Evaluación de Riesgos y Control Interno- Características y Consideraciones de CIS

NIA 6

Norma Internacional de Auditoría 6

Corporación Edi-Ábaco Cía. Ltda.

Instrucciones de Ubicación:

NIA: En este acápite ubica la información correspondiente al tema referido. Si requiere indicaciones adicionales sobre el funcionamiento y la estructura del servicio, favor diríjase a la sección ÍNDICE de la carpeta impresa o al archivo LÉAME de la carpeta EDIÁBACO de la base de datos de su computador.

Título general de la obra: ***Actualización Contable***
Título de ésta norma: ***NIA 6 Sección 1008: Evaluación de Riesgos y Control Interno-Características y Consideraciones de CIS.***

Primera Edición: En Recurso Informático: 2002

Revisión y Edición: *Corporación Edi-Ábaco Cía. Ltda.*
Revisión Técnica: *Geovanny Córdova J.*
Diseño Gráfico y Diagramación: *Margoth Coronado V.*

Tiraje: 1.000 copias Editado en Ecuador

ISBN-9978-95-009-5 Registro Nacional de Derechos de Autor: 009508

ACERCA DE ESTA EDICIÓN:

En la presente edición, Corporación Edi-Ábaco Cía. Ltda., ofrece el contenido del ***la Norma Internacional de Auditoría NIA 6: Evaluación de Riesgos y Control Interno-Características y Consideraciones de CIS. Sección 1008,*** *conforme a los textos originales del Instituto Mexicano de Contadores Públicos (IMCP).*

Se ha rediagramado íntegramente la presentación del texto, para facilitar la utilización y comprensión del mismo, y se han corregido errores tipográficos y ortográficos.

Para las siguientes ediciones se tiene previsto incluir como valor agregado, ejercicios de aplicación en lo que la norma permita

El Editor

CONTENIDO

Las Normas Internacionales de Auditoría (NIAs) se deberán aplicar en la auditoría de los estados financieros. Las NIA también deberán aplicarse, adaptadas según sea necesario, a la auditoría de otra información y a servicios relacionados.

Las NIAs contienen los principios básicos y los procedimientos esenciales (identificados en letra negra) juntos con los lineamientos relativos en forma de material explicativo y de otro tipo. Los principios básicos y los procedimientos esenciales deben interpretarse en el contexto del material explicativo y de otro tipo que proporciona lineamientos para su aplicación.

Para comprender y aplicar los principios básicos y los procedimientos esenciales junto con los lineamientos relacionados, es necesario considerar el texto íntegro de la NIA incluyendo el material explicativo y de otro tipo contenido en la NIA, y no sólo el texto resaltado en negro.

En circunstancias excepcionales, un auditor puede juzgar necesario apartarse de una NIA para lograr en forma más efectiva el objetivo de una auditoría. Cuando surge una situación así, el auditor deberá estar preparado para justificar la desviación.

Las NIAs necesitan ser aplicadas sólo a asuntos de importancia relativa.

La Perspectiva del Sector Público (PSP) emitida por el Comité del Sector Público de la Federación Internacional de Contadores se expone al final de una NIA. Cuando no se añade PSP, la NIA es aplicable, respecto de todo lo importante, al sector público.

EVALUACIÓN DE RIESGOS Y CONTROL INTERNO- CARACTERÍSTICAS Y CONSIDERACIONES DE CIS

Introducción

1. Un entorno de procesamiento electrónico de datos (CIS) se define en la Norma Internacional de Auditoría (NIA) "Auditoría en un Entorno de Sistemas de Información por Computadora," como sigue:

> Para los fines de las Normas Internacionales de Auditoría, existe un entorno de CIS cuando hay implicada una computadora de cualquier tipo o tamaño en el procesamiento por parte de la entidad de información financiera de importancia para la auditoría, ya sea que la computadora sea operada por la entidad o por un tercero.

La introducción de todos los controles deseados de CIS puede no ser factible cuando el tamaño del negocio es pequeño o cuando se usan microcomputadoras independientemente del tamaño del negocio. También, cuando los datos son procesados por un tercero, la consideración de las características del entorno de CIS puede variar dependiendo del grado de acceso al procesamiento del tercero. Se ha desarrollado una serie de Declaraciones Internacionales de Auditoría para suplementar los siguientes párrafos. Esta serie describe diversos entornos de CIS y su efecto sobre los sistemas de contabilidad y de control interno y sobre los procedimientos de auditoría.

