Ambientes de CIS-Microcomputadoras Independientes

NIA Sección 1001

Normas Internacionales de Auditoría

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: Sección 1001: Ambientes de CIS-Microcomputadoras Independientes***

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

AMBIENTES DE CIS-MICROCOMPUTADORAS INDEPENDIENTES

CONTENIDO

El Comité Internacional de Prácticas de Auditoría ("IAPC") de la Federación Internacional de Contadores emite las declaraciones internacionales de prácticas de auditoría (IAPS) ("Declaraciones") para proporcionar ayuda práctica a los auditores, con el fin de adaptar y usar las Normas Internacionales de Auditoría ("NIAs") o para promover una buena práctica. Las Declaraciones no tienen la autoridad de las NIAs.

Esta Declaración no establece nuevas normas básicas o procedimientos esenciales; su propósito es ayudar a los auditores así como al desarrollo de una buena práctica, proporcionando lineamientos sobre la aplicación de las NIAs cuando se usen microcomputadoras independientes en la producción de información que sea de importancia relativa para los estados financieros de la entidad. El auditor ejerce su juicio profesional para determinar el alcance en que puedan ser apropiados cualquiera de los procedimientos de auditoría descritos en esta Declaración, a la luz de los requerimientos de las NIAs y de las circunstancias particulares de la entidad.

El auditor comprende y considera las características de un ambiente de sistema de información de cómputo (tecnología de la información) porque afectan al diseño de sistema de contabilidad y los controles internos relacionado. Consecuentemente, un ambiente de CIS (Tecnología de la información) de aquí en adelante puede afectar al plan general de auditoría, incluyendo la selección de los controles internos en que el auditor tiene la intención de apoyarse y la naturaleza, oportunidad y alcance de los procedimientos de auditoría.

El AICPA (Instituto Americano de Contadores Públicos Certificados) aprobó esta Declaración internacional de prácticas de auditoría en junio de 2001 para su publicación en julio de 2001.

La Perspectiva del Sector Público (PSP Public Sector Perspective), emitida por el Comité del Sector Público de la Federación Internacional de Contadores, se expone al final de una IAPS.(Declaración internacional de prácticas de auditoría) Cuando no se añade PSP la Declaración aplica, respecto de todo lo importante, al sector público.

Introducción

1. Esta Declaración describe los efectos que tienen las microcomputadoras independientes sobre el sistema de contabilidad y controles internos relacionados y sobre los procedimientos de auditoria.

Microcomputadoras independientes

2. Las microcomputadoras pueden ser usadas para procesar transacciones contables y producir informes que son esenciales para la preparación de estados financieros. La microcomputadora puede constituir todo el sistema de contabilidad basado en computadoras, o solamente una parte del mismo.

3. Generalmente, los ambientes de CIS en los que se usan las microcomputadoras son de algún modo diferentes de otros ambientes de CIS. Ciertos controles y medidas de seguridad que se usan para sistemas grandes de computación pueden no ser factibles para las microcomputadoras. En contraste, se hacen más importantes ciertos tipos de controles internos debido a las características de las microcomputadoras y a los ambientes en que se usan.

4. Las computadoras independientes pueden ser operadas por uno o muchos usuarios en movimientos distintos, accediendo al mismo o a diferentes programas en la misma máquina. El usuario de una computadora independiente que procesa aplicaciones de contabilidad realiza muchas funciones (por ejemplo ingresa datos y opera aplicaciones de programas). Aunque típicamente sin conocimientos de programación, los usuarios a menudo pueden utilizar paquetes de software (programas) de terceros o tomados de la biblioteca de programas o paquetes, tales como hojas de cálculo o aplicaciones de bases de datos.

5. La estructura organizacional dentro de la que una microcomputadora independiente se usa es importante para evaluar riesgos y el alcance de los controles requeridos para aminorar dichos riesgos. Por ejemplo, los controles de vigilancia o monitoreo empleados por la administración pueden ser los únicos efectivos para un paquete de software comprado y que usa un negocio pequeño en una microcomputadora independiente, aparte de cualquier tipo de control que se incorpore en el paquete mismo. En contraste, la efectividad de los controles relacionados con una microcomputadora independiente usada dentro de una organización mayor puede depender de una estructura organizacional que claramente segrega responsabilidades y restringe el uso de las microcomputadoras independientes para funciones específicas.

