal (SIEM), que era un aplicativo desarrollado por el propio Ayuntamiento, implantado en el año 1988, que desde entonces se adaptó y evolucionó según las necesidades de la entidad. La aplicación era mantenida íntegramente desde el Servicio de Tecnologías de la Información y Comunicación del Ayuntamiento.

Este sistema ha sido sustituido en 2022 por SEDA, que es el nuevo Sistema de Información y Gestión Económico Financiero del Ayuntamiento de València, que gestiona desde la fase de elaboración del presupuesto hasta la rendición de información a los distintos intervinientes en materia económico-financiera, y tiene por objeto:

- Simplificar los procesos, unificando en un sistema integrado las diez aplicaciones utilizadas hasta ahora para la gestión económica, financiera y contable, que estaban tecnológicamente obsoletas.

- Aumentar la eficacia y eficiencia en el cumplimiento de las obligaciones legales respecto a tramitación, obtención, remisión y publicación de información.

- Garantizar la fiabilidad de la información económica, eliminando duplicidades y minimizando errores, ya que el nuevo sistema lo facilita al basarse en el dato único.

- Establecer un sistema adaptado a las necesidades de interoperabilidad que permita desarrollar una mayor coordinación entre los diferentes niveles de la Administración pública.

- Aportar mayor transparencia y seguridad a los procesos del Ayuntamiento.

A nivel técnico, SEDA utiliza como plataforma tecnológica el producto S/4 HANA, que es la versión más actual del *software* ERP (por sus siglas en inglés, *enterprise resource planning*) de la compañía SAP, que se ofrece en modo PaaS[1], esto es, "plataforma como servicio" desde una nube privada.

[1] PaaS es una de las modalidades de servicio en la nube. PaaS proporciona al cliente todas las capacidades, funcionalidades y servicios correspondientes a procesamiento, almacenamiento, redes y sistema operativo. Una nube PaaS proporciona a la entidad usuaria la capacidad de implementar aplicaciones desarrolladas o adquiridas para su utilización posterior.

El Ayuntamiento adjudicó el contrato[2] para el desarrollo e implantación de SEDA el 17 de enero de 2020. La aplicación entró en funcionamiento el 1 de enero de 2022.

Figura 1. Datos relevantes del proyecto

Por qué realizamos esta auditoría

El artículo 6 de la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, incluye entre sus funciones, además de las referidas al control externo de la gestión económico-financiera del sector público valenciano y de sus cuentas, aquellas que de acuerdo con el ordenamiento jurídico sean convenientes para asegurar adecuadamente el cumplimiento de los principios financieros, de legalidad, de eficacia, de economía y de transparencia, exigibles al sector público, así como la sostenibilidad ambiental y la igualdad de género. Por otra parte, el artículo 11 de la misma ley establece que, en el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para **verificar la seguridad y fiabilidad de los sistemas informáticos** que soportan la información económico-financiera, contable y de gestión.

El Plan Estratégico 2019-2022 de la Sindicatura de Comptes incluye la digitalización del sector público valenciano y la transformación digital de la Administración como uno de los cuatro elementos o tendencias fundamentales[3] que debe considerar la Sindicatura de Comptes en su actividad fiscalizadora. Consecuentemente, en el anexo I de ese documento se incluyó la transformación digital de la Administración como área prioritaria de actuación para la Sindicatura.

[2] Expediente 04101/2019/58-SER. "Sist. Gestión Económico Financiero tecnología SAP S/4 HANA (lote 1), Sist. Inform. Gestión RRHH Personal tecn. SAP HCM on HANA (lote 2) y 2 Oficinas Técnicas Impulso Transf Digital-PMO (lotes 3 y 4)."

[3] Véase apartado 2.4 del Plan Estratégico 2019-2022 de la Sindicatura de Comptes.

En el *Informe de seguimiento* [en 2022] *de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València del año 2019*, aprobado el 15 de diciembre de 2022 por el Consell de la Sindicatura, se analiza la situación a 31/12/2021 de los controles básicos de ciberseguridad (CBCS) del Ayuntamiento. En este informe se incluyó la revisión de los controles relacionados con el sistema SEDA por estar a esa fecha en la fase final de implantación y se indicó que, debido a su importancia para el control interno del Ayuntamiento y frente a las crecientes ciberamenazas, sería objeto de una auditoría de ciberseguridad específica de mayor profundidad, cuyos resultados se presentan en este informe.

Las razones para realizar esta auditoría sobre la eficacia de los controles de ciberseguridad relacionados con SEDA son:

a) Los controles de ciberseguridad, básicamente los controles generales de tecnologías de la información (CGTI), deben garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos.

   Estos controles tienen gran importancia, ya que su ineficacia o mal funcionamiento impediría confiar en los controles sobre el procesamiento de la información (CPI) establecidos en SEDA. La gran complejidad técnica de la plataforma tecnológica utilizada aconsejaba realizar una auditoría en profundidad para revisar que su configuración es la adecuada.

b) Gran incremento de los ciberataques al sector local.

   En los últimos años las entidades locales se han convertido en un objetivo preferente de los ciberdelincuentes, creciendo las amenazas y los ataques padecidos por los ayuntamientos. Unos sólidos CGTI representan la defensa más eficaz frente a dichas ciberamenazas en un entorno de administración electrónica avanzada que se sustenta en sistemas de información cada vez más complejos e intensamente interconectados. La auditoría de los CGTI o controles de ciberseguridad proporciona confianza respecto de la eficacia de las ciberdefensas del ayuntamiento. En este sentido, esta auditoría complementa el informe antes citado sobre los CBCS[4] del Ayuntamiento de València.

c) Obligaciones legales.

   Además, los controles de seguridad de la información, que son el núcleo de los CGTI, son de obligado cumplimiento conforme a la normativa de aplicación, especialmente por el Esquema Nacional de Seguridad (ENS).

Adicionalmente, en el momento de emitir el presente informe, la Sindicatura está realizando una auditoría específica de los controles de procesamiento de la información en la gestión de la Tesorería del Ayuntamiento, que se encuentran soportados por el sistema SEDA. Los resultados de dicha auditoría serán publicados en un informe independiente.

[4] Los CBCS son un subconjunto de los CGTI.

Objetivos de la auditoría

Atendiendo a las razones anteriores, los objetivos de la auditoría han sido:

a) Conocer el entorno tecnológico de los sistemas que dan soporte a SEDA, identificando los riesgos principales relacionados con la seguridad de la información.

b) Identificar los CGTI existentes para mitigar los riesgos anteriores y los que posibilitan el adecuado funcionamiento de los CPI existentes en SEDA.

c) Revisar y concluir sobre el diseño, implementación y la eficacia operativa de los CGTI existentes en, o relacionados con, el sistema SEDA y sobre el grado de confianza que proporcionan, medido mediante su índice de madurez, para:

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

   - servir de fundamento para el buen funcionamiento de los CPI.

Alcance

La presente auditoría se ha centrado en el análisis de la situación de los CGTI relacionados con la aplicación SEDA, que proporciona soporte a los procesos del área económica, financiera y contable.

