Auditoría Pública nº 73 (2019), pp. 53 - 58

Antonio Minguillón Roy
Director del Gabinete Técnico de la Sindicatura de Cuentas de la Comunidad Valenciana
y Coordinador de la Comisión Técnica de los OCEX

Las nuevas guías prácticas de fiscalización de los OCEX, unas guías de auditoría de la administración electrónica para el siglo XXI

RESUMEN/ABSTRACT:

A finales de 2018 la Conferencia de Presidentes de ASOCEX aprobó cuatro Guías Prácticas de Fiscalización (GPF-OCEX) elaboradas por la Comisión Técnica de los OCEX (CT-OCEX) relacionadas con la auditoría de los controles internos automatizados, la ciberseguridad, la auditoría de procesos de gestión informatizados y la utilización de herramientas para el análisis de grandes bases de datos. En el artículo se destaca la importancia de estas guías para desarrollar la fiscalización del sector público en un entorno de administración electrónica, totalmente informatizado, que es en el que actualmente se desenvuelven los OCEX. Dichas guías están fundamentadas en una larga experiencia adquirida por diversos OCEX en los últimos años y al mismo tiempo recogen la más actual metodología nacional e internacional en estas materias. Son innovadoras no solo en el ámbito público, sino en el ámbito auditor en general de nuestro país, pues no existen guías de auditoría publicadas dirigidas al auditor externo que contemplen esta materia y faciliten su trabajo en un entorno de administración electrónica. Por tanto, estas GPF-OCEX, con sus programas detallados de trabajo y orientaciones muy prácticas para aplicarlas en las auditorías serán de gran ayuda para los auditores públicos en el nuevo mundo de la administración electrónica.

At the end of 2018, the Conference of Presidents of ASOCEX approved four Practical Guidelines for Examination (GPF-OCEX). These were prepared by the Technical Commission of the OCEX (CT-OCEX) and are related to the audit of automated internal controls, cybersecurity, the audit of computerized management processes and the use of tools for the analysis of large databases. The article highlights the importance of these guidelines in the development of public sector auditing in a fully computerized, electronic administration environment. This is how the OCEXs are currently operating.

These guidelines are based on ample experience acquired by various OCEX in recent years and at the same time reflect the most current national and international methodology in these matters. They are innovative; not only in the public sphere, but in the general auditing field in our country because there are no published audit guides for external auditors that contemplate this matter and facilitate their work in an electronic administration environment. Therefore, these GPF-OCEX guidelines with their detailed work programs and very practical audit guidance allow them to be applied in audits and will be of great help to public auditors in the new world of e-government.

PALABRAS CLAVE/KEYWORDS:

GUÍAS DE AUDITORÍA, CIBERSEGURIDAD, CONTROL INTERNO, ADMINISTRACIÓN ELECTRÓNICA, TECNOLOGÍAS DE LA INFORMACIÓN
AUDIT GUIDES, CYBERSECURITY, INTERNAL CONTROL, ELECTRONIC ADMINISTRATION, INFORMATION TECHNOLOGIES

El 12 de noviembre del pasado 2018 la Conferencia de Presidentes de ASOCEX aprobó las siguientes Guías Prácticas de Fiscalización (GPF-OCEX) elaboradas por la Comisión Técnica de los OCEX (CT-OCEX):

GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad

GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica

GPF-OCEX 5340 Los controles de aplicación: qué son y cómo revisarlos

GPF-OCEX 5370 Guía para la realización de pruebas de datos

Conviene destacar la importancia de estas guías para desarrollar la fiscalización del sector público en un entorno de administración electrónica, totalmente informatizado, que es en el que actualmente nos desenvolvemos los OCEX.

Estas guías son importantes por varios motivos. No son documentos teóricos ya que están fundamentadas en una larga experiencia adquirida por diversos OCEX en los últimos años, al mismo tiempo que recogen la más actual metodología nacional e internacional en estas materias. Son totalmente innovadoras no solo en el ámbito público, sino en el ámbito auditor en general de nuestro país, pues no existen guías de auditoría publicadas que contemplen esta materia y faciliten el trabajo de los auditores externos en un entorno de administración electrónica. Por tanto, estas GPF-OCEX, con sus programas detallados de trabajo y orientaciones muy prácticas para aplicarlas en las auditorías, serán de gran ayuda para los auditores públicos en el nuevo mundo de la administración electrónica.

