Auditoría de sistemas de información. Práctica y desarrollo en la Cámara de Comptos de Navarra

José Javier García Logroño
Auditor de la Cámara de Comptos de Navarra

José Antonio Garbayo Sánchez
Técnico superior de sistemas de información de la Cámara de Comptos de Navarra

Carlos Ruiz Remírez
Técnico de auditoría de la Cámara de Comptos de Navarra

Nuria Sarasa Amatriain
Técnica de auditoría de la Cámara de Comptos de Navarra

Revista Auditoría Pública nº 84
Noviembre 2024. Páginas: 105-112

Resumen: La transformación tecnológica del sector público supone nuevos riesgos vinculados a la gestión mediante sistemas de información (SI). Resulta esencial la adaptación de las OCEX a este contexto con la realización de auditorías de seguridad de la información.
Desde 2018, la Cámara de Comptos de Navarra ha publicado siete informes de fiscalización con objetivos específicos de auditoría de SI. En este artículo se comparten algunas de los principales aprendizajes que hemos alcanzado hasta este momento.
Se considera idóneo formar equipos de fiscalización plenamente integrados incluyendo personal de perfil técnico formado en ciberseguridad y SI y se enfatiza la necesaria disposición al aprendizaje y la colaboración. Se destaca la importancia del conocimiento de la entidad y de su entorno, así como de cuidar la comunicación con la entidad auditada para establecer un clima de colaboración. Los informes de auditoría tendrán una estructura similar a los de auditoría financiera o de cumplimiento. La conclusión se expresará también de manera análoga a las opiniones de dichos informes, aunque con cierta flexibilidad para expresar las deficiencias o algún otro aspecto muy significativo.

Palabras Clave: sistemas de información, equipo de auditoría, informe de auditoría, controles generales, controles de procesamiento de información.

Abstract: The technological transformation of the public sector poses new risks linked to management through information systems (IS). It is essential that the OCEX adapt to this context by carrying out information security audits.
Since 2018, the Navarra Chamber of Accounts has published seven audit reports with specific IS audit objectives. This article shares some of the main lessons we have learned so far.
It is considered ideal to form fully integrated audit teams including technical personnel trained in cybersecurity and IS and the necessary willingness to learn and collaborate is emphasized. The importance of knowledge of the entity and its environment is highlighted, as well as taking care of communication with the audited entity to establish a climate of collaboration. The audit reports will have a similar structure to those of financial or compliance audits. The conclusion will also be expressed in a similar way to the opinions of said reports, although with some flexibility to express deficiencies or some other very significant aspect.

Keywords: information systems, audit team, audit report, general controls, information processing controls.

Las entidades públicas vienen adoptando progresivamente innovaciones en materia de sistemas de información (SI), que están conduciendo a una transformación del modo de gestión y prestación de los servicios públicos, acelerada en los últimos años, que exige que las entidades públicas tengan que funcionar como plataformas digitales que proporcionan servicios e infraestructura para SI basados en tecnologías de la información y la comunicación (TIC).

Esta transformación puede permitir evidentes beneficios para el funcionamiento del sector público desde el punto de vista de la eficacia y la eficiencia, pero, da lugar a nuevos riesgos, como pone de manifiesto el creciente número de incidentes de ciberseguridad.

En consecuencia, es necesario que las entidades públicas adopten controles para garantizar la protección de la información dentro de la entidad con independencia de su formato (seguridad de la información) y la protección de los activos de información procesada almacenada y transportada a través de redes y SI interconectados (ciberseguridad). Todo ello con el objetivo de garantizar las cinco dimensiones de la seguridad de la información: confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad.

En este entorno, es imprescindible que los OCEX desarrollen las capacidades adecuadas para tener en cuenta las cuestiones relativas la seguridad de la información en el contexto de las auditorías financieras, de cumplimiento u operativas, pero también para la realización de auditorías específicas de seguridad de la información.

