**Antonio Minguillón Roy**
Auditor de la Sindicatura de Comptes de la Comunitat Valenciana

# La fiscalización en entornos informatizados

## 1. INTRODUCCIÓN

Ha sido destacado por múltiples autores que los principios básicos de la auditoría no han sufrido cambios radicales a lo largo de las últimas décadas, ni en su vertiente de conjunto de conocimientos o disciplina, ni desde la óptica de la práctica profesional[1].

Sin embargo, se ha producido una verdadera revolución en algunas de las técnicas empleadas en la gestión, especialmente en lo que se refiere a las tecnologías de la información y las comunicaciones (TIC) aplicadas a la gestión de las administraciones públicas.

La utilización de complejas aplicaciones ERP (*Enterprise Resource Planning*) en buena parte de las administraciones españolas está cada vez más extendida. Estas aplicaciones informáticas están diseñadas para cubrir todas las áreas funcionales de una organización de tal manera que se crea un flujo de trabajo entre los distintos usuarios (sin flujo físico de papel), con acceso instantáneo a toda la información; las operaciones que suponen movimientos monetarios se recogen automáticamente (sin intervención humana y sin papel) en el módulo contable. Las personas que deben autorizar las distintas operaciones lo hacen también firmando electrónicamente a través del sistema.

Esta situación plantea una serie de problemas de auditoría a los que los auditores tenemos que hacer frente de forma adecuada. Más adelante se comentan con mayor profundidad los mismos, pero anticipemos los más evidentes:

- Ausencia de transacciones y autorizaciones documentadas en soporte papel, como pedidos, albaranes, facturas, cheques, órdenes de transferencia de fondos, etc.
- Sustitución de procedimientos de control interno manuales (realizados por empleados-funcionarios) por otros que se realizan automáticamente por los sistemas informáticos, (p.e. segregación de funciones, conciliaciones de cuentas, etc.)[2].
- Riesgo de manipulación de la información.

[1] Pablo Lanza lo recordaba desde las páginas de esta revista, ya en 1997, en el artículo "La evidencia informática"; *Auditoría Pública*, nº 11, octubre de 1997. Este artículo sigue manteniendo casi 10 años después toda su vigencia.

[2] Ver el artículo "Implementation of ERP Systems: accounting and auditing implications" de Benjamin Bae y Paul Ashcroft en la revista *Information Systems Control Journal*, volumen 5, 2004. Entre otras cosas se señala que "un problema común que se encuentra durante la implantación de un sistema ERP es la eliminación de controles tradicionales sin su reemplazo por nuevas medidas de control efectivas… Algunos sistemas como SAP permiten introducir controles que crean pistas de auditoría y permiten seguir y verificar todas las entradas de datos… No obstante, todos los maravillosos mecanismos de control disponibles en SAP R/3 son efectivos solo si se instalan correctamente."

Un ejemplo reciente de este proceso de informatización de las administraciones públicas podemos apreciarlo en la nueva "Instrucción del modelo normal de contabilidad local" (aprobada por la Orden EHA/4041/2004, de 23 de noviembre; BOE de 9-12-2004), que representa una decidida apuesta por la incorporación de las técnicas electrónicas, informáticas y telemáticas a la actividad administrativa. Así, de acuerdo con esta Instrucción, una de las consecuencias más destacadas de la utilización de las TIC en la función contable, es la desaparición de la obligación de obtener y conservar los libros de contabilidad tradicionales en papel, estableciéndose que las bases de datos del sistema informático donde residan los registros contables constituirán soporte suficiente para la llevanza de la contabilidad de la entidad. **Desaparece, por tanto, la concepción tradicional de libro de contabilidad, y se sustituye por la de base de datos contable.**

Además, como se señala en la exposición de motivos de la Instrucción, en la línea de "fomentar una nueva cultura administrativa en la que el papel, en la medida de lo posible, vaya siendo sustituido por los documentos automatizados, con los ahorros tanto económicos como de espacio físico que ello implicará, se ha establecido que los justificantes de los hechos que se registren en el SICAL-Normal podrán conservarse por medios o en soportes electrónicos, informáticos o telemáticos, con independencia del tipo de soporte en que originalmente se hubieran plasmado, siempre que quede garantizada su autenticidad, integridad, calidad, protección y conservación. En estos casos las copias obtenidas de dichos soportes informáticos gozarán de la validez y eficacia de la justificación original."

Resumiendo, y muy brevemente, el efecto de todo este proceso es que **va a llegar un momento en el que las pistas de auditoría** (firmas, documentos contables, autorizaciones, libros de contabilidad) **en soporte tradicional en papel**, como a los funcionarios tanto nos gusta, **será cosa de los libros de historia**.

El reto al que nos enfrentamos es que ese momento está cada vez más cercano, en algunos casos lo tenemos ya presente.

En este contexto, **se debe prever qué impacto tienen las circunstancias señaladas en el trabajo y organización de los órganos de control externo y a la luz de las normas técnicas de auditoría determinar qué medidas concretas se deben adoptar**.