GPF-OCEX 5313 REVISIÓN DE LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD

En la *GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa*, aprobada en 2017, se destacaba la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las administraciones públicas y, en consecuencia, la atención creciente que los auditores públicos deben conceder a dicha materia. En la medida en que cada vez un mayor número de servicios públicos se presta on-line y la conectividad por internet se ha convertido en una característica de todos los sistemas de información (contables, sanitarios, educativos, etc) los auditores deben prestar cada vez más atención a las cuestiones relacionadas con la ciberseguridad.

También se mencionan en la citada guía los distintos enfoques que los OCEX pueden adoptar a la hora de abordar una auditoría o una revisión de la ciberseguridad de los entes públicos. En síntesis, desde la perspectiva de un OCEX, se pueden adoptar tres enfoques principales:

- Realizar una auditoría de ciberseguridad consistente en un análisis a fondo de la situación en un determinado ente.
  Podría ser similar a una auditoría de seguridad de las requeridas por el Esquema Nacional de Seguridad (ENS) o una auditoría siguiendo la metodología de ISACA. Un trabajo de este tipo entraña una intensa dedicación de personal especializado tanto para el auditor como para el ente auditado.
- La revisión de controles directamente relacionados con las áreas significativas en una auditoría financiera. Consistirá en la revisión de los Controles Generales de Tecnologías de la Información (CGTI) relacionados únicamente con las áreas significativas para los fines de la auditoría financiera del ente auditado. Una parte significativa de dichos controles está formada por controles de ciberseguridad. **Este es el objeto de la GPF-OCEX 5330.**
- La revisión de una serie de controles básicos de ciberseguridad.
  Los controles básicos de ciberseguridad son un subconjunto reducido de los controles de ciberseguridad. Su revisión permitirá que el auditor pueda formarse una idea general de la situación en la entidad revisada y no requerirá la dedicación de excesivos recursos especializados ni del auditor externo ni del ente auditado. Será por tanto un trabajo más viable en entes que no dispongan de muchos recursos técnicos o humanos. **Un enfoque de este tipo es el que motiva el desarrollo de la GPF-OCEX 5313.**

En el desarrollo de la GPF-OCEX 5313, cuyo contenido está fundamentalmente relacionado con la **auditoría de la seguridad de la información**, se ha tenido especial cuidado en mantener la **máxima coherencia con los postulados del ENS** puesto que es de obligado cumplimiento para todos los entes públicos. Esta alineación facilita la realización de las auditorías de ciberseguridad y coadyuvan a la implantación del ENS. No obstante, dada su amplitud, se han seleccionado, por las razones señaladas antes, una serie limitada de controles para su revisión, priorizados según su importancia para hacer frente a las ciberamenazas.

Estos controles **están pensados para organizaciones de cualquier tipo**.

Además, en este tipo de revisión se incluirá la verificación del cumplimiento de diversas normas relacionadas con la seguridad de la información aplicables al sector público.

Los ocho controles básicos de ciberseguridad incluidos en la guía son:

Control		Objetivo de control
CBCS 1	Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.
CBCS 2	Inventario y control de software autorizado y no autorizado	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.
CBCS 4	Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Implementar la configuración de seguridad 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.
CBCS 6	Registro de la actividad de los usuarios	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.
CBCS 7	Copias de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.
CBCS 8	Cumplimiento del ENS	- Política de seguridad y responsabilidades - Declaración de aplicabilidad - Informe de Auditoría (nivel medio o alto) - Informe del estado de la seguridad - Publicación de la declaración de conformidad y los distintivos de seguridad en la sede electrónica
	Cumplimiento de la LOPD/RGPD	- Nombramiento del DPD - Registro de actividades de tratamiento - Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento (para los de riesgo alto) - Informe de auditoría de cumplimiento (cuando el responsable del tratamiento haya decidido realizarla)
	Cumplimiento de la Ley 25/2013, de 27 de diciembre (*creación del registro contable de facturas*)	- Informe de auditoría de sistemas anual del Registro Contable de Facturas

La elección de estos ocho controles no ha sido aleatoria. Los seis primeros son los seis controles básicos establecidos por el *Center for Internet Security*[1] en su versión 7[2]de 2018. Según el CIS, con carácter general, las organizaciones que apliquen sólo los cinco primeros controles pueden reducir su riesgo ante ciberataques alrededor del 85%. Si se implementan los 20 controles CIS el riesgo se puede reducir un 94%.

