Ambientes de PED – Microcomputadoras Independientes (Reemplazada)

NIA

Norma Internacional de Auditoría
Sección 1001

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 : Ambientes de PED – Microcomputadoras Independientes. Sección 1001.***

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 de la ***Norma Internacional de Auditoría NIA: Ambientes de PED – Microcomputadoras Independientes****.* ***Sección 1001,*** *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) junto 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.

AMBIENTES DE PED – MICROCOMPUTADORAS INDEPENDIENTES

Esta Declaración Internacional de Auditoría fue aprobada por el Comité Internacional de Prácticas de Auditoría en junio de 1987 para publicación en octubre de 1987.

El auditor deberá entender y considerar las características del ambiente de PED porque afectan al diseño del sistema de contabilidad y los controles internos relacionados, la selección de controles internos en los que tiene la intención de apoyarse, y la naturaleza, oportunidad, y alcance de sus procedimientos.

Esta Declaración se emite como un suplemento a la NIA "Evaluaciones del Riesgo y Control Interno." No forma parte de la NIA o Declaración Internacional de Auditoría "Características y Consideraciones del PED," y no pretende tener la autoridad de una NIA.

Esta Declaración forma parte de una serie que tiene la intención de ayudar al auditor a implementar la NIA y la Declaración antes mencionadas al describir diversos ambientes de PED y su efecto sobre el sistema de contabilidad y controles internos relacionados y sobre las procedimientos de auditoría.

Introducción

1. El propósito de esta Declaración es ayudar al auditor a implementar la NIA "Evaluación del Riesgo y Control Interno," y la Declaración Internacional sobre Auditoría "Características y Consideraciones del PED," al describir los sistemas de microcomputadoras usadas como estaciones de trabajo independientes. La Declaración describe los efectos de la microcomputadora sobre el sistema de contabilidad y controles internos relacionados y sobre los procedimientos de auditoría.

Sistemas de microcomputadoras

2. Las microcomputadoras, a menudo mencionadas como "computadoras personales" o "PCs," son computadoras integrales de uso general, económicas pero poderosas, las cuales consisten típicamente de un procesador, memoria, monitor de video, unidad de almacenamiento de datos, teclado y conexiones para una impresora y comunicaciones. Los programas y los datos son almacenados en medios de almacenamiento removibles o no removibles.

3. 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 computadora o solamente una parte del mismo.

4. Generalmente, los ambientes de PED en los que las microcomputadoras se usan son diferentes de otros ambientes de PED. Ciertos controles y medidas de seguridad que se usan para grandes sistemas de computación pueden no ser factibles para las microcomputadoras. Por otra parte, ciertos tipos de controles internos necesitan enfatizarse debido a las características de las microcomputadoras y a los ambientes en que se usan.

Configuraciones de microcomputadoras.

5. Una microcomputadora puede usarse en diversas configuraciones. Estas incluyen:

   ? una estación de trabajo independiente operada por un solo usuario o un número de usuarios en diferentes momentos:

   ? una estación de trabajo que es parte de una red de microcomputadoras de un área local; y

   ? una estación de trabajo conectada a una computadora central.

6. La estación de trabajo independiente puede ser operada por un solo usuario o un número de usuarios en diferentes momentos teniendo acceso a los mismos o diferentes programas. Los programas y datos se almacenan en la microcomputadora o muy cerca de ella y, generalmente, los datos se alimentan manualmente por medio del teclado. El usuario de la estación independiente que procesa aplicaciones contables puede ser conocedor de programación, y típicamente desempeña un número de funciones, (por ej., alimentar datos, operar programas de aplicación y, en algunos casos, escribir los programas de computadora en si'). Esta programación puede incluir el uso de paquetes de software de terceras partes para desarrollar hojas electrónicas de cálculo o aplicaciones de base de datos.

7. Una red de área local es una instalación donde dos o más microcomputadoras están enlazadas a través del uso de software especial y de líneas de comunicación. Típicamente, una de las microcomputadoras actuará como el dispensador de archivos que maneja la red. Una red de área local permite compartir recursos como instalaciones de almacenaje e impresoras. Múltiples usuarios, por ejemplo, pueden tener acceso a la información, datos y programas almacenados en archivos compartidos. Una red de área local puede conocerse como un sistema distribuido.

8. Las microcomputadoras pueden enlazarse a computadoras centrales y usarse como parte de dichos sistemas, por ejemplo, como una estación inteligente en línea o como parte de un sistema de contabilidad distribuido. A un arreglo así puede llamársele un sistema en línea. Una microcomputadora puede actuar coma una terminal inteligente a causa de su lógica, transmisión, almacenaje y capacidades básicas de cómputo.