6. Las consideraciones de control y las características del hardware (equipo físico de cómputo) y del software (programas y sistema de programación) son diferentes cuando se enlaza una microcomputadora a otras computadoras. Estas situaciones a menudo llevan a aumento de riesgos. Esta Declaración no se refiere a la consideración del auditor de la seguridad y controles de una red. Sin

embargo, esta Declaración es relevante para microcomputadoras enlazadas con otra computadora, las cuales también pueden usarse como estaciones de trabajo independientes. Muchas microcomputadoras utilizan en forma intercambiable como parte de una red o de modo independiente. Cuando se refiere a estas microcomputadoras, el auditor considera los riesgos adicionales que se encuentran por el acceso mediante una red así como los lineamientos en esta Declaración.

Control interno en ambientes de microcomputadoras independientes

7. Las microcomputadoras están orientadas a usuarios finales individuales. El grado de precisión y confiabilidad de la información financiera que producen dependerá, en parte, de los controles internos que el usuario adopte, ya sea por voluntad o porque la administración los ha prescrito. Los procedimientos de control establecidos se relacionan con la complejidad del entorno del negocio en que opera la microcomputadora. Normalmente, el ambiente de microcomputadoras independientes es menos estructurado que un ambiente de CIS controlado en forma central. En el primero, los usuarios con sólo habilidades básicas de procesamiento de datos pueden adoptar y poner en marcha los programas de aplicación en forma relativamente rápida, haciendo surgir asuntos tales como lo adecuado de la documentación de sistemas o los procedimientos de control del acceso. Dichos usuarios pueden no considerar como importantes o como de costo efectivo los controles sobre el proceso de desarrollo de la aplicación (por ejemplo, documentación adecuada) y las operaciones (por ejemplo, procedimientos de control de acceso). En tales circunstancias, como la información financiera se procesa en una computadora, los usuarios pueden tender a depositar una confianza injustificada en la misma.

8. En un ambiente típico de microcomputadoras independientes, el nivel de controles generales es más bajo del que se encontraría en un ambiente de computación a mayor escala. No obstante, los procedimientos selectos de seguridad y control pueden ayudar a mejorar el nivel general de control interno.

Políticas organizacionales y procedimientos

9. Como parte de haber obtenido una comprensión del ambiente de control, y por tanto del ambiente de CIS para microcomputadoras independientes, el auditor considera la estructura organizacional de la entidad y, en particular, la asignación de responsabilidades para el procesamiento de datos. Las políticas y procedimientos efectivos para la adquisición, desarrollo, operación y mantenimiento de microcomputadoras independientes pueden enriquecer el ambiente general de control. La falta de desarrollo de dichas políticas puede llevar a que la entidad use programas obsoletos y a errores en los datos así como de la información derivada de los mismos, lo cual puede llevar al incremento del riesgo de fraude. Dichas políticas y procedimientos incluyen lo siguiente:

- ? estándares de adquisición, desarrollo y documentación;
- ? entrenamiento del usuario;
- ? lineamientos de seguridad, respaldos y almacenamiento;
- ? administración de contraseñas (password);
- ? políticas de uso personal;
- ? estándares de adquisición y uso de software;
- ? estándares de protección de datos;
- ? mantenimiento de programas y soporte técnico;
- ? un nivel apropiado de segregación de funciones y responsabilidades; y
- ? protección contra virus.

Protección física—equipo

10. Debido a sus características físicas, las microcomputadoras independientes y sus medios de almacenamiento son susceptibles a robo, daño físico, acceso no autorizado o mal uso. Pueden protegerse físicamente de la manera siguiente:

    - ? cerrándolas bajo llave en un cuarto, gabinete o estuche de protección;
    - ? usando un sistema de alarma que se active si la microcomputadora es desconectada o movida de su lugar;
    - ? asegurando la microcomputadora a una mesa;
    - ? con políticas que expongan los procedimientos apropiados a seguir al salir de viaje con una computadora portátil “laptop” o al usarla fuera de las instalaciones;
    - ? usando la criptografía para archivos clave;
    - ? instalando un mecanismo de seguridad para controlar el interruptor de encendido/apagado. Esto quizá no prevenga el robo de la microcomputadora, pero puede ser efectivo para controlar el uso no autorizado; y
    - ? desarrollando controles ambientales para prevenir daños por desastres

naturales, como incendio, inundación, etcétera.