## 2. NORMAS TÉCNICAS APLICABLES

Los Principios y Normas de Auditoría del Sector Público (PNASP) de los OCEX, aparte de los principios generales, no contemplan la problemática aquí planteada (en esta materia están obsoletos).

No obstante, tal como se señala en la exposición de motivos de los PNASP "en todo lo no regulado en las presentes normas y en sus desarrollos posteriores, se aplicarán los principios y normas de auditoría generalmente aceptados a nivel nacional e internacional, y especialmente las normas técnicas del Instituto de Contabilidad y Auditoría de Cuentas". De acuerdo con ello, la Norma Técnica de Auditoría del ICAC sobre la auditoría de cuentas en entornos informatizados (NTAEI), aprobada por Resolución del ICAC de 23 de junio de 2003, tiene carácter supletorio, y es plenamente aplicable en las fiscalizaciones que realicen los OCEX. Dicha NTAEI es muy similar a su homónima Norma Internacional de Auditoría 401[3].

## 3. ENFOQUE DE AUDITORÍA "TRADICIONAL" O "AUDITORÍA ALREDEDOR DEL ORDENADOR"

Hasta la entrada en vigor de la NTAEI y su aplicación los auditores financieros han tenido muchas veces la tentación (ante situaciones para ellos desconocidas en mayor o menor grado y que por tanto no controlan) de asignar un riesgo alto a los sistemas de control interno informatizados y así confiar únicamente en las pruebas sustantivas para obtener evidencia suficiente y adecuada[4].

En este enfoque denominado muchas veces "auditoría alrededor del ordenador" se utilizan técnicas para comprobar la fiabilidad de la información que genera el sistema informático revisando los inputs al sistema y verificando que los outputs coinciden con los cálculos o estimaciones que realiza el auditor. Está basado casi exclusivamente en pruebas sustantivas y puede no ser viable cuando se audita una entidad con un entorno informatizado complejo, donde predomina la evidencia informática y la capacidad del auditor para obtener evidencia sólo a partir de pruebas sustantivas está muy limitada.

Este enfoque de "auditoría alrededor del ordenador" no debe ser considerado como totalmente obsoleto, pero debe limitarse estrictamente a aquellas situaciones en las que se verifique simultáneamente el cumplimiento de estas tres condiciones:

1. La pista auditora es completa y visible. Esto implica que se utilizan documentos fuente en todo tipo de transacciones, se imprimen los libros diarios detallados, y se mantienen referencias de las transacciones tanto en el diario como en el mayor.
2. Las operaciones de proceso de la información son relativamente sencillas y directas.
3. El auditor tiene a su disposición la documentación completa del sistema, incluyendo diagramas de flujo, descripción de registros, etc.

Obviamente, en los sistemas informáticos actuales será más bien rara la verificación simultánea de las tres condiciones, ya que la entidad fiscalizada normalmente operará en un entorno informatizado y en esos casos deberemos aplicar el enfoque denominado "auditoría a través del ordenador" basado en la NTAEI cuyos aspectos principales se comentan en los siguientes apartados.

## 4. ENTORNOS INFORMATIZADOS

Una auditoría se lleva a cabo en un ***entorno informatizado*, cuando la entidad, al procesar la información financiera significativa para la auditoría, emplea un ordenador, de cualquier tipo o tamaño, ya sea operado por la propia entidad o por un tercero**. De acuerdo con esta definición, hoy en día, prácticamente cualquier Administración pública opera en un entorno informatizado.

[3] La NIA 401 ha sido derogada recientemente y sustituida por las NIA 315 y 330, en las que se refuerzan los principios básicos de aquélla (evaluación de riesgos y diseño de procedimientos efectivos para contrarrestarlos). Normas que van a ser adoptadas por INTOSAI.

[4] En el artículo de Virginia y Michael Cerillo "Impact of SAS nº 94 on Computer Audit. Techniques", en *Information Systems Control Journal*, volume 1, 2003, se destaca que según una encuesta realizada antes de la entrada en vigor del SAS 94 la mayoría de los auditores en EEUU seguía la práctica mencionada. No obstante, en EEUU a raíz de los escándalos Enron, etc., la normativa se ha endurecido mucho y reforzado las exigencias de evaluación de riesgos, por lo que estas prácticas supongo que se habrán corregido.

Cuando se efectúa una auditoría en una entidad que opera en un *entorno informatizado*, **el auditor debe evaluar la manera en que el entorno informatizado afecta a la auditoría**. Obviamente, afectará de forma diferente según el grado de complejidad de ese entorno.

El objetivo global y el alcance de la auditoría no cambian en un entorno informatizado. Sin embargo, el uso de un ordenador incide en el procesamiento, almacenamiento y comunicación de la información financiera y afecta a los sistemas contables y de control interno empleados por la entidad. En consecuencia, desde el punto de vista del auditor, un entorno informatizado puede afectar de forma importante a:

- Los procedimientos seguidos por el auditor en el conocimiento y evaluación de los sistemas de control interno de la entidad auditada.
- El análisis del riesgo inherente y de control.
- El diseño y aplicación por el auditor de las pruebas de cumplimiento y de los procedimientos sustantivos adecuados para alcanzar los objetivos de la auditoría.