Las Guías Prácticas de Fiscalización de los OCEX (GPF-OCEX) sobre auditoría de TI constituyen una orientación muy valiosa y práctica. No obstante, la propia naturaleza de muchos SI y de este tipo de auditoría hace que la realización de este tipo de trabajos resulte compleja.

La Cámara de Comptos de Navarra viene realizando auditorías de SI desde 2018. Desde entonces, ha emitido los siguientes informes con objetivos específicos de auditoría de SI:

- Gestión de la prestación farmacéutica en el Servicio Navarro de Salud–Osasunbidea' (2019).
- 'Gestión de la nómina del personal funcionario del Departamento de Educación' (2019).
- 'Retribuciones variables del Servicio Navarro de Salud–Osasunbidea (2018-2019)',
- 'Gestión del Impuesto sobre la Renta de las Personas Físicas (2015-2019)'
- 'Servicios de pago telemático de la Administración de la Comunidad Foral de Navarra' (2021).
- '¿Es adecuada la gestión de las listas de espera en el Servicio Navarro de Salud-Osasunbidea (2018-2022)?'.
- 'Sistema de contratación temporal de personal docente en el Departamento de Educación (2020-2022)'.

La elaboración de estos informes ha supuesto un proceso interno de aprendizaje y adaptación que sigue en desarrollo, del cual hemos extraído una serie de conclusiones y experiencias que nos parece interesante compartir.

Auditoría de SI vs. análisis de datos en auditoría

Ante todo, es importante subrayar la diferencia entre una auditoría de SI y la realización de análisis de datos en el marco de una auditoría. Aunque ambas requieran de conocimientos en sistemas y bases de datos, el objetivo último de cada uno es esencialmente diferente.

El análisis de datos presenta indudables ventajas para realizar las pruebas de auditoría en el contexto de una auditoría financiera, de cumplimiento, operativa e incluso de una auditoría de SI.

Sin embargo, la auditoría de SI tiene como objetivo evaluar los controles de un sistema de información basado en TIC a fin de evaluar la fiabilidad de los datos utilizados en un sistema de gestión objeto de una auditoría financiera, de cumplimiento u operativa, así como formular recomendaciones con una finalidad preventiva: reducir la probabilidad de que el ejercicio de la función de la entidad pública pueda verse afectado por impactos adversos de origen interno o externo a la organización, así como el efecto negativo que estos podría tener sobre la misma.

La importancia del equipo de auditoría

La configuración del equipo de auditoría resulta determinante para el desarrollo del trabajo. Desde nuestra experiencia, consideramos idóneo formar equipos plenamente integrados. Además del auditor, el equipo incorpora, como mínimo, un miembro de perfil técnico formado en ciberseguridad y SI y un técnico o técnica de auditoría, que no es necesario que disponga de formación específica en materia informática.
Inicialmente la Cámara de Comptos contó con la cola-

boración de una firma externa de auditoría privada, pero en la actualidad estos trabajos se realizan con medios propios, lo que facilita la integración de los equipos y el aprendizaje de la institución. Con esta finalidad, se han reorientado las funciones del personal técnico informático para incluir la participación directa en los trabajos de fiscalización y también se ha incorporado nuevo personal con este perfil.

Los integrantes del equipo realizan tareas acordes con su rol, pero habitualmente necesitarán del conocimiento propio de otros roles. La integración plena del equipo genera importantes sinergias y un intenso intercambio de conocimiento. En este sentido, resulta clave una actitud de disposición al aprendizaje y a la colaboración.

Desarrollo del trabajo de auditoría

La experiencia adquirida nos ha permitido establecer un procedimiento común para este tipo de trabajos, que sirva como guía adaptable a las particularidades de los sistemas y entidades auditados. Se estructura en las siguientes fases:

▪ Objetivos y alcance de la auditoría

En términos genéricos, el objetivo de la auditoría de SI será evaluar el sistema de información que da soporte a uno o varios procesos de gestión, con la finalidad de determinar si la eficacia de los controles existentes en el mismo reduce el riesgo de errores e irregularidades de manera que aportan un nivel de confianza razonable acerca de la correcta ejecución de dicho proceso de gestión. Una auditoría de SI puede realizarse de manera aislada o combinada con objetivos de auditoría financiera o de cumplimiento.