Hemos seleccionado para su revisión y evaluación los controles básicos de ciberseguridad (CBCS), excepto el CBCS 1, "Inventario y control de dispositivos físicos", y el CBCS 8, "Cumplimiento normativo y gobernanza de ciberseguridad", por ser de gestión general del ayuntamiento e independientes de SEDA, y hemos incluido dos CGTI de gran importancia para la configuración de la seguridad de SEDA, los "Controles de acceso a usuarios" y los de "Desarrollo de aplicaciones y gestión de cambios".

En total hemos revisado 44 controles detallados, agrupados en los 8 controles principales señalados en el cuadro 1, considerados relevantes para el proceso económico-financiero.

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 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,** aprobadas por la Conferencia de Presidentes de los Órganos de Control Externo (OCEX) el 12/11/2018, que forman parte del *Manual de fiscalización* de la Sindicatura de Comptes y que puede 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.

Los controles generales de TI incluyen los CBCS y abarcan, de manera general, la totalidad de los requisitos contemplados en el ENS.

Para valorar la situación de los controles hemos utilizado 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 Esquema Nacional de Seguridad (ENS).

Aunque lo exige el ENS, no hemos obtenido evidencia de la clasificación de seguridad (alto, medio o bajo) del sistema SEDA por parte del Ayuntamiento. A los efectos de este informe, hemos considerado que le corresponde una clasificación de categoría de seguridad MEDIA, que es la más habitual en los sistemas que soportan procesos de gestión administrativa y económico-financieros. El nivel de madurez requerido por el ENS para este tipo de sistemas es el nivel 3 (N3), proceso definido y un índice de madurez del 80%.

Los resultados detallados obtenidos para cada uno de los CGTI revisados se muestran en el cuadro 1.

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 al máximo detalle de cada uno de los controles revisados solo se comunican con carácter confidencial a los responsables del Ayuntamiento para que puedan adoptar las medidas correctoras que consideren precisas. En el presente informe los resultados se muestran de forma sintética.

2. CONCLUSIONES

Con carácter general siguen vigentes las conclusiones sobre los CBCS y las recomendaciones realizadas en nuestro *Informe de seguimiento* [en 2022] *de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València del año 2019*.

Por la importancia que tiene para el establecimiento de una adecuada ciberseguridad en el conjunto del Ayuntamiento, debemos destacar que a 30 de septiembre de 2023 seguía pendiente de actualizar y aprobar la Política de Seguridad de la Información.

En este apartado formulamos las conclusiones específicas relacionadas con la ciberseguridad y los CGTI del sistema SEDA resultado de la auditoría realizada.

El índice de madurez de los CGTI relacionados con la ciberseguridad del sistema SEDA debe mejorar para alcanzar el objetivo establecido por el ENS.

Como resultado de la revisión efectuada, cabe concluir que el grado de control existente en la gestión de los CGTI del sistema SEDA revisados alcanza un **índice de madurez del 67,2%**, que se corresponde con un nivel de madurez *N2, repetible pero intuitivo*; es decir, los controles en general se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente.

Tras la revisión de 44 subcontroles o controles detallados, agrupados en los 8 controles principales, agregando los resultados obtenidos según la clasificación incluida en la *GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica*, se obtienen los resultados mostrados en el cuadro 1.

Cuadro 1. Índice de madurez por áreas de los controles de ciberseguridad

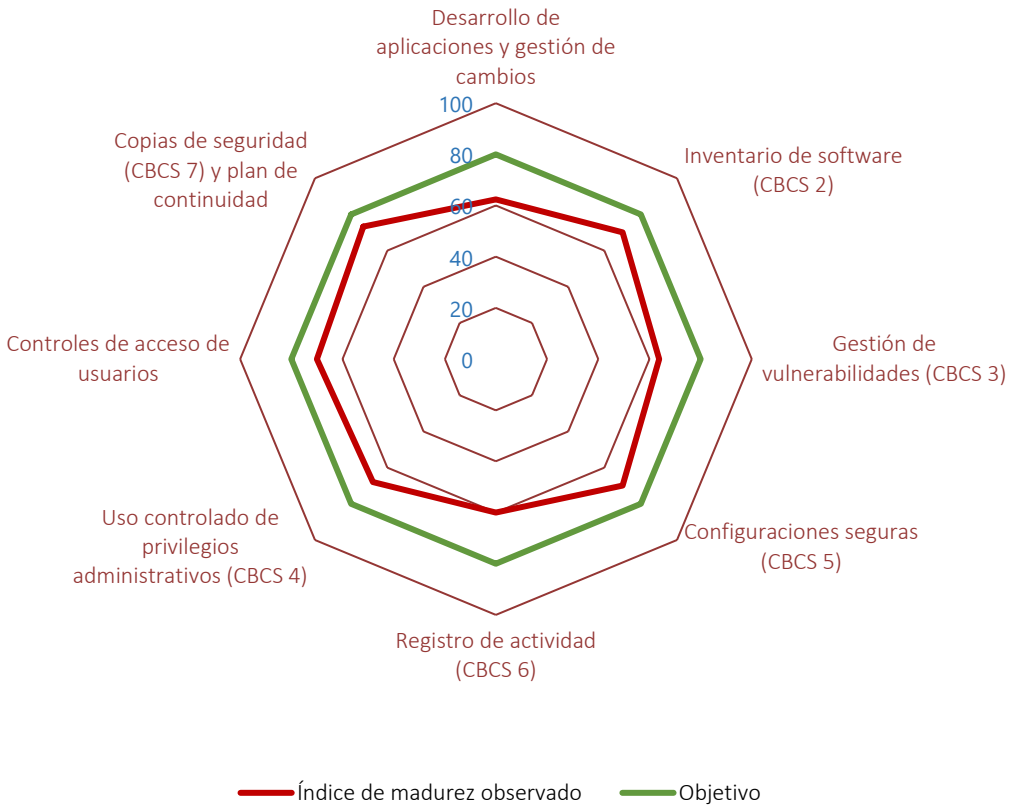
Áreas	Controles principales	Índice de madurez
B. Cambios en aplicaciones y sistemas	B2/B3 Desarrollo de aplicaciones y gestión de cambios	62,4%
C. Operaciones de los sistemas de información	C.1 Inventario de *software* (CBCS 2)	70,0%
	C.2 Gestión de vulnerabilidades (CBCS 3)	63,8%
	C.3 Configuraciones seguras (CBCS 5)	70,0%
	C.4 Registro de actividad (CBCS 6)	60,0%
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS 4)	68,0%
	D2/D3/D4 Controles de acceso de usuarios	70,0%
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	73,3%
	General	**67,2%**

En el apéndice se comenta con detalle la situación observada de estos controles.

El nivel de efectividad en los controles analizados debe mejorar, ya que ninguno alcanza el nivel del 80% objetivo y existen claras posibilidades de mejora para alcanzar el nivel de madurez N3 requerido por el ENS para la protección de los sistemas de información de nivel medio. En el apartado 5 se realizan las recomendaciones pertinentes con esa finalidad.