## 5. FORMACIÓN TÉCNICA Y CAPACIDAD PROFESIONAL

A la hora de abordar las fiscalizaciones debe tenerse presente la norma 2.2.1 de los PNASP que establece que "**la auditoría deberá ser realizada por personas con formación técnica y capacidad profesional adecuadas.**"

La anterior afirmación de carácter general, y recogida en términos semejantes por todas las normas de auditoría, ha sido concretada en lo relativo al tema informático por la NTAEI, en el sentido de que **el auditor debe tener el conocimiento suficiente de los sistemas informáticos que le permita planificar, dirigir, supervisar y revisar el trabajo realizado.**

Además, dada la complejidad creciente de los sistemas informáticos, en cada trabajo, el auditor **debe evaluar si son necesarios para la auditoría conocimientos especializados sobre esta materia**, que permitan:

- Obtener un conocimiento suficiente de los sistemas contable y de control interno afectados por el *entorno informatizado*.
- Determinar el efecto del *entorno informatizado* en la evaluación del riesgo global y del riesgo a nivel de saldos y de tipos de transacciones.
- Diseñar y aplicar las adecuadas pruebas de cumplimiento y los procedimientos sustantivos.

Si el auditor considera que **sí** se requieren conocimientos especializados, **deberá obtener el apoyo de un profesional** que los posea, bien de su organización, bien ajeno a la misma.

En el caso de utilizar la ayuda de profesionales externos especializados, se deberá tener en cuenta el contenido de la Norma Técnica de Auditoría sobre la utilización de expertos independientes.

A pesar de lo anterior, todavía buena parte de los auditores fiscalizan en entornos informatizados sin variar sus procedimientos tradicionales, tratan la evidencia digital como si tuviera las mismas características o atributos que la evidencia física tradicional. El primer paso en mejorar la competencia o capacidad profesional será darse cuenta de las propias limitaciones y de que hay algunas materias, en particular las relacionadas con los entornos informatizados, que se desconocen.

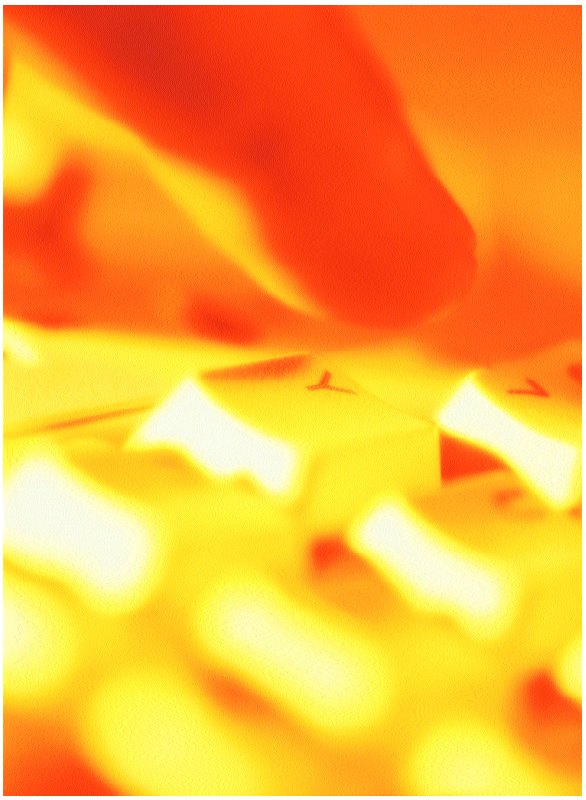
En relación con esto, y según la *International Education Guideline* nº 11 de la IFAC ("*Information Technology in the Accounting Curriculum*", párrafo 121), un auditor debe tener un conocimiento razonable de las principales técnicas de auditoría asistida por ordenador, sus ventajas, requisitos y limitaciones y debe ser capaz de usar al menos un programa de análisis y extracción de datos (como ACL o IDEA) y un programa de gestión de papeles de trabajo electrónicos (como TeamMate o Caseware Working Papers). Además de manejar Internet, el correo electrónico, agenda electrónica y, por supuesto, hoja electrónica y tratamiento de textos.

Así, de acuerdo con lo establecido en las normas técnicas citadas, los OCEX deben considerar la necesidad de formación para todos los niveles sobre

los conceptos relacionados con la auditoría en *entornos informatizados*, que debe incluir los siguientes aspectos:

- Normas técnicas de auditoría relacionadas.
- Características de los *entornos informatizados*.
- Profundización en la evaluación de los controles internos en *entornos informatizados*, distinción entre controles generales y controles de aplicación, su efecto en el riesgo de auditoría y en los procedimientos de auditoría aplicables.
- La evidencia informática.
- Introducción a los sistemas ERP y análisis de su impacto en nuestros procedimientos de auditoría.
- Introducción y aplicaciones prácticas de herramientas de análisis y extracción de datos.
- Utilización de papeles de trabajo electrónicos.
- Conceptos básicos sobre la auditoría de los sistemas de información.