El hecho de que un SI esté basado en TIC no significa que todos sus elementos y procedimientos sean de carácter informático. Puede incluir aplicaciones informáticas y procedimientos automatizados, semiautomatizados y manuales. El análisis del SI no debe limitarse a los elementos estrictamente informáticos, sino que debe considerar el sistema en su conjunto, como un todo formado por diversos elementos y las relaciones existentes entre ellos, y en su contexto.

Por otra parte, con frecuencia los SI están mutuamente interconectados. Esto puede implicar que, aunque se parta de una primera definición del alcance, esta tenga que terminar de precisarse a partir del conocimiento de la entidad, de los procesos de gestión y de los SI.

▪ Conocimiento de la entidad

Exige comprender la naturaleza, función, objetivos y organización de la entidad auditada e identificar los procesos de negocio a los que da soporte el sistema de información objeto de la auditoría. También será necesario determinar y comprender la normativa aplicable, e identificar a las personas involucradas y la infraestructura informática.

Este conocimiento se obtendrá a través de las técnicas habituales incluyendo el análisis de la normativa y de la organización, entrevistas con el personal clave, obtención de manuales de procedimiento y documentación sobre los SI y aplicaciones, utilización de cuestionarios… Resulta de gran ayuda la elaboración de narrativas y flujogramas.

Debemos llegar a responder, entre otras, estas preguntas:

- ¿Cuál es la naturaleza de la entidad o entidades que intervienen en el SI? Puede suceder que en un SI intervengan distintas entidades. Por ejemplo, en el sistema de gestión de la prestación farmacéutica del Servicio Navarro de Salud - Osasunbidea, además del propio organismo autónomo, intervienen la Hacienda Tributaria de Navarra, la Tesorería General de la Seguridad Social aportando determinados datos y las farmacias, que dispensan los medicamentos.

- ¿Qué unidades organizativas están involucradas en el proceso y cuál es el personal clave en el mismo? Puede haber procesos sencillos en los que interviene una única unidad y otros que implican a distintas unidades de una o varias organizaciones, lo que incrementará la complejidad del trabajo. La no existencia de una dirección común puede suponer un factor de riesgo al no existir nadie que asuma la responsabilidad global y tenga una visión completa del sistema.

- ¿Qué aplicaciones se utilizan? Puede tratarse de aplicaciones propias, desarrolladas para atender las necesidades específicas del proceso de gestión correspondiente, o bien de aplicaciones de uso general en la organización, que se utilizan por distintas unidades y dan soporte a distintos procesos de gestión. También cabe distinguir el uso de aplicaciones de desarrollo propio de las adquiridas a terceros.

Dentro de esta fase tienen lugar los primeros contactos con la entidad auditada. Desde el primer momento conviene establecer interlocución tanto

con las áreas responsables de los procesos de gestión como con las áreas técnicas informáticas, lo que proporcionará un conocimiento más completo y vendrá facilitado por la composición mixta del propio equipo de auditoría.

Con frecuencia, el SI no está desarrollado y mantenido por personal interno, sino por proveedores externos. Esto puede propiciar incoherencias, riesgos potenciales y dificultades para implementar actualizaciones y mejoras. Además, puede suponer una dificultad para el desarrollo del trabajo de auditoría ya que el conocimiento del SI no se encuentra en la organización y la interlocución puede resultar menos fluida.

En esta fase conviene solicitar acceso a las principales aplicaciones y bases de datos del SI. El acceso a las aplicaciones permitirá formarse una idea sobre las funcionalidades de cada una y de los distintos roles de usuario. El acceso a las bases de datos, junto a la descripción del modelo de datos, permite conocer directamente su estructura y contenido y hacer una evaluación preliminar de la calidad de los datos, que es indicativa de la calidad del SI. Todo ello deberá tenerse en cuenta en el diseño de las pruebas de auditoría, también a efectos de valorar su viabilidad.