Protección física - medios removibles y no removibles

11. Los programas y datos de las microcomputadoras pueden almacenarse en medios de almacenamiento removibles o no removibles. Por ejemplo, los disquetes y CDs pueden removerse físicamente de la microcomputadora independiente, mientras que los discos duros normalmente están integrados en la microcomputadora o en una unidad independiente anexa a la misma. Además, los componentes interiores (incluyendo el hard drive "disco duro") de muchas microcomputadoras, en particular laptops, son fácilmente accesibles. Cuando muchos individuos usan una microcomputadora particular es más probable que los medios de almacenamiento se extravíen, se alteren sin autorización o se destruyan.

12. Es responsabilidad del usuario proteger los medios de almacenamiento removibles, por ejemplo, manteniendo respaldos actualizados de dichos medios en un contenedor a prueba de incendio, ya sea en el lugar de trabajo, fuera de él o en ambos. Esto aplica igualmente a los sistemas operativos, programas de aplicación y datos.

Seguridad de programas y datos

13. Cuando muchos usuarios pueden acceder a las microcomputadoras hay un riesgo de que el sistema operativo, los programas y los datos puedan ser alterados sin autorización, o que los usuarios puedan instalar sus propias versiones de programas dando pie a responsabilidades potenciales sobre autorización del software.

14. El grado de características de control y seguridad presentes en un sistema operativo de microcomputadora varía. Aunque algunos sistemas operativos contienen características de seguridad sofisticadas selladas, los utilizados en microcomputadoras independientes generalmente no las tienen. Sin embargo, hay técnicas para ayudar a asegurar que los datos que se procesen y lean sean autorizados, aminorando la destrucción accidental de éstos. Las siguientes técnicas pueden limitar sólo a la personal autorizado el acceso a programas y datos:

    ? uso de contraseñas-password;

    ? desarrollar un paquete de control de acceso;

    ? usar medios de almacenamiento removibles;

    ? usar directorios y archivos ocultos; y

? usar la criptografía.

15. Una técnica efectiva de control es usar perfiles y contraseñas que controlen el nivel de acceso concedido a un usuario. Por ejemplo, se puede dar a un usuario un perfil protegido por una contraseña que permita sólo la alimentación de datos, y puede configurarse una microcomputadora independiente para que requiera una contraseña antes de ser "saqueada".

16. En algunos casos, un paquete de control de acceso puede proporcionar control efectivo sobre el acceso y uso de sistemas operativos, programas y datos. Por ejemplo, sólo un usuario específico puede tener acceso al archivo de contraseñas o permitírsele instalar programas. Dichos paquetes pueden también, en forma regular, examinar los programas en la microcomputadora para detectar si se están usando programas o versiones de éstos no autorizados.

17. El uso de medios de almacenamiento removibles para programas y datos críticos y sensibles puede proporcionar una mayor protección, al mantenerse fuera de línea y bajo control independiente hasta ser requeridos. Por ejemplo, los datos sobre salarios en un sistema de nóminas pueden mantenerse fuera de línea y usarse sólo cuando se requiera para el procesamiento de nóminas.

18. Remover los programas y datos de las microcomputadoras con medios de almacenamiento removibles (por ejemplo, disquetes, CDs y cartuchos) es un manera efectiva de mantenerlos seguros. Los medios se colocan después bajo custodia de los bibliotecarios de archivos o de los usuarios responsables de los datos o programas.

19. La criptografía o cifrado es una técnica que generalmente se utiliza cuando se transmiten datos sensibles por las líneas de comunicación, pero puede también usarse en datos almacenados en una microcomputadora independiente.

Continuidad de operaciones

20. En un ambiente de microcomputadoras, la administración se apoya típicamente en el usuario para asegurar la disponibilidad continua de los sistemas en caso de una falla, pérdida o destrucción del equipo, sistema operativo, programas o datos.