También debe analizarse la necesidad de contratar la colaboración de expertos externos en auditoría de sistemas de información para apoyo a los equipos de auditoría en algunos aspectos del análisis de los controles informáticos.



## 6. DILIGENCIA PROFESIONAL Y ESCEPTICISMO PROFESIONAL

La norma 2.2.3 de los PNASP establece que "**la ejecución de los trabajos y la emisión de los informes se llevará a cabo con el debido cuidado profesional**", que principalmente impone al auditor el cumplimiento de las normas técnicas de auditoría.

Aunque es un concepto no recogido expresamente en los PNASP, la realización de las auditorías con un razonable grado de **"escepticismo profesional" es un elemento esencial de la diligencia profesional.** Dicho concepto, consustancial a la actividad auditora, ha adquirido una importancia creciente en los últimos años, recogiéndose de forma expresa en las NTA del ICAC sobre cumplimiento de la normativa y sobre errores e irregularidades[5].

**El escepticismo profesional es una actitud que requiere mentalidad o espíritu crítico y una evaluación crítica de la evidencia de auditoría**. Significa no confiar únicamente en las manifestaciones del auditado y no dar por sentado que los registros proporcionados por el auditado son auténticos sin otra evidencia corroborativa[6]. Esto puede plantear problemas a veces, cuando los registros informáticos (evidencia informática de transacciones o saldos) sólo pueden ser corroborados por otra evidencia informática. En estos casos su auten-

[5] Y también en la Directriz técnica de fiscalización nº 4 (párrafos 44 y 45) de la Sindicatura de Cuentas de la Comunidad Valenciana.

[6] Según Isaac Jonás, "Se trata, en definitiva, de evitar caer en la simplificación de asumir que todo lo que está informatizado es correcto, y de aplicar el escepticismo profesional que debe regir toda actuación del auditor también al proceso realizado en los propios sistemas de información, y por supuesto a los resultados obtenidos en los mismos, ..."; Jonás González, Isaac; "La auditoría de cuentas en entornos informatizados", *Partida Doble*, nº 156, junio de 2004.

ticidad y fiabilidad puede ser difícil o imposible de verificar sin comprender y verificar los controles informáticos relacionados.

La importancia de este concepto, y la reflexión sobre si lo aplicamos correctamente o no, debemos valorarla en relación con la evolución que han experimentado los sistemas informáticos de los entes que auditamos y nuestros propios procedimientos. Varios OCEX han celebrado ya su 20 aniversario y muchos de nosotros hemos podido apreciar la evolución que las TIC han tenido tanto en nuestras instituciones como en las distintas administraciones fiscalizadas. A pesar de esta evolución, en general, el tratamiento de los datos informáticos que auditamos, es básicamente (con algunas excepciones) el mismo que si se tratara de contabilidades con un bajo nivel de informatización; a veces se trabaja casi igual que hace 20 años[7].

Utilizamos muchos listados en papel o si acaso guardados en formato digital en nuestro ordenador. Estos listados, sobre los que hacemos determinadas comprobaciones son tan sólo una **visualización "física" de una evidencia informática**, que podrían haber sido fácilmente alterados para engañar al auditor. Sin embargo nuestras pruebas son casi las mismas que hace 20 años, raras veces se comprueban los controles de seguridad e integridad (por ejemplo) de esos listados, dando implícitamente por supuesto que existen. Y cuando se actúa así, se está, desde mi punto de vista, incurriendo en un riesgo importante de auditoría y se resiente la diligencia profesional exigida.

El apartado 5.3.10 de las Normas de Auditoría del Sector Público (NASP) de la IGAE recoge esta idea y dice que "Cuando se emplee evidencia informática, o datos procedentes de sistemas informáticos del auditado, los auditores deberán evaluar la fiabilidad de esta evidencia, y no darla nunca por supuesta a priori."

Cuanto más complejo sea el *entorno informático* mayor será el grado de escepticismo profesional requerido.

Dicho todo lo anterior, debe tenerse claro que, un auditor no tiene que ser necesariamente competente (especialista) en la obtención y examen de la evidencia informática para darse cuenta que la información proporcionada por los ordenadores no es fiable si no hay otra evidencia corroborativa, o no se ha realizado y documentado una revisión de los controles generales y de aplicación. Sólo tiene que actuar con la debida diligencia y escepticismo profesional y, debería preguntarse dos cosas:

¿Cuál es la probabilidad de que este listado u otro documento informático sea erróneo, tanto accidental como intencionadamente?

¿Quiénes, de la organización auditada, tienen la oportunidad y el incentivo para alterar los datos electrónicos por algún motivo?

Además de las dos anteriores y relacionadas con ellas, un auditor debe hacerse, entre otras, las siguientes preguntas:

¿Puede alterarse la evidencia informática sin dejar pistas de auditoría o rastros del cambio?

¿Hay una pista de auditoría que liga claramente la evidencia informática al hecho que la generó y en algunos casos hacia su inclusión en las cuentas anuales?

¿Contiene la evidencia informática información que identifique quién generó la entrada y cuándo?