▪ Evaluación de los controles generales

Se revisará el cumplimento del Esquema Nacional de Seguridad (ENS). Si la entidad dispone de una auditoría sobre el cumplimiento del ENS, esta ofrecerá información muy valiosa para nuestra evaluación de los controles generales de tecnologías de la información (CGTI).

En todo caso, se analizará una selección de controles generales considerados más relevantes en función de las particularidades del sistema de gestión objeto de la auditoría.
Los principales tipos de controles que analizamos de manera habitual son:

- Los relativos a control de acceso a la información (alta, baja, revisión de usuarios y sus roles y permisos).
- Revisión de los privilegios administrativos, tanto a nivel de aplicación como de bases de datos.
- Gestión de cambios en las aplicaciones.
- Gestión de trazas.
- Revisión de los interfaces.
- Gestión de las tareas de operación.

Con cierta frecuencia, los SI auditados comparten infraestructura o algunas aplicaciones con otros SI que han sido auditados con anterioridad. En la medida en que los resultados de dichas auditorías sigan siendo relevantes, podremos tenerlos en cuenta en nuestro trabajo a efectos de establecer el diseño, extensión y momento de realización de las pruebas.

▪ Identificación de riesgos y controles

Se trata de identificar tanto las posibilidades de que el funcionamiento o los resultados del SI se vean alterados de manera indebida como consecuencia de

fraude o error, como los controles existentes en el sistema para mitigar el riesgo de que esto suceda.

Esta identificación se basa en el conocimiento adquirido sobre la entidad, los procesos de gestión y el SI, por lo que puede presentar grandes diferencias entre los distintos trabajos.

Puesto que partimos de un enfoque de auditoría basado en riesgos, esta fase resulta fundamental en la auditoría. Constituye el núcleo de la planificación de la auditoría, por lo que merece la pena invertir tiempo y esfuerzo en la misma. Consideramos fundamentales las reuniones de trabajo del equipo de auditoría en las que se discuten los riesgos y controles con la finalidad de identificarlos, analizarlos y evaluarlos.

En procesos de gestión o SI complejos, analizar el proceso en su conjunto es complicado. Resulta útil distinguir distintos subprocesos o subsistemas y hacer un análisis detallado de cada uno de ellos. En este caso, deberá cuidarse luego de tener una visión integrada que tenga en cuenta las interrelaciones entre los distintos subprocesos y/o subsistemas.

El resultado de este análisis se presentará en una matriz de riesgos y controles (RyC), en la que se relacionan los riesgos identificados con los controles establecidos para mitigarlos y las pruebas de controles que se van a realizar sobre los mismos.

La identificación de riesgos y controles, con frecuencia conducirá fácilmente al diseño de las pruebas de auditoría a realizar.

▪ Pruebas de controles de procesamiento de información (CPI)

Una vez identificados los riesgos significativos y los controles asociados en la matriz de RyC, en esta fase se trata de evaluar los CPI en cuanto a su diseño, implantación y funcionamiento. Dada la multitud de controles que pueden existir en un SI, la eficiencia en el trabajo de auditoría exige centrar las pruebas en los que se consideren relevantes, que son aquellos que, individualmente o en combinación con otros, permiten reducir el riesgo a un nivel aceptablemente bajo.

En todo caso, la evaluación de los CPI tiene sentido únicamente sobre la base de que exista una confianza razonable en los CGTI. Por tanto, en principio no deberían abordarse las pruebas de CPI sin antes haber evaluado los CGTI.