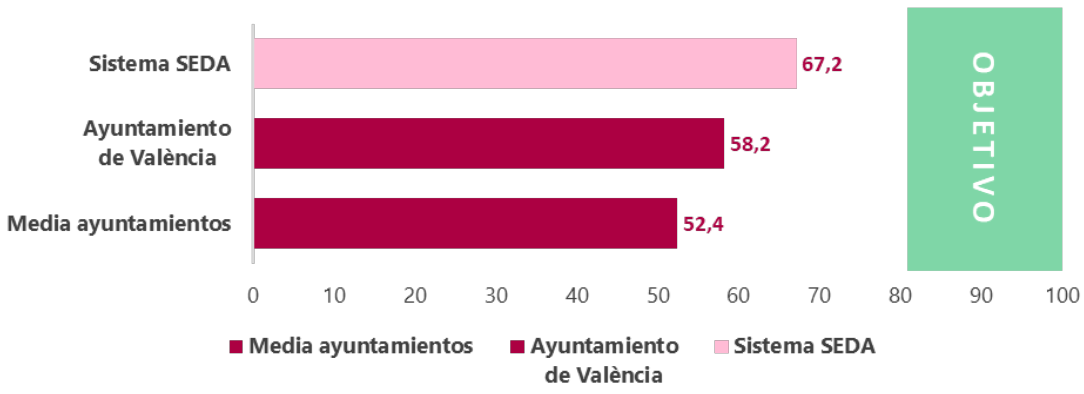
La situación observada de los controles queda reflejada en el gráfico 1.

Gráfico 1. Índice de madurez, por áreas, de los controles de ciberseguridad



Contextualizando los resultados obtenidos en el presente trabajo en el marco del *Informe de síntesis de las auditorías de ciberseguridad de los quince mayores ayuntamientos y de las tres diputaciones de la Comunitat Valenciana. Ejercicio 2021*, podemos constatar (véase gráfico 2) la posición relativa del nivel de madurez general de los controles de ciberseguridad del sistema SEDA con respecto a la media de los controles básicos de ciberseguridad a 31/12/2021 de los 15 ayuntamientos analizados y con el Ayuntamiento de València.

Gráfico 2. Índices de madurez comparados



Se ha realizado una adecuada gestión del proyecto de desarrollo y despliegue del sistema SEDA y el sistema cumple con los requisitos funcionales y satisface las necesidades operativas de los usuarios.

Aunque revisar la gestión del proyecto de implantación de SEDA no ha formado parte de los objetivos de esta auditoría, durante su ejecución, como parte del proceso de obtención de conocimiento del sistema SEDA, hemos constatado que dicha gestión ha sido realizada con un buen nivel de competencia por parte de los responsables del proyecto en el Ayuntamiento y por parte de los adjudicatarios del proyecto y de su dirección.

Hemos verificado mediante entrevistas con determinados responsables que:

- Se ha realizado una adecuada aplicación de las metodologías de gestión de proyectos y de desarrollo de aplicaciones.
- Ha existido una elevada implicación de los responsables de proyecto y el respaldo de los órganos superiores del Ayuntamiento, factor clave para el desarrollo y la implantación exitosa de un proyecto TI tan complejo.
- Se ha realizado una ejecución competente del proyecto por parte del adjudicatario y una adecuada dirección independiente de este.
- Se ha realizado una adecuada gestión de requisitos funcionales, facilitando la adaptación de la herramienta a las necesidades operativas de los distintos servicios.

Esta gestión adecuada del proyecto ha tenido, como consecuencias más destacables:

- El cumplimiento de los objetivos de proyecto definidos en base a los requisitos funcionales identificados.
- El cumplimiento de plazos planificados para la puesta en operación del sistema sin exceder el presupuesto.
- La aceptación y adaptación por parte de los usuarios finales al nuevo aplicativo y a los nuevos procesos de gestión asociados.
- La ausencia de incidencias relevantes que hayan mermado la capacidad operativa del sistema y la confianza de la organización en el nuevo aplicativo.

3. RESPONSABILIDADES DE LOS ÓRGANOS DEL AYUNTAMIENTO

Los órganos superiores del Ayuntamiento son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones. De acuerdo con sus competencias, deben garantizar que el funcionamiento de la entidad resulte conforme con las normas aplicables y que los controles internos proporcionen una garantía razonable de que la información, los servicios y los sistemas de información que les dan

soporte cumplan las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el ENS: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Adicionalmente a la responsabilidad sobre la seguridad de los sistemas de información, el establecimiento y aplicación práctica de las medidas de seguridad la deben asumir los órganos y roles designados en las políticas de seguridad de la información aprobadas por el Ayuntamiento, principalmente el Comité de Seguridad TIC y el responsable de seguridad.

Por otra parte, la responsable funcional de SEDA ha definido, durante las fases de desarrollo y despliegue del sistema, los requisitos para su desarrollo, la validación de las pruebas funcionales realizadas, la tipología de usuarios y su asignación al personal del Ayuntamiento ejerciendo funciones de responsable del servicio y de la información para este sistema.

4. RESPONSABILIDAD DE LA SINDICATURA DE COMPTES

Nuestro objetivo ha sido obtener una seguridad limitada y concluir sobre la situación de los controles generales de tecnologías de la información revisados, proporcionando una evaluación sobre su diseño e implementación y, en su caso, formular recomendaciones que contribuyan a la subsanación de las deficiencias observadas y a la mejora de los procedimientos de control.

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. 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 realizado sobre los sistemas de información, este se ha efectuado por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI), con la asistencia de una firma especializada.

Consideramos que la evidencia de auditoría obtenida proporciona una base suficiente y adecuada para fundamentar nuestras conclusiones sobre el estado de los CGTI relacionados con el sistema SEDA, 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.

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.

5. RECOMENDACIONES

Con carácter general siguen siendo aplicables las recomendaciones realizadas en nuestro *Informe de seguimiento* [en 2022] *de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València del año 2019*.

Con la finalidad de ayudar a subsanar las deficiencias identificadas en la presente auditoría y mejorar los niveles de control señalados en el apartado 2, en este apartado realizamos las recomendaciones relacionadas con el sistema SEDA, dirigidas al Comité de Seguridad TIC y al resto de roles de seguridad designados o que se designen conforme a la política de seguridad de la información del Ayuntamiento, que está pendiente de actualizarse.

Sobre el desarrollo de aplicaciones y la gestión de cambios (B2/B3)

1. Aprobar formalmente un procedimiento para la gestión continua de cambios en SEDA, que especifique los siguientes requisitos:

   - Registro de todas las solicitudes de cambio, incluidos los urgentes debido a necesidades sobrevenidas o para la solución de incidencias y los originados desde el equipo técnico o desde los responsables funcionales del servicio.
   - Evaluación de las solicitudes teniendo en cuenta los riesgos de seguridad.
   - Autorización de los cambios por parte del personal responsable, previamente a su pase a producción.
   - Realización de pruebas, con carácter previo a la implantación del cambio y aceptación por parte del usuario final y de los responsables funcionales correspondientes.
   - Planificación de puesta en funcionamiento del cambio.
   - Mejorar la gestión documental del proceso e incluir toda la información necesaria.