¿Qué controles existen para prevenir cambios no autorizados en la evidencia informática después de su correcta generación?

¿Quién tiene derechos de acceso para cambiar la evidencia informática?

[7] Resulta interesante comprobar cómo en abril de 1991 la Sindicatura de Cuentas de Cataluña organizó un, avanzado para la época, "Curso sobre auditoría informática" al que asistimos auditores de los OCEX entonces existentes.
A pesar de su interés, la materia no fue desarrollada en ninguna institución, pero entiendo que la situación es muy diferente en estos momentos y la concienciación general de la necesidad de trabajar en esa dirección también, como ha podido contrastarse en el *I Foro tecnológico de los OCEX* celebrado en Valencia el pasado septiembre (ver información en www.sindicom.gva.es).

¿Cómo sabe el auditor que la evidencia informática no ha sido intencionadamente alterada para engañar o llevar a conclusiones equivocadas?

¿Tienen el sistema un "log" de auditoría adecuadamente establecido para registrar los intentos de acceso (éxitos y fracasos) a la evidencia informática?

¿Han sido revisados los "log" de auditoría por alguien independiente?

La respuesta a estas cuestiones ayudará al auditor a evaluar la fiabilidad de los datos informáticos, el riesgo de que existan incidencias significativas y a planificar pruebas de auditoría más eficaces, incluyendo la necesidad de que participe un experto en auditoría informática.

## 7. EVALUACIÓN PRELIMINAR DEL CONTROL INTERNO

De acuerdo con la segunda Norma Técnica sobre Ejecución del Trabajo del ICAC "deberá efectuarse un estudio y evaluación adecuada del control interno como base fiable para la determinación del alcance, naturaleza y momento de realización de las pruebas a las que deberán concretarse los procedimientos de auditoría".

El apartado 2.4.10 de la misma norma dice: "El estudio y evaluación del control interno incluye dos fases:

a) La revisión preliminar del sistema con objeto de conocer y comprender los procedimientos y métodos establecidos por la entidad. En particular, el conocimiento y evaluación preliminar de los sistemas de control interno de la entidad, **incluyendo los sistemas informáticos**, constituye un requisito mínimo de trabajo que sirve de base a la planificación de la auditoría.
b) La realización de pruebas de cumplimiento para obtener una seguridad razonable de que los controles se encuentran en uso y que están operando tal como se diseñaron."

Es decir, el auditor debe obtener una comprensión del control interno suficiente del ente fiscalizado para planificar la auditoría, realizando procedimientos para (1) identificar y comprender el diseño de los controles relevantes para una auditoría de las cuentas anuales y (2) comprobar si estos controles están siendo operativos.

Esta comprensión debe incluir la consideración de los métodos que una entidad usa para procesar la información contable, porque dichos métodos influyen en el diseño del control interno. La extensión con que los sistemas de información electrónicos son utilizados en aplicaciones contables importantes, así como la complejidad de dicho proceso pueden influir en la naturaleza, calendario y alcance de los procedimientos de auditoría.

La NTAEI establece que en la planificación de los aspectos de la auditoría susceptibles de ser influidos por el entorno informatizado de la entidad fiscalizada, el auditor deberá alcanzar una adecuada comprensión de:

- La importancia (materialidad) y la complejidad (volumen de transacciones, generación automática de transacciones, validación automática, etc) de la actividad de los sistemas informáticos de dicha entidad.
- La estructura organizativa de las actividades de los sistemas informáticos de la entidad.
- Así como la disponibilidad de datos para su utilización en la fiscalización.

El auditor debe documentar su comprensión de los componentes del control interno de una entidad relativo a las aplicaciones informáticas que procesan información usada en la preparación de los estados financieros, y basándose en dicha comprensión, se debe desarrollar un plan de auditoría con suficiente detalle como para demostrar su eficacia en reducir el riesgo de auditoría.

Cuando el entorno informatizado sea significativo, el auditor debe obtener el necesario conocimiento del entorno del mismo, y de su influencia en la evaluación del riesgo inherente y de control.

## 8. EVALUACIÓN DEL RIESGO DE AUDITORÍA

De acuerdo con las Normas Técnicas sobre Ejecución del Trabajo del ICAC (apartados 2.4.24 y 2.4.25), **el auditor debe evaluar el riesgo inhe-**