Entre las pruebas habituales, cabe mencionar las pruebas de recorrido o "paso a paso", que consisten en realizar el seguimiento de una transacción concreta a lo largo de todo el proceso de gestión. Cuando es posible evitar que ello llegue a tener un impacto negativo efectivo, se puede introducir una transacción errónea y comprobar si la incorrección es prevenida, detectada o corregida por los controles. En la misma línea, pueden realizarse comprobaciones directas sobre si las aplicaciones permiten realizar ciertas operaciones, ya sea utilizando los perfiles de usuario asignados al equipo de auditoría o bien con la colaboración del personal del ente auditado. Estas pruebas, no obstante, tienen el inconveniente de que se realizan siempre durante el trabajo de campo, por lo que su relevancia en relación con el periodo auditado está condicionada por la posibilidad de que se hayan efectuado cambios en el SI con posterioridad a la finalización del mismo.

Cuando los controles están estandarizados y documentados, la consulta de los manuales de procedimiento y de la documentación de los controles aplicados puede proporcionar evidencia de auditoría al respecto.

Como resultado de las pruebas, calificamos cada uno de los controles relevantes como 'efectivo', 'bastante efectivo', 'poco efectivo', 'no efectivo o no implantado' (conforme a la GPF-OCEX 5340) o como 'no verificable'. Esta última categoría, no prevista en las GPF-OCEX, la utilizamos para aquellos controles sobre cuya implantación y eficacia operativa no ha sido posible obtener evidencia adecuada y suficiente. Por ejemplo, cuando se trata de comprobaciones manuales realizadas por el personal sin dejar constancia alguna de las mismas.

▪ Revisión de coherencia e integridad de los datos

Revisar mediante consultas que los datos son coherentes y que se respeta la integridad de los datos, es decir, que no existen datos que no figuran en las tablas maestras.

▪ Pruebas sustantivas

La ausencia de CGTI y/o CPI o la poca robustez de los mismos constituye una deficiencia del SI que deberá ponerse de manifiesto en el informe de auditoría. No obstante, en estos casos procede practicar pruebas sustantivas para verificar si los riesgos identificados han llegado a materializarse. Puede suceder que un SI con deficiencias haya producido resultados válidos, ya sea debido a que no han llegado a materializarse las circunstancias que hubieran dado lugar a un impacto negativo o bien, por ejemplo, debido al

comportamiento ético y diligente del personal.

Cuando la auditoría de SI se realice combinada con otro tipo de auditoría, las pruebas sustantivas pueden ser imprescindibles para responder a los objetivos de la auditoría financiera, de cumplimiento u operativa. Pero, incluso cuando la auditoría solo tiene un objetivo de evaluar el SI, las conclusiones sobre si los riesgos identificados han llegado a materializarse pueden ser muy relevantes para los destinatarios y usuarios del informe.

Habitualmente las pruebas sustantivas se basan en el análisis de datos con ayuda de TI, lo que permite realizar pruebas de gran fiabilidad sobre grandes volúmenes de datos. Sin embargo, encontramos casos en los que el modelo de datos no permite una trazabilidad suficiente para realizar este tipo de pruebas, lo que puede hacer necesario realizar pruebas mediante muestreo.

En todo caso, el hecho de que, durante el periodo auditado, los riesgos no hayan llegado a materializarse no conducirá a una conclusión favorable sobre un SI cuyos controles no sean suficientes para reducir el nivel de riesgo a un nivel aceptablemente bajo. Las deficiencias deberán ponerse de manifiesto en el informe y procederá formular las recomendaciones correspondientes.

▪ Pruebas de interfaces

Es habitual que en un SI haya implicadas diferentes aplicaciones, en ocasiones utilizadas por distintas unidades organizativas.

Las interfaces pueden ser de distinta naturaleza. Existen interfaces manuales, en las que la transferencia de los datos se realiza mediante su registro manual (p.ej. tecleándolos en una aplicación) o enviando ficheros por correo electrónico. También existen interfaces automáticas o semiautomáticas, en las que la transferencia de datos se ejecuta de manera automática de manera programada o bien a petición del usuario, pero sin intervención manual de este.