Además de los seis controles CIS básicos se ha incluido en los CBCS el control "Copias de seguridad de datos y sistemas" (control CIS número 10) ya que es un elemento fundamental para mantener un grado razonable de ciberresiliencia[3]. Si todos los controles preventivos fallan y un ciberataque traspasa todas las líneas de defensa y tiene éxito, el último recurso de la entidad atacada es restaurar sus sistemas y datos en un plazo predeterminado para poder continuar prestando sus servicios.

Además de los CBCS vistos en el apartado anterior, en este tipo de revisión se incluirá la verificación del cumplimiento de diversas normas relacionadas con la

[1] Organización de reconocido prestigio internacional.
[2] Con objeto de seleccionar los más relevantes se ha atendido al marco conceptual establecido por Los Controles CIS priorizan y clasifican los controles según su importancia para hacer frente a las ciberamenazas.
[3] Ciber-resiliencia es la capacidad para continuar prestando servicios mientras se previenen y responden los ciberataques. También reduce la probabilidad de que los ciberataques tengan éxito. Para ser ciber-resiliente, una entidad pública debe tener implementado un sólido sistema de CGTI, cuya función es proporcionar un entorno TI fiable sobre el que otros procesos y controles TI pueden apoyarse y funcionar.

seguridad de la información, por la importancia que el cumplimiento de las normas tiene en el sector público.

Dado que los CBCS están alineados con el ENS, cuando su revisión se realice en entidades que hayan pasado la auditoría de seguridad obligatoria establecida en el artículo 34 del RD 3/2010 por el que se aprueba el ENS, la revisión podrá basarse, en la medida de lo posible, en los resultados de dicha auditoría.

GPF-OCEX 5330 REVISIÓN DE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE INFORMACIÓN EN UN ENTORNO DE ADMINISTRACIÓN ELECTRÓNICA

El enfoque de auditoría basado en el análisis del riesgo es el fundamento central de la actividad auditora desarrollada de acuerdo con las Normas Internacionales de Auditoría (NIA-ES) y las ISSAI-ES.

Actualmente, en una auditoría financiera basada en el análisis de los riesgos realizada de acuerdo con la ISSAI-ES 200, el estudio y revisión de los sistemas de información en los que se sustenta la gestión de una entidad (empresa o fundación pública, ayuntamiento, administración de la comunidad autónoma, etc.) se ha convertido en una actividad de importancia creciente, en la medida en que esa gestión se apoya en unos sistemas de información interconectados que, con la plena implantación de la administración electrónica, han ido adquiriendo una complejidad cada vez mayor. Esta situación ha generado una serie de nuevos e importantes riesgos de auditoría (inherentes y de control) que deben ser considerados en la estrategia de auditoría.

De acuerdo con las ISSAI-ES/NIA-ES y la GPF-OCEX 1315, una vez adquirido un conocimiento general de la entidad, incluyendo sus sistemas de información y de control interno, y antes de iniciar la revisión de los procesos y aplicaciones de gestión significativos a los efectos de la auditoría financiera y de sus controles, se debe revisar la situación de los **controles generales**, ya que el grado de confianza en los mismos determinará la posterior estrategia de auditoría.

Tal como se señala en la guía, el objetivo de la auditoria de los CGTI será verificar si el sistema de control interno proporciona una seguridad razonable sobre la confidencialidad, integridad, autenticidad, disponibilidad, y trazabilidad de los datos, la información y los activos de los sistemas de información. Estos son atributos de los que debe gozar la evidencia electrónica de auditoría y que los auditores de los OCEX debemos verificar, de otro modo, la evidencia no sería suficiente y adecuada.

En un entorno informatizado de complejidad media o alta, como sucede con la administración electrónica, la revisión de los controles generales de tecnologías de la información (CGTI) requerirá, normalmente, la colaboración de un experto en auditoría de sistemas de información y la aplicación de una metodología específica.

En estas circunstancias la revisión de los CGTI (y de los controles de aplicación) es un procedimiento indispensable para reducir los riesgos de auditoría a un nivel aceptable.

