Resolución de 23 de junio de 2003, del Instituto de Contabilidad y Auditoría de Cuentas, por la que se publica la Norma Técnica de Auditoría sobre "la auditoría de cuentas en entornos informatizados"

En la actualidad, las distintas empresas y entidades utilizan, con carácter general, sistemas informáticos en el procesamiento, registro, almacenamiento, elaboración y presentación de su información financiera, además de, en muchos casos, en el propio ejercicio de su actividad. Este hecho afecta a los sistemas contable y de control interno de las entidades, por lo que el auditor debe tener presente tal circunstancia en el desarrollo de sus trabajos de auditoría de cuentas.

A estos efectos, con el objeto de establecer reglas y suministrar criterios de actuación al auditor en los casos en los que la entidad auditada se encuentre inmersa en un entorno informatizado, el Instituto de Censores Jurados de Cuentas de España, el Consejo General de Colegios de Economistas de España y el Consejo Superior de Colegios Oficiales de Titulados Mercantiles de España presentaron ante este Instituto la Norma Técnica de Auditoría sobre "la auditoría de cuentas en entornos informatizados", para su tramitación y sometimiento a información publica, conforme a lo previsto en el artículo 5.2 de la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas.

Por Resolución de 26 de septiembre de 2002 del Instituto de Contabilidad y Auditoría de Cuentas se procedió a su publicación íntegra en el propio Boletín de este Instituto, de septiembre de 2002 (número 51), y a la oportuna reseña en el Boletín Oficial del Estado de 15 de noviembre de 2002, para someterla al trámite de información pública previsto legalmente.

En dicho trámite no se han presentado alegaciones al texto sometido a información pública, por lo que, de acuerdo con lo establecido en el citado artículo 5.2 de la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas, **la Presidencia de este Instituto dispone lo siguiente:**

Una vez superado el trámite de información pública, establecido por la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas, se acuerda el paso a definitiva de la Norma Técnica de Auditoría sobre "la auditoría de cuentas en entornos informatizados", y se ordena, asimismo, su publicación íntegra en el "Boletín Oficial del Instituto de Contabilidad y Auditoría de Cuentas" y la inserción de la oportuna reseña en el "Boletín Oficial del Estado".

NORMA TÉCNICA DE AUDITORÍA SOBRE "LA AUDITORÍA DE CUENTAS EN ENTORNOS INFORMATIZADOS"

INTRODUCCIÓN

1. Las Normas Técnicas de Auditoría en su apartado 2.4.1 y 2.4.2 establecen lo siguiente:

> *"2.4.1. Deberá efectuarse un estudio y evaluación adecuada de 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 auditoria.*
>
> *2.4.2. A tal efecto es preciso distinguir entre el estudio destinado a evaluar y mejorar el sistema de control interno de una entidad, realizado por el auditor en su calidad de experto y en virtud de mandato específico, del estudio y evaluación de control interno que se realiza en el contexto de una auditoría, y al que se refieren estas Normas Técnicas."*

Asimismo, dichas Normas Técnicas de Auditoría en su apartado 2.4.10, establecen:

> *"2.4.10. El estudio y evaluación del sistema de 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."*

2. A los efectos de esta Norma Técnica:

a) existe un entorno informatizado cuando la entidad, al procesar información financiera que sea significativa a efectos de la auditoría, emplea un ordenador, de cualquier tipo o tamaño, ya esté gestionado por la propia compañía o por un tercero.

b) se entiende por sistemas informáticos, aquellos relacionados con el procesamiento, almacenamiento, transmisión y emisión de la información financiera.

OBJETO

3. El objeto de la presente norma es establecer reglas y suministrar una guía respecto a los procedimientos a seguir cuando se realice una auditoría en un entorno informatizado.

4. El auditor debe evaluar la manera en que el entorno informatizado afecta a la auditoría.

5. El objetivo global y el alcance de una auditoría no cambian en un entorno informatizado. Sin embargo, el uso de un ordenador puede afectar a los sistemas contable y de control interno empleados por la entidad. Consecuentemente, un entorno informatizado puede afectar a:

a. Los procedimientos seguidos por el auditor en el conocimiento y evaluación preliminar de los sistemas de control interno de la entidad

b. El análisis del riesgo inherente y de control mediante el que el auditor llega a la evaluación del riesgo.

c. El diseño y aplicación por el auditor de las pruebas de control y de los procedimientos sustantivos adecuados para alcanzar el objetivo de la auditoría.