Sobre el inventario y control de *software* autorizado (C1/CBCS 2)

2. Elaborar y aprobar un procedimiento para la gestión de componentes del sistema SEDA, que contemple las medidas actualmente implantadas:

- El inventario y control de componentes instalados en el sistema.
- La gestión de licencias.
- La gestión de versiones de los distintos componentes con objeto de asegurar el soporte del fabricante.
- La gestión de interfaces y conexiones con elementos externos al sistema y las medidas de seguridad aplicadas a estas.

Sobre el proceso continuo de identificación y remediación de vulnerabilidades (C2/CBCS 3)

3. Elaborar y aprobar un procedimiento para la identificación y resolución de vulnerabilidades del sistema SEDA, que contemple, además de las medidas actualmente implantadas, la priorización basada en el análisis de riesgos, la resolución y la documentación de las vulnerabilidades tratadas.

Sobre las configuraciones seguras del *software* y *hardware* (C3/CBCS 5)

4. Mejorar la configuración de seguridad de los distintos entornos del sistema, producción, preproducción y desarrollo.

5. Finalizar la licitación para la adquisición de un sistema EDR para la protección de los dispositivos finales de usuario (*endpoint*) del Ayuntamiento.

Sobre el registro de actividad de los usuarios (C4/CBCS 6)

6. Elaborar y aprobar formalmente un procedimiento para el tratamiento de registros de actividad de los usuarios del sistema SEDA, que especifique, como mínimo, la información que se retiene, el periodo de retención, copias de seguridad, gestión de derechos de acceso al registro e implantación y documentación de un proceso de revisión de los *logs* (aunque este proceso no es de aplicación obligatoria según el ENS).

Sobre el uso controlado de privilegios administrativos (D1/CBCS 4)

7. Elaborar y aprobar un procedimiento que describa la gestión de los usuarios que disponen de derechos de acceso privilegiados sobre el sistema SEDA.

Sobre el control de acceso de los usuarios (D2/D3/D4)

8. Elaborar y aprobar un procedimiento de control de acceso para el sistema SEDA que describa el control implantado en la actualidad e incluya el detalle necesario sobre la identificación y autenticación de los usuarios, la gestión y provisión de derechos de acceso y su gestión continuada. También debería analizarse la conveniencia de utilizar

herramientas automatizadas para gestionar este proceso, que actualmente se realiza de manera manual.

Sobre la copia de seguridad de datos y sistemas (E1/CBCS 7)

9. Ampliar el Plan de Contingencia para el sistema SEDA de manera que recoja y formalice la realización periódica de pruebas de recuperación planificadas para todos los tipos de copia existentes.

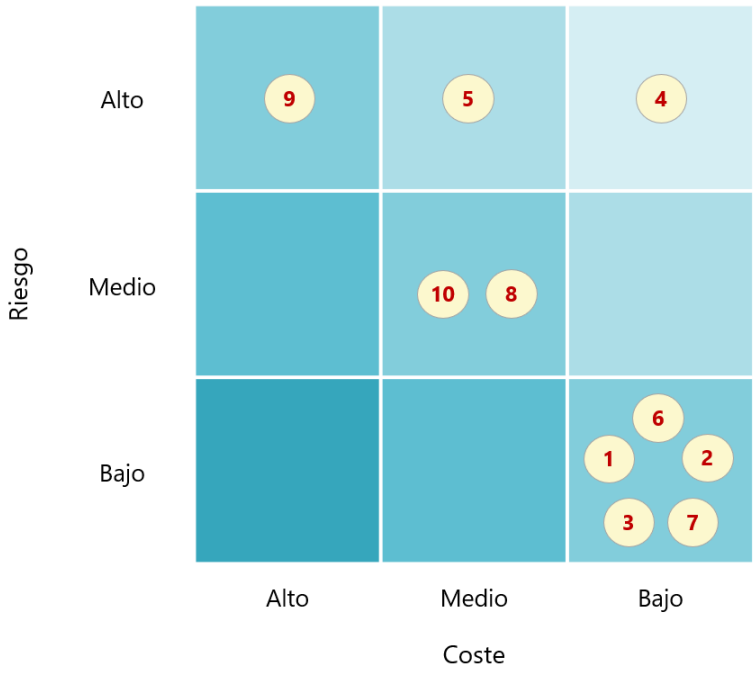
Sobre la disponibilidad de los sistemas

10. Elaborar y aprobar un Plan de Continuidad de la Actividad corporativo y de aplicación en todo el Ayuntamiento, que incluya el análisis sobre elementos críticos de negocio existente, la estrategia de continuidad, los planes particulares de contingencia de los sistemas del Ayuntamiento (incluido el Plan de Contingencia del sistema SEDA) y la ejecución planificada de pruebas periódicas del plan. No obstante, este proceso no es de aplicación obligatoria según el ENS.

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico 3 se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación.

Gráfico 3. Riesgos que se atienden y coste de implantación de las recomendaciones



APÉNDICE

Situación de los controles auditados

A continuación, se detallan las observaciones y deficiencias de control obtenidas en nuestra auditoría. En el apartado 2 de este informe se han incluido las conclusiones más relevantes y en el apartado 5, las recomendaciones que derivan de esta revisión.

Con carácter previo y para facilitar la comprensión de algunas observaciones que siguen, señalamos que los agentes que han intervenido en la gestión de la aplicación SEDA son:

- Responsable funcional del Ayuntamiento: la Viceintervención de Contabilidad.
- Responsable técnico del Ayuntamiento: el Servicio de Tecnologías de la Información y Comunicación.
- Desarrollador del proyecto SEDA y proveedor del servicio *cloud* en modalidad PaaS: el adjudicatario del contrato de desarrollo del sistema (lote 1)[5].
- Dirección del proyecto: el adjudicatario del lote 3 del contrato anterior.
- Mantenimiento del sistema SEDA: el adjudicatario del contrato de mantenimiento del sistema[6].

1. Desarrollo de aplicaciones y gestión de cambios (B2/B3)

Objetivo de control

Disponer de un procedimiento para el desarrollo de aplicaciones y sistemas de forma que se tenga en consideración los criterios de seguridad y asegure que los cambios realizados se gestionan de manera metodológica, incluyendo su análisis, comunicación y registro.

Por qué es importante este control

Cualquier cambio realizado en los sistemas de información, si se realiza de manera no planificada, puede suponer un riesgo para el correcto funcionamiento de estos sistemas o facilitar la realización de fraudes. La implantación de nuevas aplicaciones o la modificación de las existentes sin aplicar los controles de una buena metodología podrían poner en riesgo la estabilidad de los sistemas de información utilizados en la entidad.

Es esencial en la ejecución de las tareas de gestión de cambios y desarrollo de aplicaciones la aprobación de procedimientos que regulen cómo se deben realizar los cambios en componentes del sistema y su configuración. Además, deben designarse los órganos o personas responsables de realizar y aprobar las diferentes fases de esos cambios y asegurar

[5] El contrato "Sist.Gestión Económico Financiero tecnología SAP S/4 HANA (lote 1), Sist Inform Gestión RRHH Personal tecn SAP HCM on HANA (lote 2) y 2 Oficinas Técnicas Impulso Transf Digital-PMO (lotes 3 y 4). Expediente 04101/2019/58-SER." Fue adjudicado el 15 de mayo de 2020 a la empresa IECISA.