En las pruebas de interfaces debe tenerse en cuenta la integridad de los datos que transfieren entre aplicaciones, pues existe el riesgo de que los datos sufran alteraciones al pasar de una aplicación a otra. También deben tenerse en cuenta la forma en que se ordena y verifica la ejecución del proceso, ya que existe el riesgo de que la transferencia de datos no se produzca, dando lugar, por ejemplo, a una falta de actualización de los datos. En general, estos riesgos serán mayores cuanto mayor sea la intervención manual en la interfaz. El riesgo también puede agravarse cuando las distintas aplicaciones son utilizadas por distintas unidades u organizaciones y no existe un responsable global del proceso o del SI.

A lo largo de todo el proceso de la auditoría es fundamental cuidar la comunicación fluida con la entidad auditada. En este tipo de trabajos es probable que contactemos con unidades y personal que no tienen interlocución habitual con el OCEX. Es muy conveniente realizar una cierta labor didáctica, explicando nuestros objetivos y la naturaleza de nuestro trabajo para superar posibles suspicacias y establecer un clima de entendimiento, confianza y colaboración constructiva que resultan esenciales en este tipo de trabajos. A ello contribuirá el trato directo, explicar la motivación de las pruebas, ir contrastando las observaciones… Todo ello también facilita la adecuación de las conclusiones y recomendaciones, así como la implantación de éstas desde el convencimiento del ente auditado. De hecho, algunos de nuestros trabajos han dado lugar a la implantación de algunas recomendaciones ya antes de la publicación de los informes.

El informe de auditoría

El resultado del trabajo de auditoría se reflejará en un informe. En estos trabajos, la evaluación del SI no se concibe solo como un medio para la valoración de los riesgos de incorrección material relativos a una auditoría financiera, de cumplimiento u operativa, sino como un objetivo de auditoría en sí mismo. Por tanto, el informe de auditoría expresará las conclusiones de la auditoría de SI.

Las GPF-OCEX no establecen una estructura estándar de este tipo de informes. Los informes emitidos por la Cámara de Comptos en este ámbito, en líneas generales, siguen la siguiente estructura:

- Introducción
- Descripción de la actividad, de los procesos de gestión y del SI (en algunos casos).
- Objetivos, alcance y, en su caso, limitaciones de la fiscalización.
- Opinión y fundamento de la opinión.
- Conclusiones y recomendaciones.
- Responsabilidades de la entidad auditada.
- Responsabilidades de la Cámara de Comptos.
- Apéndices.

En la sección de 'Descripción de la actividad, de los procesos de gestión y del SI' se proporciona información general de la actividad de que se trata y se describe su organización, los procesos de gestión, el SI y la principal normativa aplicable. Frecuentemente va acompañada de esquemas o flujogramas que faciliten su compresión. Debe hacerse un esfuerzo de claridad y concisión y valorar la posibilidad de trasladar información a los anexos siempre que ello no dificulte la comprensión del informe. Generalmente, en aras de la brevedad y concisión, estos contenidos se incluyen como apéndice. Únicamente se presentan como una sección específica antepuesta a la de objetivos y alcance cuando se considera que ello resulta imprescindible para que las personas destinatarias y usuarias del informe puedan comprender los objetivos, alcance, conclusiones y recomendaciones del informe.

La sección de 'Opinión' incluye una conclusión de síntesis sobre el control interno y, según el caso, la opinión de auditoría financiera y/o de cumplimiento. Por su parte, la sección 'Conclusiones y recomendaciones' desarrolla las principales conclusiones del informe, tanto relativas a SI y a otros aspectos de la fiscalización, y presenta las principales recomendaciones destacando algunas de ellas como prioritarias.