9. Ya que las consideraciones de control y las características del hardware y software son diferentes cuando una microcomputadora está enlazada a otras computadoras,

tales ambientes se describen en otros Suplementos a la NIA 6. Sin embargo, al grado que una microcomputadora que está enlazada a otra computadora pueda también ser usada como una estación independiente, la información en esta Declaración es de importancia.

Características de las microcomputadoras

10. Aunque las microcomputadoras proporcionan al usuario capacidades de cómputo importantes, son suficientemente pequeñas para transportarse, son relativamente poco costosas, y pueden ponerse en operación rápidamente. Los usuarios con habilidades básicas en computadoras pueden aprender a operar una microcomputadora fácilmente ya que mucho del software de sistemas operativas y muchos programas de aplicación son "amigables con el usuario" y contienen instrucciones paso a paso. Otra característica es que el software del sistema operativo, que generalmente se surte por el fabricante de la microcomputadora, es menos integral que el que se encuentra en los ambientes de computadoras mayores; por ej., puede no contener tantas características de control y seguridad, como los controles de palabras clave.

11. El software para un amplio rango de aplicaciones de la microcomputadora puede comprarse de proveedores distintos para su uso (por ej., contabilidad de libro mayor, contabilidad de cuentas por pagar, y control de producción y de inventario). Estos paquetes de software son usados típicamente sin modificación de los programas. Los usuarios pueden también desarrollar otras aplicaciones con el uso de paquetes de software genérico, como hojas de cálculo electrónicas, o bases de datos, compradas a vendedores distintos.

12. El software del sistema operativo, los programas de aplicación y datos, pueden ser almacenados en, y recuperados de medios de almacenamiento removibles, incluyendo diskettes, cartuchos y discos duros removibles. Estos medios de almacenamiento, debido a su tamaño pequeño y a que son portátiles, están sujetos a borrarse accidentalmente, a daños físicos, a pérdidas o robo, particularmente por personas no familiarizadas con dichos medios o por usuarios no autorizados. El software, los programas y datos también pueden ser almacenados en discos duros que no son removibles.

Control interno en ambientes de microcomputadoras

13. Generalmente, el ambiente de PED en el que se usan microcomputadoras es menos estructurado que un ambiente de PED controlado en forma central. En el primero, los programas de aplicación pueden desarrollarse relativamente rápido por usuarios que poseen sólo habilidades básicas de procesamiento de datos. En dichos casos, los controles sobre el proceso de desarrollo de sistemas (p. ej., procedimientos de control de acceso), que son esenciales para el control efectivo de un ambiente mayor de computadoras, pueden no ser considerados por el que los desarrolla, el usuario o la administración, como importantes o como de costo efectivo en un

ambiente de microcomputadoras. Sin embargo, a causa de que los datos están siendo procesados en una computadora, los usuarios de dichos datos pueden tender a depositar una confianza no justificada en la información financiera almacenada o generada por una microcomputadora. Ya que las microcomputadoras están orientadas a usuarios finales individuales, el grado de exactitud y seguridad de la información financiera producida dependerá de los controles internos fijados por la administración y adoptados por el usuario. Por ejemplo, cuando hay varios usuarios de una sola microcomputadora, sin controles apropiados, los programas y datos almacenados en medios de almacenamiento no removibles por un usuario pueden ser susceptibles al acceso, uso o alteración no autorizados, o a robo, por otros usuarios.

14. En un ambiente típico de microcomputadoras, no puede ser claramente asegurada la distinción entre controles generales de PED y controles de aplicación de PED. Los párrafos 15-32 describen procedimientos de control y seguridad que pueden ayudar a mejorar el nivel global del control interno.

Autorización de la administración para operación de microcomputadoras

15. La administración puede contribuir a la operación efectiva de microcomputadoras independientes fijando y ejecutando políticas para su control y uso. La declaración de políticas de la administración puede incluir:

- ? responsabilidades de la administración;
- ? instrucciones sobre el uso de las microcomputadoras;
- ? requisitos de entrenamiento;
- ? autorización para el acceso a programas y datos;
- ? políticas para prevenir el copiado no autorizado de programas y datos;
- ? requisitos de seguridad, respaldo y almacenamiento;
- ? desarrollo de aplicaciones y normas de documentación;
- ? normas para formato de informes y controles para distribución de informes;
- ? políticas sobre uso personal;
- ? normas de integridad de datos;
- ? responsabilidad por los programas, datos y corrección de errores y
- ? segregación apropiada de funciones.

Seguridad física — equipo

16. A causa de sus características físicas, las microcomputadoras son susceptibles de robo, daño físico, acceso no autorizado, o mal uso. Esto puede resultar en la pérdida de información almacenada en la microcomputadora, por ejemplo, datos financieros

vitales para el sistema de contabilidad.