[6] El contrato "Servicio de mantenimiento correctivo, evolutivo y adaptativo del Sistema de Gestión Económico-Financiero del Ayuntamiento de València, con tecnología SAP S/4 HANA (SEDA). Expediente 04101/2022/112-SER2" fue adjudicado el 9 de noviembre de 2022 a la empresa Inetum España, SA.

que se realizan las pruebas previas a la implantación de esos cambios en los sistemas de gestión en uso.

Situación del control

El Ayuntamiento dispone de una normativa, escrita y formalmente aprobada, para la realización de desarrollos a medida en el entorno SAP, que incluye una descripción detallada de la metodología a utilizar, incluyendo aspectos relevantes como el aseguramiento de la calidad de código fuente.

La aceptación de los desarrollos realizados se efectúa mediante correo electrónico por el responsable del módulo al que está destinado el desarrollo, y posteriormente por la responsable funcional del Ayuntamiento, documentándose como parte del proceso de gestión de cambios. Hemos verificado mediante muestreo sobre las órdenes de transporte registradas que, para aquellos cambios que por su naturaleza lo requieren, se realizan pruebas, pero de manera general estas no se documentan.

Hemos verificado que existe un control efectivo sobre la gestión de cambios, que es un proceso correctamente diseñado e implantado y que, finalizada la fase de puesta en operación del sistema, se aplica a la totalidad de los cambios efectuados. No obstante, aunque existen procedimientos aprobados que abordan parcialmente la gestión de cambios, no describen completamente el control.

El control de cambios se encuentra respaldado por el uso combinado de herramientas de registro de incidencias corporativas, herramientas ofimáticas específicas y subprocesos manuales. Las solicitudes de cambio son registradas y procesadas en estas herramientas, facilitando su revisión y aprobación por parte de los responsables funcionales, incluidos los cambios urgentes debido a necesidades sobrevenidas o para la solución de incidencias, que son registrados con posterioridad a la resolución de la incidencia.

Hemos verificado que, para determinados cambios registrados, la información contenida en el registro es incompleta o imprecisa y, de manera general, no se incluye información sobre las pruebas realizadas ni la aprobación previa al transporte a producción.

En cuanto a capacidad para la ejecución de los cambios, hemos realizado pruebas para identificar aquellos usuarios que disponen de privilegios para promover cambios en el entorno de producción y hemos verificado que, durante la fase inicial de puesta en explotación, existía un número excesivo de usuarios con esta capacidad, en una deficiente aplicación del principio de mínimo privilegio. No obstante, esta deficiencia de control ha sido subsanada una vez finalizada la fase inicial de puesta en operación del sistema.

Se dispone de entornos de desarrollo y de preproducción separados del de producción. Estos entornos han sido configurados considerando requisitos de seguridad, y las rutas de transporte entre estos se encuentran adecuadamente configuradas. Además, hemos verificado que se han aplicado configuraciones de seguridad sobre modificación de parámetros con afección a los distintos entornos, aunque se han identificado posibilidades de mejora.

La valoración de este control alcanza un **índice de madurez del 62,4%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero los procedimientos no han sido formalizados documentalmente.

2. Inventario de *software* (CBCS 2)

Objetivo de control

Gestionar activamente (inventariar, revisar y corregir) todo el *software*, de forma que solo se pueda instalar y ejecutar *software* autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

Por qué es importante este control

Mantener un inventario actualizado de *software* es importante, ya que permite conocer qué hay que proteger.

Situación del control

El Ayuntamiento ha establecido un control efectivo para la gestión de los módulos de la aplicación SEDA, las licencias asociadas y las interfaces autorizadas con otras aplicaciones. No obstante, no se dispone de un procedimiento escrito y aprobado que defina las medidas de control implantadas.

El Ayuntamiento realiza, a través del adjudicatario del contrato de mantenimiento del sistema, la gestión y revisión de los módulos desplegados en SEDA mediante una herramienta propietaria proporcionada por el fabricante del sistema. Se realiza periódicamente la revisión de los componentes instalados, verificando que los módulos desplegados en el sistema se encuentran en versiones soportadas por el fabricante. En estas revisiones se incluye tanto la verificación de los componentes del sistema como de los sistemas operativos, bases de datos y demás sistemas subsidiarios.

Además, el Ayuntamiento realiza una correcta y exhaustiva gestión del licenciamiento de la aplicación. Esta gestión se realiza de manera conjunta por el adjudicatario del mantenimiento del sistema y la responsable funcional de la aplicación en el Ayuntamiento, e incluye la gestión de usuarios del sistema, sus funciones, los permisos necesarios para su ejecución y las licencias necesarias. Esta gestión continua del licenciamiento permite contener y limitar los costes asociados a la explotación del sistema, proporcionando los recursos únicamente a aquellos empleados que por sus funciones necesitan hacer uso de la aplicación.

Hemos verificado que existe un control efectivo sobre las comunicaciones del sistema con elementos externos. El Ayuntamiento dispone de un inventario actualizado de las interfaces del sistema SEDA con sistemas externos, inventario que se encuentra correctamente actualizado y mantenido. Además, hemos comprobado que han sido aplicadas medidas de seguridad específicas para la protección de dichas interfaces, particularmente aquellas que requieren del acceso a carpetas del sistema, incluyendo una correcta gestión de los usuarios y sus privilegios de acceso.

Además, para las comunicaciones entre sistemas SAP, hemos verificado que existe un inventario de conexiones para el intercambio de datos y nos han indicado que la totalidad de conexiones existentes se encuentran gestionadas y en uso.

Este control alcanza un **índice de madurez del 70,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero los procedimientos no han sido formalizados documentalmente.

3. Proceso continuo de identificación y remediación de vulnerabilidades (CBCS 3)

Objetivo de control

Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.

Por qué es importante este control

La finalidad de este control es conocer y eliminar debilidades técnicas que puedan existir en los sistemas de información de la entidad, reduciendo la probabilidad de que los sistemas sean vulnerables.

Situación del control

Hemos analizado la gestión de las vulnerabilidades del sistema SEDA y hemos observado que han sido implantadas medidas para su identificación y resolución, en un proceso de gestión manual pero efectivo.

No obstante, aunque existe una norma interna que aborda parcialmente la gestión de parches, carece del detalle necesario y no se dispone de un procedimiento específico, escrito y formalmente aprobado que detalle las acciones para la gestión de riesgos y vulnerabilidades del sistema SEDA actualmente implantadas.