La conclusión de síntesis sobre el control interno incluye una tabla resumen de los controles analizados en la auditoría, distinguiendo los controles generales y los controles de procesamiento de información. Con base en lo previsto en la GPF-OCEX 5340–'Revisión de los CPI en un entorno de administración electrónica', cada uno de los controles se califica como 'efectivo', 'bastante efectivo', 'no efectivo' o 'no verificable'. Dentro de la categoría 'No efectivo' se incluyen los controles que, de acuerdo con la mencionada GPF-OCEX, se calificarían como 'Poco efectivos' y 'No efectivos o no implantados'. En todo caso, este cuadro tiene un carácter meramente ilustrativo. La conclusión de síntesis no se expresa en términos cuantitativos y se alcanza mediante la aplicación del juicio del auditor, teniendo en cuenta los niveles de madurez de los procesos según la Guía de seguridad CCN-STIC 804 (GPF-OCEX 5330), la importancia relativa de los distintos controles, procesos y subprocesos, así como las relaciones existentes entre ellos.

El párrafo que expresa la conclusión de la auditoría de SI tiene una redacción análoga a la utilizada en los informes de fiscalización financiera y de cumplimiento, aunque con cierta flexibilidad para expresar las deficiencias o algún otro aspecto muy significativo de la auditoría. Así, por ejemplo, en el informe 'Gestión de la prestación farmacéutica en el Servicio Navarro de Salud-Osasunbidea', se concluye:
'De los resultados derivados del cuadro anterior destacamos que el control sobre el proceso de gestión de altas, modificaciones y bajas de usuarios de las aplicaciones ATENEA, HCI y LAMIA es inefectivo, habiendo constatado, entre otros aspectos indicados en el epígrafe V de este informe, que el procedimiento existente no está actualizado, si bien existen actualmente dos proyectos para llevar a cabo esta actualización.
En nuestra opinión, a excepción de lo señalado en el párrafo anterior, cabe concluir que el nivel de control interno existente en los procedimientos de gestión de la prestación farmacéutica y en los sistemas de información que los soportan, aporta un nivel de confianza razonable para garantizar su correcta ejecución, la adecuada contabili-

zación de las transacciones realizadas y la validez, integridad, exactitud, confidencialidad y disponibilidad de la información relacionada'.

Por su parte, el informe 'Sistema de contratación temporal de personal docente en el Departamento de Educación (2020-2022)' concluye:
'En definitiva, a partir del trabajo realizado concluimos que el sistema de contratación temporal de personal docente en el Departamento de Educación, considerado en su conjunto, aporta un nivel de seguridad razonable acerca de la correcta ejecución de dicha actividad de contratación. Esta seguridad se sustenta, en buena medida, en la adjudicación automática de la mayor parte de las plazas a través de la aplicación ATP y en la transparencia del sistema derivada de la publicidad de las ofertas, listas y adjudicaciones.
No obstante, señalamos que los procesos anteriores y posteriores a la adjudicación adolecen de cierta falta de integración. El sistema presenta deficiencias en la segregación de funciones e incluye numerosas intervenciones manuales muy dependientes del conocimiento, experiencia y compromiso profesional del personal. Una parte significativa del control descansa en procedimientos manuales no estandarizados ni documentados y en el seguimiento de la actividad de contratación por parte de los centros docentes'.

Al elaborar el informe, se tienen en cuenta las advertencias de la GPF-OCEX 5300 sobre el posible impacto negativo en caso de que el informe revele información sensible o confidencial que dé a conocer vulnerabilidades del sistema. En caso de considerarse necesario, se ofrece a los responsables de la entidad auditada un mayor detalle sobre las conclusiones y recomendaciones de manera verbal o, cuando se considera conveniente, mediante una comunicación complementaria al informe.

En definitiva, hemos destacado que en el Sector Público estamos asistiendo a una evolución tecnológica que supone la aparición de nuevos riesgos vinculados a los SI en la gestión de la actividad. Para los OCEX esto supone un cambio de paradigma al que debemos adaptarnos de forma proactiva. En este sentido, resulta indispensable la colaboración y la puesta en común del conocimiento entre distintos perfiles profesionales, siendo conscientes de que ello no solo constituye un aspecto imprescindible para la realización del trabajo concreto, sino también un proceso de aprendizaje que redunda en beneficio de todos los miembros del equipo y de los propios OCEX con la finalidad de seguir aportando valor a la sociedad.