17. Un método de seguridad física es restringir el acceso a las microcomputadoras cuando no están en uso, por medio de cerraduras en las puertas u otra protección de seguridad durante las horas no hábiles. La seguridad física adicional para las microcomputadoras puede establecerse, por ejemplo:

    ? guardando bajo llave la microcomputadora en un gabinete o estuche;

    ? usando un sistema de alarma que se active cada vez que la microcomputadora sea desconectada o movida de su lugar;

    ? fijando la microcomputadora a una mesa; o

    ? instalando un mecanismo de cierre para controlar el acceso al botón de encendido/apagado. Esto puede no prevenir el robo de la microcomputadora, pero puede ser efectivo para controlar el uso no autorizado.

Seguridad física — medios removibles y no removibles

18. Los programas y datos usados en una microcomputadora pueden ser almacenados en medios de almacenamiento removibles o no removibles. Los diskettes y cartuchos pueden ser removidos físicamente de la microcomputadora, mientras que los discos duros normalmente están sellados en la microcomputadora o en una unidad independiente anexa a la microcomputadora. Cuando se usa una microcomputadora por muchos individuos, los usuarios pueden desarrollar una actitud despreocupada sobre el almacenamiento de los diskettes o cartuchos de aplicación por los que son responsables. Como resultado, diskettes o cartuchos muy importantes pueden ser mal colocados, alterados sin autorización o destruidos.

19. El control sobre los medios removibles puede establecerse poniendo la responsabilidad por dichos medios en personal cuyas responsabilidades incluyen funciones de custodios de software o de bibliotecarios. El control puede reforzase más cuando se usa un sistema de verificación de entradas y salidas de archivos de programas y datos y se cierran con llave los lugares de almacenamiento. Dichos controles internos ayudan a asegurar que los medios de almacenamiento removibles no se pierdan, se desubiquen o se den a personal no autorizado. El control físico sobre medios de almacenamiento no removibles probablemente se establezca mejor mediante aditamentos de cerraduras de seguridad.

20. Dependiendo de la naturaleza de los archivos de programas y de datos, es apropiado conservar copias vigentes de diskettes, cartuchos y discos duros en un contenedor a prueba de fuego, ya sea en el local, fuera de él, o ambos. Esto aplica igualmente a software del sistema operativo y de utilería, y a copias de respaldo de discos duros.

Seguridad de programas y de datos

21. Cuando las microcomputadoras están accesibles a muchos usuarios, hay un riesgo de que los programas y datos puedan ser alterados sin autorización.

22. Ya que el software del sistema operativo de la microcomputadora puede no contener muchas características de control y seguridad, hay diversas técnicas de control interno que pueden integrarse a los programas de aplicación para ayudar a asegurar que los datos son procesados y leídos según se autorice, y que se previene la destrucción accidental de datos. Estas técnicas, que limitan el acceso a programas y datos sólo a personal autorizado, incluyen:

    ? separar datos en archivos organizados bajo directorios de archivos separados;

    ? usar archivos ocultos y nombres secretos de archivos;

    ? emplear palabras clave; y

    ? usar criptografía.

23. El uso de un directorio de archivos permite al usuario segregar información en medios removibles y no removibles. Para información critica y sensitiva, esta técnica puede suplementarse asignando nombres secretos de archivos y "ocultando" los archivos.

24. Cuando se usan las microcomputadoras por muchos usuarios, una técnica efectiva de control interno es el uso de palabras clave, que determinan el grado de acceso concedido a un usuario. La palabra clave se asigna y monitorea por un empleado que es independiente del sistema especifico al que se aplica la palabra clave. El software para palabras clave puede ser desarrollado por la entidad, pero en la mayoría de los casos se compra. En cualquiera de los dos casos, los controles internos pueden reforzarse instalando software que tenga una baja probabilidad de ser sobrepasado por los usuarios.

25. La criptografía puede dar un control efectivo para proteger programas e información confidenciales o sensitivos del acceso no autorizado y de modificación por parte de los usuarios. Generalmente es usada cuando se transmiten datos sensitivos por las líneas de comunicación, pero también puede usarse en información procesada por una microcomputadora. La criptografía es el proceso de transformar programas e información a una forma ininteligible. El cifrado y descifrado criptográfico de datos requiere el uso de programas especiales y una clave de código conocidos sólo a aquellos usuarios para quienes es la información restringida.

26. Los directorios y archivos ocultos, el software de autenticación de usuarios y la criptografía pueden ser usados para microcomputadoras que tienen medios de almacenamiento tanto removibles como no removibles. Para las microcomputadoras que tienen medios de almacenamiento removibles, un medio efectivo de seguridad para programas y datos es remover los diskettes y cartuchos de la microcomputadora y colocarlos bajo custodia de los usuarios responsables por los datos o de los bibliotecarios de archivos.