    Esto implicará que:

    (a) el usuario retenga copias del sistema operativo, programas y datos; cuando menos una almacenada en un lugar seguro, lejos de la microcomputadora; y

    (b) esté disponible el acceso aun equipo alterno dentro de un tiempo razonable, dado el uso e importancia del sistema fundamental.

El efecto de microcomputadoras independientes sobre el sistema de contabilidad y los controles internos relacionados

21. El efecto de las microcomputadoras sobre el sistema de contabilidad y los riesgos asociados generalmente dependerá de:

    (a) el grado en que se use la microcomputadora para procesar aplicaciones contables;

    (b) el tipo e importancia de las transacciones financieras que se procesen; y

    (c) la naturaleza de los programas y datos usados en las aplicaciones.

22. A continuación un resumen de algunas de las consideraciones clave y sus efectos, se presenta tanto sobre los controles generales como sobre los de aplicación.

Controles generales -segregación defunciones

23. En un ambiente de microcomputadoras, los usuarios generalmente pueden desempeñar dos o más de las siguientes funciones en el sistema de contabilidad:

    (a) iniciar, documentos fuente;

    (b) autorizar documentos fuente;

    (c) alimentar datos al sistema;

    (d) procesar datos que se han alimentado;

    (e) cambiar programas y datos;

    (O usar o distribuir datos de salida; y

    (g) modificar los sistemas operativos.

24. En otros ambientes de CIS, estas funciones normalmente se segregarían mediante controles generales apropiados. Esta falta de segregación de funciones en un ambiente de microcomputadoras puede permitir que se dejen de detectar los errores, permitiendo que se cometa y oculte el fraude.

Controles de aplicación

25. La existencia y uso de controles apropiados de acceso sobre los programas y datos, combinados con controles sobre la alimentación, procesamiento y salida de datos pueden, en coordinación con las políticas de administración, compensar

algunas de las debilidades en los controles generales en ambientes de microcomputadoras. Los controles efectivos incluyen lo siguiente:

? procedimientos de control programados, como verificaciones de límites;

? un sistema de registro de transacciones y contrapartidas de lotes, incluyendo seguimiento y resolución de cualquier excepción;

? supervisión directa, por ejemplo, una revisión de informes; y

? conciliación de recuentos de registros o cifras de control.

26. El control puede establecerse por una función independiente que normalmente:

(a) recibe todos los datos para procesamiento;

(b) asegura que todos los datos sean autorizados y registrados;

(c) hace un seguimiento de todos los errores detectados durante el procesamiento;

(d) verifica la distribución apropiada de los datos de salida; y

(e) restringe el acceso físico a los programas de aplicación y datos.

Normalmente se requieren controles separados sobre el archivo maestro y datos de transacciones.

El efecto de un ambiente de microcomputadoras independientes sobre los procedimientos de auditoría

27. En un ambiente de microcomputadoras independientes, puede no ser factible o efectivo, desde el punto de vista de costo efectivo para la administración, implementar controles suficientes para reducir a un nivel mínimo los riesgos de errores sin detectar. En esta situación, después de obtener la comprensión del sistema de contabilidad y del ambiente de control requeridos por la NIA 400 “Evaluaciones del Riesgo y Control Interno”, el auditor puede encontrar que es mas efectivo, desde el punto de vista de costo, no hacer una revisión adicional de los controles generales o de los controles de aplicación, sino concentrar los esfuerzos de auditoria en los procedimientos sustantivos. Esto puede implicar un examen físico más amplio y confirmación de los activos, más pruebas de las transacciones, tamaños mayores de muestras así como mayor uso de TAAC (técnicas de auditoria asistidas por computadora).

28. Cuando el nivel de los controles generales parezca adecuado, el auditor puede

decidir adoptar un enfoque diferente. Por ejemplo, una entidad que procesa un gran número de transacciones de ventas en una microcomputadora independiente, puede establecer procedimientos de control que reduzcan el riesgo de control.

29. Las microcomputadoras independientes frecuentemente se encuentran en entidades pequeñas. El IAPS 1005 "Consideraciones especiales en la auditoria de entidades pequeñas", proporciona más lineamientos. Con base en una revisión preliminar de los controles, el plan de auditoria podría incluir someter a prueba los controles en los que el auditor piensa apoyarse.