Estructura organizacional

2. En un entorno de CIS, una entidad establecerá una estructura organizacional y procedimientos para administrar las actividades de CIS. Las características de una estructura organizacional de CIS incluyen:

   a. *Concentración de funciones y conocimiento.*- aunque la mayoría de los sistemas que emplean métodos de CIS incluye ciertas operaciones manuales, generalmente el número de personas involucradas en el procesamiento de información financiera es significativamente reducido. Más aún, cierto personal de procesamiento de datos pueden ser los únicos con un conocimiento detallado de la interrelación entre las fuentes de datos, cómo se procesan, y la distribución y uso de los datos de salida. Es también probable que estén conscientes de cualesquiera debilidades en el control interno y, por lo tanto, pueden estar en posición de alterar programas o datos mientras están almacenados o durante el procesamiento. Todavía más, pueden no existir muchos controles convencionales basados en la segregación adecuada de funciones incompatibles, o en ausencia de controles de acceso u otros, pueden ser menos efectivos.

b. *concentración de programas y datos.*- a menudo están concentrados los datos por transacción y del archivo maestro, generalmente en forma legible por la máquina, ya sea en una instalación de computadora localizada centralmente o en un número de instalaciones distribuidas por toda una entidad. Es probable que los programas de computadora que dan la capacidad de obtener acceso a, y de alterar dichos datos estén almacenados en la misma locación que los datos. Por lo tanto, en ausencia de controles apropiados, hay un mayor potencial para acceso no autorizado a, y alteración de, programas y datos.

Naturaleza del procesamiento

3. El uso de computadoras puede dar como resultado el diseño de sistemas que proporcionen menos evidencia que aquellos que usen procedimientos manuales. Además, estos sistemas pueden ser accesibles a un mayor número de personas. Las características del sistema que pueden ser resultado de la naturaleza del procesamiento CIS incluyen:

   a. *Ausencia de documentos de entrada*—los datos pueden ser alimentados directamente al sistema por computadora sin documentos que los soporten. En algunos sistemas de transacción en línea, la evidencia por escrito de la autorización de alimentación de datos individuales (por ej., aprobación para entrada de CISidos) puede ser reemplazada por otros procedimientos, como controles de autorización contenidos en los programas de computadora (por ej., aprobación de límite de crédito).

   b. *Falta de rastro visible de transacciones*— ciertos datos pueden mantenerse en archivos de computadora solamente. En un sistema manual, normalmente es posible seguir una transacción a través del sistema examinando los documentos fuente, libros de cuentas, registros, archivos y reportes. En un entorno de CIS, sin embargo, el rastro de la transacción puede estar parcialmente en forma legible por máquina, y todavía mas, puede existir sólo por un periodo limitado de tiempo.

   c. *Falta de datos de salida visibles*— ciertas transacciones o resultados del procesamiento pueden no imprimirse. En un sistema manual, y en algunos sistemas de CIS, es posible normalmente examinar en forma visual los resultados del procesamiento. En otros sistemas de CIS, los resultados del procesamiento no pueden imprimirse, o pueden imprimirse sólo datos resumidos. Así, la falta de datos de salida visibles puede dar como resultado la necesidad de tener acceso a datos retenidos en archivos legibles sólo por computadora.

   d. *Facilidad de acceso a datos y programas de computadora* —se puede tener acceso a los datos y los programas de computadora, y pueden ser alterados, en la computadora o por medio del uso de equipo de computación en locaciones remotas. Por lo tanto, en ausencia de controles apropiados, hay un potencial mayor para el acceso no autorizado a, y la alteración de, datos y programas por personas dentro o fuera de la entidad.

Aspectos de diseño y de procedimiento

4. El desarrollo de sistemas de CIS generalmente dará como resultado el diseño y características de procedimientos que son diferentes de los que se encuentran en los sistemas manuales. Estos aspectos diferentes de diseño y de procedimiento de los sistemas de CIS incluyen:

   a. *Consistencia de funcionamiento*— los sistemas de CIS desempeñan funciones exactamente como se les programe y son potencialmente más confiables que los sistemas manuales, previsto que todos los tipos de transacción y todas las condiciones que puedan ocurrir se anticipen e incorporen en el sistema. Por otra parte, un programa de computadora que no esté correctamente programado y probado puede procesar en forma consistente transacciones u otros datos en forma errónea.

   b. *Procedimientos de control programados*— la naturaleza del procesamiento por computadora permite el diseño de procedimientos de control interno en los programas de computadora. Estos procedimientos pueden ser diseñados para proporcionar controles con visibilidad limitada (por ej., se puede dar protección de datos contra acceso no autorizado mediante el uso de palabras clave.) Pueden diseñarse otros procedimientos para uso con intervención manual, tales como la revisión de informes impresos para reportar excepciones y errores, y verificaciones de razonabilidad y limites de los datos.