CONOCIMIENTOS Y COMPETENCIA

6. El auditor debe tener el conocimiento suficiente de los sistemas informáticos, que le permita planificar, dirigir, supervisar y revisar el trabajo realizado. Debe evaluar si es necesario para la auditoría disponer de conocimientos especializados sobre esta materia que permitan:

a. Entender suficientemente de los sistemas contable y de control interno afectados por el entorno informatizado.

b. Determinar el efecto del entorno informatizado en la evaluación del riesgo global y del riesgo a nivel de saldos contables y de tipos de transacciones.

c. Diseñar y aplicar las adecuadas pruebas de control y los procedimientos sustantivos.

Si el auditor estima que se requieren conocimientos específicos para cubrir los aspectos anteriormente indicados, podrá obtener asesoramiento de otros profesionales que los posean, bien de su propia organización o bien ajenos a la misma.

En el caso de que el auditor obtenga asesoramiento de otros profesionales externos especializados, deberá tener en cuenta el contenido de la Norma Técnica de Auditoría sobre la utilización del trabajo de expertos independientes por auditores de cuentas.

PLANIFICACIÓN

7. De acuerdo con las Normas Técnicas de Auditoría, el auditor debe entender suficientemente los sistemas contable y de control interno para planificar la auditoría y definir un enfoque adecuado a la misma.

8. Al planificar las áreas de la auditoría que pueden resultar afectadas por el entorno informatizado de la entidad, el auditor debe alcanzar una adecuada comprensión de la importancia y complejidad de las actividades de los sistemas informáticos, así como de la disponibilidad de datos para su utilización en la auditoría. Tal conocimiento podría incluir los siguientes aspectos:

a) Importancia y complejidad del proceso informático en cada una de las aplicaciones contables significativas. La importancia, en este caso, se refiere a la materialidad de las informaciones contenidas en las cuentas anuales afectadas por el proceso informático. Una aplicación informática puede considerarse compleja cuando, por ejemplo:

i) El volumen de transacciones es tal que los usuarios de la misma podrían tener dificultades para identificar y corregir errores de proceso.

ii) El ordenador genera de forma automática transacciones significativas o anotaciones directas en otras aplicaciones.

iii) 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.

iv) Se intercambian electrónicamente transacciones con otras organizaciones (sistemas de intercambio electrónico de datos) sin validación manual.

b) La estructura organizativa de las actividades de los sistemas informáticos de la entidad, así como el grado de centralización del proceso informático, ya que pueden afectar a la segregación de funciones.

c) La disponibilidad de los datos. En ocasiones sólo se mantienen durante un corto periodo de tiempo o únicamente en soportes de lectura informatizada los documentos fuente, determinados archivos informáticos y otras evidencias que el auditor pudiera requerir. Los sistemas informáticos de la entidad pueden generar información interna útil para la aplicación de pruebas sustantivas (especialmente procedimientos analíticos). La posibilidad de utilizar técnicas de auditoría asistida por ordenador puede permitir aumentar la eficiencia de los procedimientos de auditoría, o hacer posible la aplicación, sin excesivo coste, de algunos procedimientos sobre la población completa de saldos o transacciones.

9. Cuando los sistemas informáticos sean significativos, el auditor debe asimismo obtener el necesario entendimiento del entorno de los mismos, y si pueden influir en la evaluación del riesgo inherente y de control. Un entorno informatizado implica entre otros los siguientes tipos de riesgos y características de control interno:

a) Ausencia de rastro de las transacciones. Algunos sistemas informáticos están diseñados de manera que el rastro completo de una transacción, útil para la auditoría, puede existir sólo durante un periodo corto de tiempo, o de manera que su lectura sólo sea posible a través de medios informáticos. Cuando una aplicación informática compleja lleva a cabo un amplio número de etapas de procesamiento, puede no existir un rastro completo. Consecuentemente, los errores que pudiera tener un programa serían difíciles de detectar de manera oportuna por procedimientos manuales.

b) Proceso uniforme de transacciones. El ordenador procesa uniformemente transacciones similares. De esta forma se eliminan en su totalidad los errores administrativos asociados a procesos manuales. Pero, por el contrario, 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.

c) Falta de segregación de funciones. Muchos de los procedimientos de control que normalmente serían ejecutados por personas diferentes en sistemas manuales pueden encontrarse concentrados en sistemas informáticos. Así, una persona que

tenga acceso a los programas, a los procesos o a los datos podría realizar funciones incompatibles.

d) Posibilidad de errores e irregularidades. La posibilidad de errores humanos en el desarrollo, mantenimiento y ejecución de sistemas informatizados de control pueden ser mayores que en los sistemas manuales, en parte a causa del nivel de minuciosidad requerido.

Además, 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.