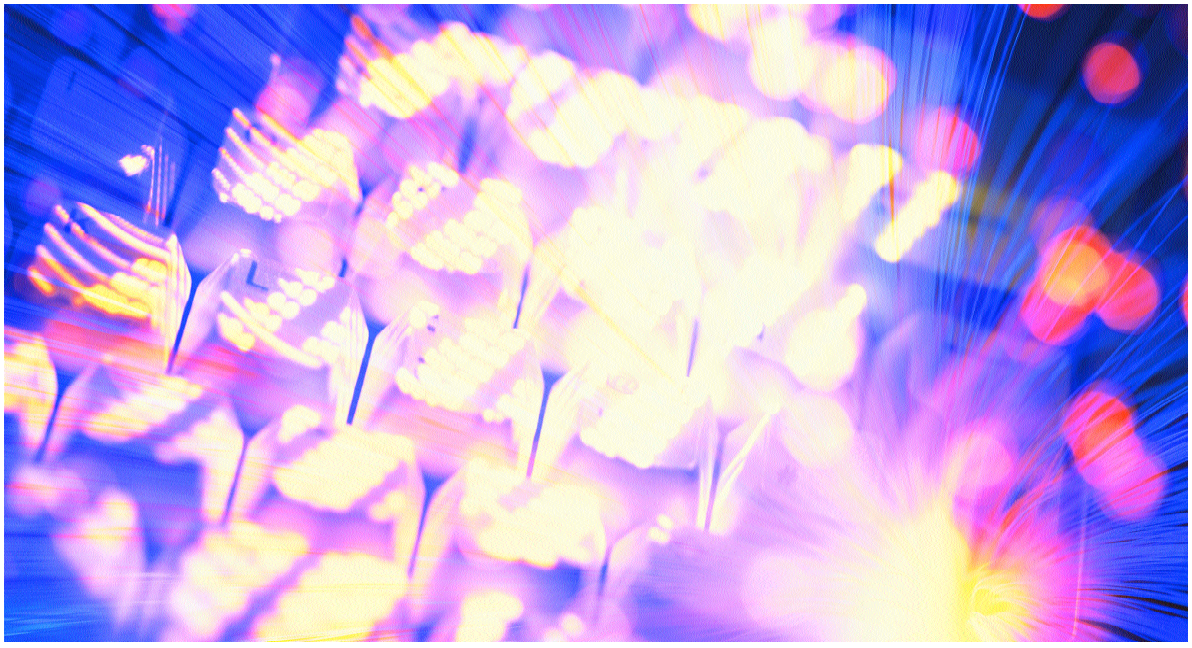
**rente y el riesgo de control para los componentes significativos de los estados financieros y minimizar el riesgo final (riesgo inherente + riesgo de control + riesgo de detección) a través de la combinación adecuada de pruebas de auditoría.**

Los problemas y factores de riesgo que con más frecuencia pueden aparecer en un *entorno informatizado* son, muy brevemente, los siguientes:

- Ausencia de rastro de las transacciones.
- Proceso uniforme de transacciones. Los errores de programación, u otros errores sistemáticos en el hardware o en el software, darán lugar a que todas las transacciones similares procesadas bajo las mismas condiciones, lo sean incorrectamente.
- Falta de segregación de funciones.
- Posibilidad de errores e irregularidades. La posibilidad de que algunas personas no autorizadas accedan a datos o los alteren sin que haya pruebas visibles de ello puede ser mayor con un sistema informático que con un sistema manual.
- Inicio o ejecución automático de transacciones. El sistema informático puede incluir la posibilidad de iniciar o ejecutar automáticamente determinados tipos de transacciones, cuya autorización puede no estar documentada de la misma forma que lo estaría en los sistemas manuales.
- El volumen de transacciones es tal que los usuarios de la aplicación podrían tener dificultades para identificar y corregir errores de proceso.
- El ordenador genera de forma automática tansaciones significativas o anotaciones directas en otras aplicaciones.
- El ordenador realiza cálculos complicados de información financiera y/o genera de forma automática transacciones significativas que no pueden ser, o no son, validadas independientemente.

Podemos decir que como consecuencia de los problemas que pueden presentarse en un entorno informatizado el riesgo de auditoría es creciente conforme se incrementa la complejidad del mismo.

Para minimizar el riesgo de auditoría a un nivel aceptable deben actualizarse las técnicas y procedimientos de auditoría, ya que en caso contrario se producirá un desfase creciente entre los métodos, tecnología, procedimientos de los entes fiscalizados y los de los auditores y como consecuencia podría



producirse un debilitamiento de la calidad y cantidad general de la evidencia obtenida si no se reacciona de forma adecuada.

Ante cada uno de los riesgos de auditoría que se identifiquen debe existir una respuesta clara y directa del auditor (un procedimiento de auditoría) que contrarrestre y minimice ese riesgo.

## 9. EVIDENCIA INFORMÁTICA DE AUDITORÍA

Las NASP regulan con una cierta profundidad aspectos relacionados con la obtención por el auditor de evidencia adecuada en un entorno informatizado.

De acuerdo con el apartado 5.3.2 de las NASP además de las tradicionales formas de evidencia (física, documental, analítica y testimonial), actualmente, en entornos informatizados, el auditor debe de tener en consideración la evidencia informática, que queda definida así:

> "**Evidencia informática**. – Información y datos contenidos en soportes electrónicos, informáticos y telemáticos, así como los elementos lógicos, programas y aplicaciones utilizados en los procedimientos de gestión del auditado. Esta evidencia informática incluirá los elementos identificados y estructurados que contienen texto, gráficos, sonidos, imágenes o cualquier otra clase de información que pueda ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información, o usuarios de tales sistemas, como unidades diferenciadas."