La identificación de vulnerabilidades de la aplicación la realiza el adjudicatario del mantenimiento del sistema y se basa en el análisis de notas y avisos de seguridad emitidos por el fabricante del sistema. En caso de identificar vulnerabilidades que puedan afectar al sistema SEDA, se informa a los responsables funcional y técnico del Ayuntamiento para validar y programar las acciones pertinentes, realizándose acciones para la resolución de todas ellas. Este proceso es extensivo tanto a la aplicación como a las bases de datos y los sistemas operativos que la soportan. Su gestión es manual pero efectiva, no utilizándose herramientas específicas para la gestión de vulnerabilidades y de las tareas correctivas.

Hemos verificado que el adjudicatario del mantenimiento del sistema aplica los parches que el fabricante recomienda para su mantenimiento, como parte del proceso de gestión de vulnerabilidades implantado y que se encuentra recogido y detallado en la documentación contractual que regula el servicio de mantenimiento y soporte del sistema SEDA.

Los sistemas físicos y de comunicaciones de la infraestructura que soportan la aplicación son mantenidos por el proveedor del servicio *cloud*, incluyendo la gestión de vulnerabilidades. Este dispone de diversas certificaciones de seguridad que proporcionan una seguridad razonable de que las vulnerabilidades de dichos sistemas son gestionadas adecuadamente y está especificado en las cláusulas del contrato.

La valoración global del control da un **índice de madurez del 63,8%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero los procedimientos no han sido formalizados documentalmente.

4. Configuraciones seguras (CBCS 5)

Objetivo de control

Establecer una configuración base segura del *software* y *hardware* de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente, utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.

Por qué es importante este control

Por defecto, la mayoría de los sistemas están configurados para facilitar su uso y no necesariamente pensando en la seguridad. Tal como lo entregan los fabricantes y vendedores, cuando se recibe un equipo es habitual encontrarse con controles poco robustos, servicios y puertos abiertos, cuentas o contraseñas predeterminadas, protocolos antiguos, *software* preinstalado innecesario. Todos estos aspectos son vulnerables en su estado predeterminado.

Para implantar de manera efectiva este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad. El desarrollo de opciones de configuración con buenas propiedades de seguridad no es una tarea sencilla y va más allá de la capacidad de los usuarios individuales, requiriendo análisis a veces complejos y costosos para tomar buenas decisiones. Por esta razón, es altamente recomendable el seguimiento y aplicación de buenas prácticas que algunos organismos publican en materia de seguridad, aplicables a dispositivos y sistemas.

Incluso si se desarrolla e instala una configuración inicial fuerte, debe ser revisada y actualizada continuamente para evitar el deterioro de la seguridad, en particular, cuando el *software* se actualiza o parchea, se divulgan las nuevas vulnerabilidades de la seguridad, o las configuraciones se ajustan para permitir la instalación de nuevos programas o para dar soporte a nuevos requerimientos operacionales. Si no se revisa y actualiza de forma continua, los atacantes encontrarán oportunidades para explotar tanto el *software* como los servicios accesibles en la red.

Situación del control

El Ayuntamiento dispone del documento "Diseño de Seguridad Lógica y Física" que recoge las normas, buenas prácticas, nomenclaturas y procedimientos referentes a la seguridad

lógica y física. Este documento detalla aspectos clave para la configuración segura del sistema SEDA.

Hemos verificado determinadas configuraciones críticas del sistema y hemos confirmado que, en general, se aplica lo especificado en el documento de seguridad, incluyendo la eliminación de cuentas por defecto. No obstante, existen determinadas carencias que deben ser subsanadas.

La configuración de seguridad de los distintos entornos es correcta, aunque existen posibilidades de mejora, tal y como se ha especificado en el control "Desarrollo de aplicaciones y gestión de cambios".

Para la configuración de los sistemas operativos que soportan la aplicación y las bases de datos del sistema, el adjudicatario del mantenimiento dispone de guías corporativas que detallan configuraciones específicas de seguridad y son actualizadas periódicamente.

Hemos revisado el estado de la licitación para adquisición de un sistema EDR para protección de la red y dispositivos finales de usuario y nos han indicado que no se han realizado avances con respecto a la situación reportada en el *Informe de seguimiento [en 2022] de las recomendaciones realizadas en el informe de auditoría de los controles básicos de ciberseguridad del Ayuntamiento de València del año 2019*. Nos han indicado que se han habilitado nuevos mecanismos dinámicos de contratación y se ha previsto su utilización para el suministro del sistema EDR, sobre el que se han realizado pruebas de concepto con distintos fabricantes y se han definido requisitos para la elaboración de los pliegos técnicos.

La valoración global del control da un **índice de madurez del 70,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos.

5. Registro de actividad de los usuarios (CBCS 6)

Objetivo de control

Desarrollar procesos y utilizar herramientas para recoger, gestionar y analizar los registros de actividad (*logs*) de eventos que puedan ayudar a detectar, entender o recuperarse de un ataque.

Por qué es importante este control

Deficiencias en los registros de seguridad y en su análisis permiten a los atacantes ocultar su ubicación, el *software* malicioso introducido y las actividades ilícitas que realizan en las máquinas víctimas. Incluso si los entes atacados saben que sus sistemas han sido comprometidos, sin *logs* completos y protegidos, permanecen ciegos a los detalles del ataque y a las posteriores acciones de los atacantes.

Sin unos *logs* de auditoría sólidos, un ataque puede pasar desapercibido por tiempo indefinido y los daños infligidos pueden ser irreversibles. Debido a deficientes o inexistentes procesos de análisis de registros, a veces los atacantes controlan las máquinas

víctima durante meses o años sin que nadie se percate en la organización de destino, a pesar de que la evidencia del ataque consta en dichos registros no examinados.

Situación del control

Aunque el sistema SEDA permite configurar el almacenamiento de *logs* de auditoría y la gestión del periodo de almacenamiento, el Ayuntamiento no dispone de ningún procedimiento aprobado que recoja los parámetros de recolección de *logs,* que determine el periodo de almacenamiento, ni los análisis que se deben realizar.

Hemos verificado que el *log* de auditoría se encuentra habilitado en los servidores de la aplicación, y que existen configuraciones para asegurar un almacenamiento mínimo de 30 días para los registros de actividad. Además, este periodo de retención se encuentra extendido por las copias de seguridad de datos y sistema que se realizan. No obstante, este periodo no ha sido formalmente definido, ni establecido en base a criterios funcionales.

El Ayuntamiento no ha implantado un sistema de revisión sobre el *log* de auditoría con el objetivo de identificar acciones no autorizadas realizadas por los usuarios y únicamente se realizan revisiones en caso de incidente.

Además, no se han integrado los *logs* del sistema SEDA en el SIEM corporativo ni en otro sistema de correlación de eventos, con el objeto de identificar comportamientos anómalos en la red y sistemas corporativos.

La valoración global del control alcanza un **índice de madurez del 60,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero existen controles parcialmente establecidos o los procedimientos no han sido formalizados documentalmente.

6. Uso controlado de privilegios administrativos (CBCS 4)

Objetivo de control

Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir la asignación y uso de privilegios administrativos en los sistemas de información.

Por qué es importante este control

Este control garantiza que los privilegios de administración de los sistemas estén asignados únicamente a los empleados que los necesitan, en base a las funciones que desempeñan (principio de mínimo privilegio) y que la entidad pueda atribuir las acciones administrativas a usuarios identificables (trazabilidad).