Al disminuir la participación humana en las transacciones procesadas por sistemas informáticos se puede reducir la posibilidad de detectar errores e irregularidades. Igualmente, los errores e irregularidades incurridos durante el diseño o modificación de los programas o aplicaciones pueden permanecer ocultos durante largos períodos de tiempo.

e) 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, e incluso dicha autorización puede estar implícita en la aceptación por parte de la dirección del diseño del sistema informático y sus posteriores modificaciones.

f) Controles basados en procesos informáticos. El proceso informático puede producir informes y otros datos utilizados en la realización de controles manuales. La efectividad de estos controles manuales puede depender de la efectividad de los controles sobre la integridad y la exactitud del proceso informático. A su vez, la efectividad y el funcionamiento uniforme de los controles específicos de las aplicaciones que procesen transacciones depende a menudo de la efectividad de los controles generales de los sistemas informáticos.

g) Posibilidad de mayor supervisión de la dirección. Los sistemas informáticos pueden ofrecer a la dirección una variedad de herramientas analíticas que se pueden utilizar para revisar y supervisar las operaciones de la entidad. La disponibilidad de estos controles adicionales, si se utilizan, puede servir para mejorar la estructura global de control interno.

h) Posibilidad de utilización de técnicas de auditoría asistidas por ordenador. La facilidad que los sistemas informáticos ofrecen para procesar y analizar grandes cantidades de datos brinda al auditor la oportunidad de aplicar técnicas generales o especializadas de auditoría asistida por ordenador, como instrumentos para la ejecución de pruebas de auditoría.

10. Los riesgos y los controles derivados de estas características de los sistemas informáticos tienen un impacto potencial en la evaluación del riesgo por parte del auditor, así como en la naturaleza, momento de realización y alcance de los procedimientos de auditoría.

11. Como Anexo a esta Norma Técnica se incluye, a título meramente informativo, una guía descriptiva de las características y controles internos que pueden encontrarse en un entorno informatizado.

EVALUACIÓN DEL RIESGO

12. De acuerdo con las Normas Técnicas de Auditoría de ejecución del trabajo, el auditor debe tener en cuenta el riesgo inherente y el riesgo de control respecto a la posibilidad de que existan errores significativos en los estados financieros y, consecuentemente, minimizar el riesgo final a través de la combinación adecuada de pruebas de auditoría.

13. La probabilidad de que se produzcan errores e irregularidades significativas en el conjunto de la información financiera o en cuentas específicas depende de los riesgos inherentes y de control en un entorno informatizado, según se expone a continuación:

a) Estos riesgos pueden resultar de deficiencias en las actividades generales del sistema informático, tales como desarrollo y mantenimiento de programas, soporte de los sistemas, operaciones del sistema, seguridad física del centro informático y control de acceso a programas de utilización restringida. Estas deficiencias pueden tener un impacto global en todas las aplicaciones informáticas.

b) Asimismo estos riesgos pueden incrementar la posibilidad de errores o irregularidades en aplicaciones específicas, en bases de datos concretas o en archivos maestros, o en determinados procesos. Por ejemplo, no es inusual encontrar errores en sistemas que realizan procesos lógicos o de cálculo complejos, o que pueden tratar con multitud de condiciones de excepción diferentes. Asimismo, los sistemas que controlan desembolsos en efectivo u otros activos líquidos son susceptibles de acciones fraudulentas por parte de los usuarios o por el personal del área informática.

c) La aparición de nuevas tecnologías informáticas, aumenta la sofisticación global del sistema informático y la complejidad de sus aplicaciones específicas. Como resultado, pueden verse incrementados los riesgos inherentes y de control.

PROCEDIMIENTOS DE AUDITORÍA

14. De acuerdo con las Normas Técnicas de Auditoría 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.

15. 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.

ANEXO

Guía descriptiva de características y controles internos en entornos informatizados

A. Características de los entornos informatizados

Un entorno informatizado puede presentar las siguientes características que lo diferencien, en mayor o menor grado, de un entorno manual:

1. Estructura organizativa

a) Concentración de funciones e información.

b) Concentración de programas y datos.

2. Naturaleza del procesamiento

a) Ausencia de documentos de entrada.

b) Inexistencia de rastro visible de la transacción.

c) Inexistencia de datos de salida tangibles.

d) Mayor facilidad de acceso a los datos y programas informáticos.

3. Diseño y procesamiento

a) Uniformidad en la ejecución de procesos.

b) Procedimientos de control incluidos en los propios programas.

c) Actualización de varios archivos o bases de datos con una sola transacción.

d) Transacciones generadas directamente por el sistema.

e) Vulnerabilidad de acceso a los archivos de datos y programas.