En un primer análisis de esta definición de evidencia informática vemos que se produce una distinción entre dos tipos de evidencia informática de características muy diferenciadas y que **requerirán capacidades profesionales, técnicas y procedimientos ad hoc**. Esta distinción es:

a) Información y datos

La implantación de sistemas de información automatizados en la administración ha provocado que la pista visible de muchas transacciones que rastreamos los auditores en las fiscalizaciones haya desaparecido físicamente, transformándose en algo más intangible[8].

No vamos a disponer, ya no disponemos en algunos casos, de los documentos físicos para poderlos visualizar, comprobar firmas, fotocopiar, poner tildes, etc. En muchos casos las facturas de proveedores, albaranes, etc. se escanean, se archivan en el ordenador y el original en papel desaparece, pudiéndose visualizar únicamente a través del sistema informático. En otros casos ni siquiera llega un documento físico a la entidad auditada ni se genera en la misma, sino que dichos documentos llegan en formato electrónico desde el exterior o desde otro departamento de la empresa o entidad, es decir los datos o documentos solo existen en formato electrónico.

Se hace necesario desarrollar nueva metodología de trabajo e introducir nuevas técnicas para poder recuperar y evaluar este tipo de evidencia informática.

Hay que tener presente que los atributos de la evidencia informática son diferentes de los de la evidencia tradicional en varios aspectos. En el siguiente cuadro se señalan las principales diferencias[9].

[8] En este sentido es conveniente repasar la IMNCL, que va en esa dirección:

Regla 14.- Soporte de los registros contables

1. Los registros de las operaciones y del resto de la información capturada en el SICAL-Normal, **estarán soportados informáticamente** según la configuración que se establece en la regla anterior, **constituyendo el soporte único y suficiente** que garantice su conservación de acuerdo con la regla 93.

2. **Las bases de datos del sistema informático** donde residan los registros **contables constituirán soporte suficiente** para la llevanza de la contabilidad de la entidad contable, sin que sea obligatoria la obtención y conservación de libros de contabilidad…

Regla 88.- Medios de justificación

1. La **justificación** de los distintos hechos susceptibles de incorporación al SICAL-Normal **podrá estar soportada en documentos en papel o a través de medios electrónicos, informáticos o telemáticos...**

[9] Édmond, Caroline; *Electronic Audit Evidence*; The Canadian Institute of Chartered Accountants, 2003.

| Evidencia de auditoría tradicional | Evidencia informática de auditoría |
|---|---|
| Origen | |
| Se puede establecer con facilidad el origen/procedencia. | Es difícil determinar el origen si únicamente se examina información en soporte informático. Se requiere la utilización de controles y de técnicas de seguridad que permitan la autenticación y reconocimiento. |
| Alteración | |
| La evidencia en papel es difícil de alterar sin que se detecte. | Es difícil, si no imposible, detectar cualquier alteración únicamente mediante el examen de la información en soporte informático. La integridad de la información depende de los controles fiables y de las técnicas de seguridad empleadas. |
| Aprobación | |
| Los documentos en papel muestran la prueba de su aprobación en su superficie. | Es difícil de establecer la aprobación si únicamente se examina la información en soporte informático. Se requiere la utilización de controles y de técnicas de seguridad. |
| Compleción | |
| Todos los términos relevantes de una operación/transacción se incluyen por lo general en un mismo documento. | Los términos más significativos aparecen a menudo en distintos archivos de datos. |
| Lectura | |
| No se requiere ningún tipo de herramienta o equipo. | Es necesaria la utilización de distintas tecnologías y herramientas. |
| Formato | |
| Parte integral del documento. | El formato viene separado de los datos y puede modificarse. |
| Disponibilidad y accesibilidad | |
| Normalmente no es una restricción durante la fiscalización. | Las pistas de auditoría para la información en soporte informático puede que no estén disponibles en el momento de la auditoría y el acceso a los datos puede resultar más difícil. |
| Firma | |
| Es sencillo firmar un documento en papel y comprobar la firma. | Se necesitan las tecnologías adecuadas para realizar una firma electrónica fiable y revisarla. |

Las operaciones de recolección y análisis de esta evidencia, empleando para ello las técnicas y herramientas de auditoría asistida por ordenador necesarias y/o disponibles en cada momento (como ACL o IDEA), son abordables por cualquier auditor que reúna unos requisitos de formación mínima[10].

A fin de poder valorar la suficiencia y lo apropiado de la evidencia informática recopilada para respaldar el informe de auditoría, el auditor debería considerar los riesgos específicos asociados al uso de este tipo de evidencia. Estos riesgos no pueden ser evaluados únicamente revisando la evidencia documental, como suele hacerse con los documentos en papel. La copia impresa de la información en soporte informático o la lectura de la información directamente de la pantalla del ordenador es solamente un formato. Y éste no proporciona ninguna indicación del origen y autorización, ni tampoco garantiza la integridad ni la compleción de la información. Los auditores deberían asegurar que los controles y las distintas tecnologías utilizadas para crear, procesar, transmitir y guardar información en soporte informático son suficientes para garantizar su fiabilidad.

b) Programas y aplicaciones

La revisión de los procedimientos administrativos y contables, el flujo de documentos, autorizaciones, segregación de funciones, etc. existentes en el seno de la organización auditada ha formado parte siempre de los procedimientos ordinarios de auditoría. En este sentido la revisión de los sistemas lógicos informáticos de gestión proporcionan evidencia de auditoría ya que nos permiten conocer cuál es el flujo de documentos electrónicos, las autorizaciones explícitas a implícitas, segregación de funciones, los controles de seguridad existentes y otros procedimientos de control interno[11].