Desafortunadamente, para facilitar la agilidad y la comodidad, muchas organizaciones permiten que su personal tenga derechos de administrador tanto a nivel de una aplicación de gestión como en los sistemas que le dan soporte (sistema operativo, base de datos, etc.), así como en sus equipos. Esta situación deriva en la existencia del riesgo de acceso y de cambios no autorizados a los sistemas y datos, que puede materializarse utilizando los

privilegios excesivos de un usuario como puerta de entrada para acceder desde fuera a la red interna de la entidad.

Este control conlleva que las cuentas de usuarios administradores de aplicaciones, bases de datos, sistemas operativos y equipos de usuario deben estar identificadas y su uso controlado, eliminando las que no se utilizan y cambiando las contraseñas que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

Situación del control

El Ayuntamiento no dispone de un inventario formal de gestión de cuentas de administración del sistema SEDA. Además, no existe un procedimiento para la gestión de dichas cuentas.

Hemos verificado que los usuarios que disponen de derechos de administración sobre el sistema forman parte en su totalidad del equipo de operadores y desarrolladores del adjudicatario del mantenimiento. Estos usuarios no realizan una explotación funcional de la aplicación ni se encuentran implicados en ninguno de los procesos de gestión del Ayuntamiento.

La autenticación de usuarios con privilegios de administración del sistema SEDA se realiza mediante el uso de contraseñas asociadas a las cuentas de usuario, del mismo modo que se realiza para el resto de los usuarios. Los requisitos de autenticación mediante contraseña se encuentran adecuadamente establecidos en el procedimiento de configuración de la seguridad, que está formalmente aprobado, y hemos verificado que el sistema se encuentra configurado considerando los criterios establecidos en dicho documento.

Hemos identificado al conjunto de los usuarios que disponen de perfiles SAP_ALL que proporcionan derechos críticos sobre el sistema. El conjunto de estos derechos proporciona un acceso completo a las funciones y datos del sistema y debe ser restringido a un uso de emergencia, limitando su asignación a cuentas de usuarios utilizadas únicamente para la resolución de problemas que lo requieran. Durante la fase de puesta en operación de la aplicación, este conjunto estaba constituido por un total de 29 usuarios, siendo este un número de usuarios elevado, lo que supone una deficiencia grave de control por los riesgos que representa. Esta situación ha sido subsanada una vez superada la fase de puesta en operación del sistema.

Sobre la auditoría y control de las acciones de los usuarios con derechos críticos sobre el sistema, aunque existen usuarios con los privilegios adecuados para verificar las entradas al sistema y las transacciones y programas ejecutados, no hemos podido verificar que exista un proceso establecido para la revisión periódica de sus acciones.

En cuanto al control de acceso a la base de datos del sistema, hemos verificado que se encuentra adecuadamente implementado en tanto que solo los usuarios administradores disponen de acceso privilegiado.

Hemos verificado que para las cuentas por defecto se ha modificado la contraseña o bien no existen en todos los entornos, considerándose adecuada su implementación.

La valoración global del control supone un **índice de madurez del 68,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero los procedimientos no han sido formalizados documentalmente.

7. Controles de acceso de usuarios (D2/D3/D4)

Objetivo de control

Disponer de mecanismos que permitan la identificación segura de los usuarios, gestionar y limitar su acceso a los recursos de los sistemas y gestionar sus privilegios para realizar una correcta provisión de derechos de acceso.

Por qué es importante este control

Establecer mecanismos de identificación a todos los usuarios que acceden a los sistemas o aplicaciones de las entidades es la única manera de conocer quién recibe determinados derechos de acceso o quién ha realizado acciones concretas.

Para acceder a los distintos sistemas o aplicaciones, los usuarios deberán utilizar sus identificadores singulares y existir, además, mecanismos que permitan validar su identidad.

Sin un proceso adecuado de gestión de derechos de acceso, los sistemas o aplicaciones pueden albergar usuarios con mayores privilegios de los que requieren sus funciones. Una adecuada gestión de altas, bajas y modificación de usuarios permite a las organizaciones mantener un inventario actualizado de usuarios, de manera que únicamente los usuarios actuales acceden a los sistemas y aplicaciones a los que se ha autorizado el acceso.

Situación del control

Hemos analizado los controles de acceso de los usuarios al sistema SEDA y hemos verificado que existe un control efectivo, pero que dicho control no se encuentra contemplado en un procedimiento formalmente aprobado.

La identificación de usuarios del sistema SEDA se realiza mediante usuarios locales y su autenticación mediante el uso de contraseñas asociadas a dichas cuentas. Los requisitos de autenticación mediante contraseña se encuentran establecidos en el procedimiento de configuración de la seguridad, que está formalmente aprobado. Además, hemos verificado que el sistema se encuentra configurado considerando los criterios establecidos en dicho documento.

La gestión de derechos de acceso de los usuarios a los distintos módulos del sistema se realiza de manera manual, dado que no se dispone de herramientas automatizadas. No obstante, el proceso establecido, cuya responsabilidad se encuentra compartida entre los responsables del sistema en el Ayuntamiento y la empresa adjudicataria del mantenimiento, se encuentra adecuadamente diseñado e implantado.

Hemos verificado que el proceso de asignación de derechos de accesos es efectivo y se encuentra bien ejecutado. Los privilegios de los usuarios del sistema, aplicados mediante roles y objetos de autorización, se corresponden con aquellos que han sido asignados por los responsables, con una aplicación correcta del principio de mínimo privilegio. Los responsables del sistema SEDA en el Ayuntamiento han modelizado los puestos de trabajo, establecido tipos y subtipos de usuarios y una descripción detallada de sus atribuciones.

Además, hemos realizado una revisión de los roles asignados al grupo completo de usuarios del departamento de Tesorería del Ayuntamiento y hemos verificado que la asignación de derechos es adecuada y se corresponde con la realizada por los responsables.

La gestión de bajas o modificación de usuarios es efectiva y se ejecuta correctamente, siendo su gestión particularmente exhaustiva. Se realiza de manera parcialmente manual por parte de los responsables del sistema en el Ayuntamiento, que mantienen una comunicación constante con los responsables de los distintos servicios, que informan de todos los cambios producidos en los equipos de trabajo. Hemos verificado mediante muestreo que, para aquellos usuarios del sistema que cesan o modifican sus funciones en el Ayuntamiento, se realizan las modificaciones necesarias en sus perfiles.

Para el control de los accesos desde internet, fuera de la red del Ayuntamiento, adicionalmente al uso de usuario y contraseña, se utiliza una conexión VPN corporativa que dispone de doble factor de autenticación que se encuentra en fase de despliegue en el momento de realización de la auditoría.

En síntesis, la valoración global del control alcanza un **índice de madurez del 70,0%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo***; es decir, los controles se realizan, pero los procedimientos no han sido formalizados documentalmente.