B. Controles internos en entornos informatizados

Los controles internos relativos a los procesos informáticos comprenden tanto los controles generales que afectan al entorno informatizado en su conjunto como los controles específicos de las distintas aplicaciones contables. Tales controles se pueden desarrollar mediante procedimientos manuales o mediante procedimientos diseñados en los propios programas informáticos.

1. Controles generales de un entorno informatizado

El propósito de los controles generales de un entorno informatizado es establecer un marco conceptual de control general sobre las actividades del sistema informático y asegurar razonablemente la consecución de los objetivos generales de control interno. Los controles generales de un entorno informatizado pueden incluir:

1.1 Controles de organización y dirección.- Diseñados para establecer el marco general de organización de las actividades del sistema informático, incluyendo:

a) Políticas y procedimientos relativos a funciones de control.

b) Adecuada segregación de funciones incompatibles (preparación de transacciones de entrada, programación y explotación).

1.2 Controles sobre el desarrollo y mantenimiento de aplicaciones.- Diseñados para asegurar razonablemente que los sistemas se desarrollan y mantienen previa autorización y de forma eficiente. Se diseñan, por lo general para establecer control sobre:

a) Ejecución de pruebas, conversión, implantación y documentación de sistemas nuevos o de revisiones.

b) Cambios en las aplicaciones.

c) Acceso a la documentación de los sistemas.

d) Adquisición de aplicaciones de terceros.

1.3 Controles sobre operaciones realizadas a través del ordenador.- Diseñadas para controlar las operaciones que se realizan desde el sistema y para asegurar razonablemente que:

a) El sistema se está utilizando exclusivamente para propósitos autorizados.

b) El acceso a las operaciones realizadas desde el ordenador está restringido a personal autorizado.

c) Sólo se utilizan programas autorizados.

d) Se detectan y corrigen los errores de procesamiento.

1.4 Controles sobre el software de los sistemas.- Diseñados para asegurar r azonablemente que el software de los sistemas se ha adquirido y desarrollado de forma autorizada y eficiente, incluyendo:

a) Autorización, aprobación, pruebas, implantación y documentación de los nuevos software de sistemas y de sus modificaciones.

b) Restricción de acceso al software de sistemas y documentación al personal autorizado.

1.5 Controles de entrada de datos y de programa.- Diseñados para asegurar razonablemente que:

a) Se ha establecido una adecuada estructura de autorización sobre las transacciones a introducir en el sistema.

b) El acceso a los datos y programas se encuentra restringido al personal autorizado.

1.6 Existen otras salvaguardas que contribuyen a la continuidad de las operaciones de procesamiento en entornos informatizados. Entre estas se pueden citar:

a) Mantenimiento aprobación, pruebas, implantación y documentación de los nuevos software de sistemas y de sus modificaciones.

b) Procedimientos de e recuperación aplicables en el caso de robo, pérdida o destrucción accidental o intencionada.

c) Establecimiento de centros alternativos de procesamientos en el caso de catástrofes.

2. Controles de aplicación de un entorno informatizado

El objetivo de los controles de aplicación en un entorno informatizado es establecer procedimientos de control específicos sobre las aplicaciones contables con el fin de asegurar razonablemente que todas las transacciones son autorizadas y registradas, y que son procesadas de forma completa, adecuada y oportuna. Los controles de aplicación de un entorno informatizado incluyen:

2.1 Controles de entrada.- Diseñados para asegurar razonablemente que:

a) Las transacciones son adecuadamente autorizadas antes de que sean procesadas informáticamente.

b) Las transacciones se trasfieren correctamente al soporte informático y se incluyen en los archivos de datos del ordenador.

c) Las transacciones no son objeto de pérdida, duplicación, manipulación o alteración.

d) Las transacciones incorrectas son rechazadas, corregidas y, en su caso, reprocesadas oportunamente.

2.2 Controles sobre el procesamiento y los ficheros informáticos de datos.- Diseñados para asegurar razonablemente que:

a) Las transacciones, incluidas las que genera el propio sistema, son adecuadamente procesadas por el ordenador.

b) Las transacciones no son objeto de pérdida, duplicación, manipulación o alteración.

c) Los errores de procesamiento se identifican y corrigen a tiempo.

2.3 Controles de salida.- Diseñados para asegurar razonablemente que:

a) Los resultados del procesamiento son adecuados.

b) El acceso a los datos de salida del sistema está restringido al personal autorizado.

c) Los datos de salida del sistema llegan al personal autorizado en tiempo oportuno.