Actualmente con sistemas complejos que interrelacionan e integran distintas áreas funcionales de las organizaciones, y la desaparición progresiva del soporte papel, etc, el análisis y evaluación de tales sistemas **excederá normalmente las competencias de un auditor financiero requiriéndose la intervención de un especialista en auditoría informática**.

## 10. PROCEDIMIENTOS DE AUDITORÍA

De acuerdo con la NTAEI "el auditor debe tener en cuenta el entorno informatizado en el diseño de los procedimientos de auditoría necesarios para reducir el riesgo de auditoría a un nivel aceptable.

Los objetivos específicos de auditoría no se ven afectados por el hecho de que los datos contables se procesen manualmente o mediante ordenador. Sin embargo, los métodos para obtener la evidencia de auditoría adecuada y suficiente, pueden verse influenciados por los procesos informáticos. El auditor puede utilizar tanto procedimientos manuales como técnicas de auditoría asistidas por ordenador o bien una combinación de ambos métodos, al objeto de obtener dicha evidencia. Sin embargo, en algunos sistemas contables que utilizan un ordenador para llevar a cabo aplicaciones significativas, puede ser difícil o imposible que el auditor obtenga ciertos datos sin apoyo informático."

[10] El Plan Trienal 2005-2007 de la Sindicatura de Cuentas de la Comunidad Valencia, plantea como objetivo para 2006 que el 50% del personal de auditoría sea capaz de manejar la herramienta de análisis y extracción de datos implantada en la Institución (ACL).

[11] Resulta pertinente recordar, a modo de ilustración, lo que se establece en la Regla 90.2 de la IMNCL:

2. Cuando las operaciones se incorporan al sistema mediante la utilización de soportes electrónicos, informáticos o telemáticos, los procedimientos de autorización y control mediante diligencias, firmas manuscritas, sellos u otros medios manuales podrán ser **sustituidos por autorizaciones y controles establecidos en las propias aplicaciones informáticas** que garanticen el ejercicio de la competencia por quien la tenga atribuida.

Y en la Regla 91.2 Toma de razón:

2. En el caso de que las operaciones sean registradas a partir de los datos contenidos en soportes electrónicos, informáticos o telemáticos, la diligencia de toma de razón se sustituirá por los oportunos **procesos de validación en el sistema**, mediante los cuales dichas operaciones queden referenciadas en relación con las anotaciones contables que hayan producido.

Los auditores deberán tener evidencia suficiente y adecuada de que los datos provenientes de sistemas informáticos sean válidos y fiables cuando tales informaciones sean significativas para los resultados de la auditoría.

La NTAEI explícitamente exige al auditor la revisión de los sistemas de control informatizados, la evaluación del riesgo de auditoría correspondiente y la realización de pruebas de cumplimiento.

Aunque deberemos efectuar en todo caso pruebas sustantivas para verificar transacciones y saldos de importe significativo, **en determinadas situaciones, no será posible reducir el riesgo de detección a un nivel aceptable, realizando únicamente pruebas sustantivas.**

La decisión para adoptar un determinado enfoque de auditoría no dependerá tanto del tamaño de la entidad auditada como del grado de complejidad del *entorno informatizado*.

## 11. CONCLUSIÓN

He tratado en estas breves líneas de señalar la necesidad de que los órganos de control externo aborden decididamente la implantación de nuevas técnicas y metodología de auditoría para ejecutar con plena eficacia y la máxima eficiencia las fiscalizaciones que tienen encomendadas, sobre unas administraciones públicas que operan en entornos informatizados de una complejidad cada vez mayor.

Se debe realizar un profundo cambio para evolucionar de unas fiscalizaciones/auditorías realizadas "alrededor del ordenador" a otras realizadas "a través del ordenador". Para ello, algunas de las medidas que se deberían adoptar son:

- Formación general del personal auditor en las técnicas y procedimientos relacionados con la auditoría en entornos informatizados, evaluación de riesgos y revisión de procedimientos de control.
- Creación de un grupo pequeño especializado en auditoría informática y/o incorporación de personal técnico especialista (CISA).
- Contratar la colaboración externa de especialistas en auditoría informática para que colaboren en las fiscalizaciones (en una primera etapa, esta medida la considero casi ineludible, como paso previo a la disposición de personal propio especializado).
- Realización de fiscalizaciones por equipos pluridisciplinares.

Para terminar, la conclusión final sería que todos los OCEX deben adoptar las medidas apropiadas, según su situación particular, con la máxima celeridad, ya que los ciudadanos esperan que se les proporcionen informes de fiscalización de la máxima calidad técnica, acordes con las tecnologías utilizadas en el siglo XXI.