Además de las normas técnicas de auditoría, las normas reguladoras de la auditoría pública más recientes recogen la necesidad de que los auditores revisen la fiabilidad de los sistemas de información, de los controles internos y de la seguridad de la información. A modo de ejemplo:

a) La Ley 16/2017 que modifica la Ley 6/1985, de 11 de mayo, de Sindicatura de Comptes de la Comunitat Valenciana establece:

"Artículo 11. Uno. En el desarrollo de su función fiscalizadora, la Sindicatura de Comptes está facultada para: …

*d) **Verificar la seguridad y fiabilidad de los sistemas informáticos** que soportan la información* económico-financiera, contable y de gestión."

b) El Real Decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local establece:

"CAPÍTULO III De la auditoría pública

Artículo 33. Ejecución de las actuaciones de auditoría pública.

4. Para la aplicación de los procedimientos de auditoría podrán desarrollarse las siguientes actuaciones: …

*e) **Verificar la seguridad y fiabilidad de los sistemas informáticos** que soportan la información económico-financiera y contable."*

c) La Resolución de 30 de julio de 2015, de la Intervención General de la Administración del Estado, por la que se dictan instrucciones para el ejercicio de la auditoría pública, establece:

"*Duodécima. Procedimientos para el ejercicio de la auditoría pública.*

2. Para la aplicación de los procedimientos de auditoría podrán desarrollarse las siguientes actuaciones:

*e) **Verificar la seguridad y fiabilidad de los sistemas informáticos** que soportan la información económico-financiera y contable."*

Hay 24 controles principales que se agrupan en las siguientes categorías:

A. Marco organizativo

B. Gestión de cambios en aplicaciones y sistemas

C. Operaciones de los sistemas de información

D. Controles de acceso a datos y programas

E. Continuidad del servicio

En el desarrollo de esta GPF-OCEX 5330, cuyo contenido está fundamentalmente relacionado con la auditoría de la seguridad de la información, también se ha tenido especial cuidado en mantener la **máxima coherencia con los postulados del ENS** puesto que es de obligado cumplimiento para todos los entes públicos y esta alineación facilita la realización de las auditorías de CGTI y coadyuvan a la implantación del ENS.

Dado que los CGTI están alineados con el ENS, cuando su revisión se realice en entidades que hayan pasado la auditoría de seguridad obligatoria establecida en el artículo 34 del RD 3/2010 por el que se aprueba el ENS, la revisión podrá basarse, en la medida de lo posible, en los resultados de dicha auditoría.

GPF-OCEX 5340 LOS CONTROLES DE APLICACIÓN: QUÉ SON Y CÓMO REVISARLOS

De acuerdo con las ISSAI-ES/NIA-ES, dentro del proceso auditor, la revisión de los controles internos implementados en las aplicaciones informáticas de gestión y en las interfaces es un aspecto muy relevante, tanto más importante cuanto más complejo sea el sistema de información que soporta el proceso de gestión incluido en el alcance de la auditoría.

Esta guía trata de la revisión de los controles de aplicación y de los controles sobre las interfaces, cuya finalidad es:

- Adquirir un conocimiento profundo de los procesos de gestión revisados, de los riesgos significativos existentes en las aplicaciones informáticas que los soportan y en las interfaces relacionadas.
- Identificar, analizar y comprobar el adecuado funcionamiento de los controles de los procesos y aplicaciones de gestión y de los controles sobre las interfaces.
- Determinar la extensión de los procedimientos sustantivos a ejecutar.
- Reducir el riesgo de auditoría a un nivel aceptable.

Tal como se señala en la guía, el objetivo de la auditoria de los controles de aplicación será obtener una seguridad razonable de que el sistema de control interno garantiza la integridad (completitud), exactitud, validez y legalidad de las transacciones y datos registrados en la aplicación de gestión revisada y su posterior contabilización; es decir, verificar si la eficacia de los controles relevantes garantiza la correcta ejecución de los procesos de gestión auditados y mitigan el riesgo de errores e irregularidades.

En la guía se señala cual es la interrelación de los CGTI con los controles de aplicación, destacando que los CGTI ayudan a asegurar el correcto funcionamiento de los sistemas de información mediante la creación de un entorno adecuado para el correcto funcionamiento de los controles de aplicación. Una evaluación favorable de los CGTI da confianza al auditor sobre los controles de aplicación automatizados integrados en las aplicaciones de gestión. Sin embargo, unos CGTI ineficaces pueden impedir que los controles de aplicación funcionen correctamente y permitir que se den manifestaciones erróneas significativas en las cuentas anuales y que éstas no sean detectadas. Por tanto, la importancia de una

deficiencia de un CGTI debe ser evaluada en lo que se refiere a su efecto en los controles de aplicación, es decir, hay que comprobar si los controles de aplicación dependientes son ineficientes.