   c. *Actualización sencilla de una :transacción en archivos múltiples o de base de datos*— una entrada sencilla al sistema de contabilidad puede automáticamente actualizar todos los registros asociados con la transacción (por ej., los documentos de embarque de mercancías pueden actualizar las ventas y los archivos de cuentas por cobrar a clientes, así como el archivo de inventario). Así, una entrada equivocada en dicho sistema puede crear errores en diversas cuentas financieras.

   d. *Transacciones generadas por sistemas*— ciertas transacciones pueden iniciarse por el sistema de CIS mismo sin necesidad de un documento de entrada. La autorización de dichas transacciones puede no ser evidenciada con documentos de entrada visibles ni documentada en las misma forma que las transacciones que se inician fuera del sistema de CIS (por ej., el interés puede ser calculado y cargado automáticamente a los saldos de cuentas de clientes con base en términos previamente autorizados contenidos en un programa de computadora).

   e. *Vulnerabilidad de datos y ,medios de almacenamiento de programas*— grandes volúmenes de datos y los programas de computadora usados para procesar dichos datos pueden almacenarse en medios de almacenamiento portátil o fijo**,** como discos y cintas magnéticos. Estos medios son vulnerables al robo, pérdida, o destrucción intencional o accidental.

Controles internos en un entorno de CIS

5. Los controles internos sobre el procesamiento por computadora, que ayudan a lograr los objetivos globales del control interno, incluyen tanto procedimientos manuales como procedimientos integrados en programas de computadora. Dichos procedimientos de control manuales y por computadora comprenden los controles globales que afectan al entorno de CIS (controles generales de CIS) y los controles específicos sobre las aplicaciones contables (controles de aplicación de CIS).

Controles generales de CIS

6. El propósito de los controles generales de CIS es establecer un marco de referencia de control global sobre las actividades de CIS y proporcionar un nivel razonable de certeza de que se logran los objetivos globales del control interno. Los controles generales de CIS pueden incluir:

   a. *Controles de organización y administración—diseñados* para establecer un marco de referencia organizacional sobre las actividades de CIS, incluyendo:

      ? Políticas *y* procedimientos relativos a funciones de control.

      ? Segregación apropiada de funciones incompatibles (por ej., preparación de transacciones de entrada, programación y operaciones de computadora).

   b. *Desarrollo de sistemas de aplicación y controles de mantenimiento*— diseñados para proporcionar certeza razonable de que los sistemas se desarrollan y mantienen de manera eficiente y autorizada. También están diseñados típicamente para establecer control sobre:

      ? Pruebas, conversión, implementación y documentación de sistemas nuevos o revisados.

      ? Cambios a sistemas de aplicación.

      ? Acceso a documentación de sistemas.

      ? Adquisición de sistemas de aplicación con terceros.

   c. *Controles de operación de computadoras*— diseñados para controlar la operación de los sistemas y proporcionar certeza razonable de que:

      ? Los sistemas son usados para propósitos autorizados únicamente.

      ? El acceso a las operaciones de la computadora es restringido a personal autorizado.

      ? Sólo se usan programas autorizados.

      ? Los errores de procesamiento son detectados y corregidos.

   d. *Controles del software de sistemas*— diseñados para proporcionar razonable certeza de que el software del sistema se adquiere o desarrolla de manera autorizada y eficiente, incluyendo:

- ? Autorización, aprobación, pruebas, implementación y documentación de software de sistemas nuevos y modificaciones del software de sistemas.
- ? Restricción de acceso a software y documentación de sistemas al personal autorizado.

e. *Controles de entrada de datos y de programas*— diseñados para proporcionar razonable certeza de que:

- ? Hay establecida una estructura de autorización sobre las transacciones que se alimentan al sistema.
- ? El acceso a datos y programas está restringido a personal autorizado.

7. Hay otras salvaguardas de CIS que contribuyen a la continuidad del procesamiento de CIS. Estas pueden incluir:

- ? Respaldo de datos y programas de computadora en otro sitio.
- ? Procedimientos de recuperación para usarse en caso de robo, pérdida o destrucción intencional o accidental.
- ? Provisión para procesamiento externo en caso de desastre. Controles de aplicación de CIS

Controles de aplicación de CIS

8. El propósito de los controles de aplicación de CIS es establecer procedimientos específicos de control sobre las aplicaciones contables para proporcionar razonable certeza de que todas las transacciones están autorizadas y registradas, y son procesadas completamente, con exactitud y con oportunidad. Los controles de aplicación de CIS incluyen:

A. ***Controles sobre datos de entrada—*** diseñados para proporcionar razonable certeza de que:

- ? Las transacciones son autorizadas en forma apropiada antes de ser procesadas por la computadora.
- ? Las transacciones son convertidas con exactitud a una forma legible por máquina y registradas en los archivos de datos de la computadora.
- ? Las transacciones no están perdidas, añadidas, duplicadas o cambiadas en forma impropia.
- ? Las transacciones incorrectas son rechazadas, corregidas y, si es necesario, vueltas a someter oportunamente.