8. Copia de seguridad de datos y sistemas (CBCS 7)

Objetivo de control

Utilizar procesos y herramientas para realizar copias de seguridad de la información crítica con una metodología que permita su recuperación 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 o las consecuencias de los incidentes no provocados intencionadamente se pueden mitigar si se dispone de copia de seguridad de los datos afectados.

Situación del control

El Ayuntamiento ha implantado un proceso para realizar copias de seguridad que se encuentra recogido en el Plan de Contingencia para el sistema SEDA, que está formalmente aprobado por los responsables del proyecto.

El control se encuentra respaldado por el uso de dos herramientas de copia, una para la copia de la aplicación y otra para la copia de la base de datos, siendo ambas herramientas administradas y gestionadas por el adjudicatario del mantenimiento, que proporciona el servicio *cloud* que alberga los equipos y sistemas que soportan este proceso.

Hemos verificado que el proceso de copias de seguridad establecido está correctamente diseñado e implementado y es efectivo. El adjudicatario del mantenimiento reporta sobre el resultado de las copias realizadas como parte de un informe de estado del sistema y del servicio que es elaborado y remitido diariamente, y revisado por los responsables del Ayuntamiento.

Pero no se realizan pruebas de restauración planificadas y su realización no se encuentra recogida en el Plan de Contingencia. No obstante, sí se realizan recuperaciones de copias debido a incidencias y pérdidas de datos.

Durante la fase de puesta en producción del proyecto fueron realizadas pruebas de recuperación de las bases de datos que componen el sistema, adecuadamente planificadas, ejecutadas y documentadas.

Las copias se encuentran duplicadas en dos ubicaciones, lo que proporciona redundancia de datos reduciendo los riesgos de pérdida de información en caso de incidente. La ubicación secundaria únicamente almacena copias de seguridad, y no alberga sistemas para la ejecución de la aplicación.

Las copias de seguridad únicamente son accesibles desde las herramientas de copia, que se encuentran instaladas y operadas por el adjudicatario del mantenimiento. No es posible acceder a las copias de seguridad desde las redes del Ayuntamiento, lo que impide que, en caso de incidente de seguridad, las copias de seguridad se vean afectadas. Además, las copias de seguridad de bases de datos se encuentran cifradas y únicamente pueden ser recuperadas por los sistemas desde los que se realizó la copia original, lo que evita la exfiltración de datos en caso de incidente.

La valoración global del control existente sobre las copias de seguridad es que el Ayuntamiento alcanza un **índice de madurez del 73,3%**, que se corresponde con un **nivel de madurez *N2, repetible pero intuitivo;*** es decir, los controles se realizan, pero existen controles parcialmente establecidos.

9. Plan de continuidad

Objetivo de control

Disponer de un plan con medidas que permitan el restablecimiento de los servicios en caso de perturbación grave de los sistemas.

Por qué es importante este control

Para proteger y mantener en funcionamiento los servicios que se prestan por la entidad es necesario identificar aquellos que son más importantes, los sistemas que los soportan y planificar adecuadamente su recuperación en caso de incidente grave que afecte a su funcionamiento.

En esta planificación se debe incluir la priorización de los servicios a recuperar, los objetivos de tiempo de recuperación y punto de recuperación, así como los medios materiales y personales a utilizar en caso de ser necesaria esta recuperación de sistemas. También es necesario planificar la realización de pruebas periódicas de estos planes.

Situación del control

El Ayuntamiento no dispone de un plan de continuidad de la actividad que sea de aplicación para toda la entidad, ni de un plan específico para el sistema SEDA.

Aunque este requisito únicamente es de aplicación para sistemas categorizados como de nivel alto en el ENS, y no hemos valorado su índice de madurez, lo hemos revisado por considerar que la existencia de un plan de continuidad es una práctica recomendable para organismos con alto impacto en la ciudadanía.

Sí se dispone de un documento de análisis de impacto en el negocio, elemento clave en la elaboración de un plan de continuidad de la actividad. Este documento identifica los servicios críticos de la entidad y su relación con los sistemas y activos físicos que soportan estos servicios. Y detalla, para cada uno de los sistemas que soportan los servicios esenciales, los requisitos en cuanto a disponibilidad de los sistemas, incluyendo los tiempos RTO (objetivo de tiempo de recuperación) y RPO (objetivo de punto de recuperación) para cada uno de ellos.

Además, tal y como se ha indicado anteriormente, se dispone de un plan de contingencia para el sistema SEDA, que es una parte fundamental para la elaboración del plan de continuidad de la actividad. Este plan de contingencia detalla la solución de alta disponibilidad desplegada para bases de datos HANA, la solución de alta disponibilidad en la capa de virtualización para los servidores de aplicación y la configuración de copias de seguridad para el sistema SEDA.

ACRÓNIMOS Y GLOSARIO DE TÉRMINOS

CBCS: Controles básicos de ciberseguridad

CCN: Centro Criptológico Nacional

CGTI: Controles generales de tecnologías de la información

ENS: Esquema Nacional de Seguridad

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).

EDR[7]: Un sistema EDR, sigla en inglés de *endpoint detection and response*, es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.

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*.

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:

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

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.

Plan de contingencia: Definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

Plan de continuidad: Plan cuyo objetivo es mantener la funcionalidad de una organización a un nivel mínimo aceptable durante una contingencia. Define los pasos que se requieren para el restablecimiento de los procesos de negocio después de una interrupción.

Política de seguridad de la información: Es un documento de alto nivel que define lo que significa *seguridad de la información* en una organización de acuerdo con el artículo 11 del Real Decreto 3/2010 y articula la gestión continuada de la seguridad. Debe ser aprobada por el presidente o presidenta o la junta de gobierno de una entidad local o el consejo de administración de una sociedad. 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.

RPO: El objetivo de punto de recuperación (Recovery Point Objective, RPO) es la cantidad máxima de información que puede ser perdida cuando el Servicio es restaurado tras una interrupción. El RPO se expresa como una longitud de tiempo antes del fallo.

RTO: El objetivo de tiempo de recuperación (Recovery Time Objective, RTO) es la máxima cantidad de tiempo tolerable que un ordenador, sistema, red o aplicación puede estar inactivo después de un fallo o un desastre. El RTO se mide en segundos, minutos, horas o días, y es una consideración importante en la planificación de recuperación en caso de desastre.

TRÁMITE DE ALEGACIONES

Previamente al trámite de alegaciones y conforme a lo previsto en la sección 1220 del *Manual de fiscalización* de esta Sindicatura, un borrador previo del Informe de auditoría se discutió con la Interventora de Contabilidad y Presupuestos, con la jefa del Servicio de Contabilidad, y con el jefe del Servicio de Tecnologías de la Información y Comunicaciones, 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 a 2023, este se remitió al cuentadante para que, en el plazo concedido, formulara alegaciones.

Transcurrido dicho plazo no se han recibido alegaciones.

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 22 de noviembre de 2023, aprobó este informe de auditoría.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Documento bajo custodia en Sede Electrónica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Auditoria ciberseguridad SEDA_cas - SEFYCU 4633112

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 HZX3 LP4Y Q2R3 YUNT

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 - 29/11/2023 8:53 VICENT CUCARELLA TORMO