Si no existieran controles generales o no fueran efectivos, no se podría confiar en los controles de aplicación y sería necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos.

La GPF-OCEX 5340 es necesariamente genérica, ya que la variedad de aplicaciones informáticas de gestión que puede encontrarse un auditor de los OCEX es muy grande. Por tanto la metodología señalada en la guía deberá adaptarse a cada caso y sería deseable que la CT-OCEX desarrollara guías específicas para auditar las aplicaciones más habituales del sector público, por ejemplo gestión de personal, nóminas, compras, contratación, contabilidad, etc.

GPF-OCEX 5370 GUÍA PARA LA REALIZACIÓN DE PRUEBAS DE DATOS

Las expresiones herramientas y técnicas de auditoría asistida por ordenador (CAATs) y análisis de datos de auditoría (ADA) hacen referencia a metodología de auditoría basada en la utilización de programas informáticos que ayudan a los auditores en el tratamiento y análisis de la información en formato electrónico, con objeto de obtener evidencia que soporte las conclusiones de auditoría y a efectos de la guía tienen el mismo significado.

En la guía también se utiliza el término más genérico de **pruebas de datos**, para referirnos a pruebas sobre datos masivos archivados en bases de datos estructuradas utilizando herramientas ADA/CAAT.

Las CAAT/ADA son técnicas y herramientas de TI que ayudan a un auditor en la realización de diversas pruebas automatizadas para evaluar un sistema de TI o los datos utilizados como evidencia de auditoría. Son muy útiles en aquellos casos en que un volumen importante de datos de la entidad auditada está disponible en formato electrónico. Son útiles para las pruebas de los controles y las pruebas sustantivas en la auditoría financiera, la auditoría de cumplimiento y la auditoría operativa.

El uso de las CAAT/ADA otorga muchas ventajas en comparación con el examen manual. Algunas de estas son:

a. Las pruebas sustantivas y el análisis de grandes volúmenes de datos se pueden hacer en un corto espacio de tiempo y con menos esfuerzo.
b. Las pruebas se pueden repetir fácilmente en diferentes archivos/datos/entidades.
c. Las pruebas flexibles y complejas se pueden hacer con un cambio en los parámetros.
d. Documentación automatizada de pruebas y resultados de auditoría.
e. Implementación más eficiente de los recursos de auditoría.
f. Análisis del 100% de los datos.

El actual entorno de administración electrónica, basado en el uso intensivo de sistemas de información interconectados, hace que en los trabajos de fiscalización exista la **necesidad de analizar información contenida en grandes bases de datos o ficheros con herramientas CAAT/ADA potentes como ACL/IDEA.**

El uso de estas técnicas posibilita una mayor extensión (alcance) de las pruebas sobre transacciones electrónicas y archivos contables digitales, circunstancia que puede ser útil cuando el auditor decida modificar la extensión de las pruebas, en respuesta a los riesgos de incorrecciones materiales en las cuentas anuales.

Algunas de las pruebas de auditoría se realizan tradicionalmente sobre una muestra seleccionada aleatoriamente o mediante muestreo estadístico; actualmente, si se dispone de herramientas ADA, puede hacerse un planteamiento diferente y ejecutar la comprobación sobre el 100% de la población, aumentando el grado de seguridad que el auditor puede alcanzar.

La finalidad de la guía es proporcionar orientaciones generales para realizar pruebas de datos con herramientas ADA, como ACL/IDEA, sobre bases de datos estructuradas. En particular para:

- Establecer criterios homogéneos y metodologías comunes para la realización de las pruebas de datos para todos los auditores del OCEX.
- Asegurar la adecuada planificación y realización de las pruebas, evitando errores en su ejecución.
- Asegurar la generación de evidencia de auditoría suficiente y adecuada en las pruebas de datos.
- Automatizar en la medida de lo posible la ejecución de las pruebas de datos, con el objetivo de incrementar la eficiencia en su ejecución.
- Estandarizar la documentación de las pruebas de datos.
- Generar un fondo documental de conocimiento para la realización de las pruebas de datos de las entidades fiscalizadas en beneficio de fiscalizaciones subsiguientes.

La utilización de herramientas de visualización de datos, aunque son complementarias del ADA, no se incluye en esta guía. Sí que se incluyen diversos ejemplos de cómo planificar, ejecutar y documentar los resultados de pruebas de datos, que sin duda servirán de gran ayuda a los auditores de los OCEX.