B. ***Controles sobre el procesamiento y sobre archivos de datos de la computadora***—diseñados para proporcionar razonable certeza de que:

? Las transacciones, incluyendo las transacciones generadas por el sistema, son procesadas en forma apropiada por la computadora.

? Las transacciones no están perdidas, añadidas, duplicadas o cambiadas en forma no apropiada.

? Los errores de procesamiento son identificados y corregidos oportunamente**.**

C. ***Controles sobre los datos de salida***— diseñados para proporcionar razonable certeza de que:

? Los resultados del procesamiento son exactos.

? El acceso a los datos de salida está restringido a personal autorizado.

? Los datos de salida se proporcionan al personal autorizado apropiado oportunamente.

Revisión de controles de aplicación de CIS

9. Los controles generales de CIS que el auditor puede desear probar se describen en el párrafo 6. El auditor deberá considerar cómo estos controles generales de CIS afectan las aplicaciones de CIS importantes para la auditoría. Los controles generales de CIS que se relacionan a algunas o todas las aplicaciones son controles típicamente interdependientes en cuanto que su operación es a menudo esencial para la efectividad de los controles de aplicación de CIS. Consecuentemente, puede ser más eficiente revisar el diseño de los controles generales antes de revisar los controles de aplicación.

Revisión de controles de aplicación de CIS

10. El control sobre los datos de entrada, procesamiento, archivos de datos y datos de salida puede desempeñarse por personal de CIS, por usuarios del sistema, por un grupo de control separado, o puede ser programado en el software de aplicación. Los controles de aplicación de CIS que el auditor puede desear probar incluyen:

A. ***Controles manuales ejercidos por el usuario***—si los controles manuales ejercidos por el usuario del sistema de aplicación tienen la capacidad de dar una certeza razonable de que los datos de salida del sistema son completos, exactos y autorizados, el auditor puede decidir limitar las pruebas de control a estos controles manuales (por ej., los controles manuales ejercidos por el usuario sobre un sistema computarizado de nóminas para empleados asalariados podría incluir un total anticipado del control de entradas para los pagos brutos, la comprobación de los cálculos de salida de salarios netos, la aprobación de pagos y transferencia de fondos, la comparación con las cifras del registro de nómina, y una rápida conciliación bancaria). En este caso, el auditor puede desear probar sólo los controles manuales ejercidos por el

usuario.

B. ***Controles sobre los datos de salida del sistema***— si, además de los controles manuales ejercidos por el usuario, los controles que deben probarse usan información producida por la computadora o están contenidos dentro de programas de computadora, puede ser posible probar dichos controles examinando los datos de salida del sistema usando técnicas de auditoría ya sea manuales o con ayuda de computadora. Dichos datos de salida pueden ser en forma de medios magnéticos, microfilm o impresos (por ej., el auditor puede probar los controles ejercidos por la entidad sobre la conciliación de totales de reportes con las cuentas de control del libro mayor y puede realizar pruebas manuales de dichas conciliaciones). Alternativamente, cuando la conciliación se realiza por computadora, el auditor puede desear probar la conciliación volviendo a ejecutar el control con el uso de técnicas de auditoría con ayuda de computadora (ver Declaración Internacional de Auditoría "Técnicas de Auditoría con Ayuda de Computadora").

C. ***Procedimientos de control programados***— en el caso de ciertos sistemas por computadora, el auditor puede encontrar que no sea posible o, en algunos casos, no sea práctico probar los controles examinando sólo los controles del usuario o los datos de salida del sistema (por ej., en una aplicación que no da resultados impresos de aprobaciones críticas o violaciones a las políticas normales, el auditor puede querer probar los procedimientos de control contenidos dentro del programa de aplicación). El auditor puede considerar llevar a cabo pruebas de control con el uso de técnicas de auditoría con ayuda de computadora, como prueba de los datos, reprocesamiento de datos de transacciones o, en situaciones inusuales, examinar la codificación del programa de aplicación.

Evaluación

11. Los controles generales de CIS pueden tener un efecto penetrante en el procesamiento de transacciones en los sistemas de aplicación. Si estos controles no son efectivos, puede haber un riesgo de que pudiera ocurrir representaciones erróneas y no ser detectadas en los sistemas de aplicación. Así, las debilidades en los controles generales de CIS pueden imposibilitar la prueba de ciertos controles de aplicación de CIS; sin embargo, los procedimientos manuales ejercidos por los usuarios pueden proporcionar control efectivo al nivel de aplicación.