27. Un control adicional de acceso para información confidencial o sensitiva al-

macenada en medios de almacenamiento no removibles es copiar la información a un diskette o cartucho y borrar los archivos en los medios de almacenamiento no removibles. El control sobre el diskette o cartucho puede establecerse entonces en la misma manera que para otros datos sensitivos o confidenciales almacenados en diskettes o cartuchos. El usuario deberá tener presente que muchos programas en software incluyen una función de "borrar" o "suprimir", pero que dicha función quizá realmente no limpie los archivos borrados o suprimidos del disco duro. Dichas funciones pueden simplemente limpiar el nombre del archivo del directorio del disco duro. Los programas y datos son quitados de hecho del disco duro sólo cuando se escriben nuevos datos sobre los viejos archivos o cuando programas especiales de utilería se usan para limpiar los archivos.

Integridad del software y de los datos

28. Las microcomputadoras están orientadas a usuarios finales para el desarrollo de programas de aplicación, alimentación y procesamiento de datos y generación de informes. El grado de exactitud y confiabilidad de la información financiera producida dependerá de los controles internos instituidos por la administración y adoptados por los usuarios, así como de controles incluidos en los programas de aplicación. Los controles de integridad del software y de los datos puede asegurar que la información procesada está libre de errores y que el software no sea susceptible de manipulación no autorizada (por ej., que los datos autorizados sean procesados en la manera instituida).

29. La integridad de los datos puede reforzarse incorporando procedimientos de control interno como un formato y verificaciones en línea y verificaciones cruzadas de los resultados. Una revisión del software comprado puede determinar si contiene recursos apropiados para verificación y detección de errores. Para software desarrollado para usuarios, incluyendo plantillas electrónicas de hojas de cálculo y aplicaciones de bases de datos, la administración puede especificar por escrito los procedimientos para desarrollar y poner a prueba los programas de aplicación. Para ciertas aplicaciones criticas, puede esperarse que la persona que procesa los datos, demuestre que se usaron datos apropiados y que los cálculos y otras operaciones de manejo de datos se llevaron a cabo apropiadamente. El usuario final podría usar esta información para validar los resultados de la aplicación.

30. La documentación adecuada por escrito de las aplicaciones que son procesadas en la microcomputadora puede reforzar aun más los controles sobre la integridad del software y los datos. Dicha documentación puede incluir instrucciones paso a paso, una descripción de informes preparados, fuente de los datos procesados. una descripción de informes individuales, archivos y otras especificaciones, como cálculos.

31. Si la misma aplicación contable se usa en varias localidades, la integridad y consistencia del software de aplicaciones puede mejorarse cuando los programas de aplicación se desarrollan y se mantienen en un lugar y no por cada usuario disperso por toda una entidad.

Respaldo del hardware, software y datos

32. El respaldo se refiere a planes hechos por la entidad para obtener acceso a hardware, software, y datos comparables en caso de falla, pérdida o destrucción. En un ambiente de microcomputadoras, los usuarios normalmente son responsables por el procesamiento, incluyendo la identificación de programas y archivos de datos importantes que deben ser copiados periódicamente y almacenados en una localidad lejana de las microcomputadoras. Es particularmente importante establecer procedimientos de respaldo para que lleven a cabo los usuarios regularmente. Los paquetes de software comprados de proveedores distintos generalmente vienen con una copia de respaldo o con provisión para hacer una copia de respaldo.

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

33. El efecto de las microcomputadoras en el sistema de contabilidad y los riesgos asociados generalmente dependerán de:

    ? el grado en el que se esté usando la microcomputadora para procesar aplicaciones contables;

    ? el tipo e importancia de las transacciones financieras que están siendo procesadas; y,

    ? la naturaleza de los archivos y programas utilizados en las aplicaciones.

34. Las características de los sistemas de microcomputadoras, descritas anteriormente en esta Declaración, ilustran algunas de las consideraciones para diseñar procedimientos de control de costo efectivo para microcomputadoras independientes. Abajo se describe un resumen de algunas de las consideraciones clave y sus efectos sobre los controles generales del PED y los controles de aplicación del PED.

Controles generales del PED—segregación de funciones

35. En un ambiente de microcomputadoras, es común para los usuarios poder desempeñar dos o más de las siguientes funciones en el sistema de contabilidad:

    ? iniciar y autorizar documentos fuente;

    ? alimentar datos al sistema;

    ? operar la computadora;

    ? cambiar programas y archivos de datos;

    ? usar o distribuir datos de salida; y

    ? modificar los sistemas operativos.

En otros ambientes PED, dichas funciones se segregarían normalmente por medio de controles generales de PED apropiados. Esta falta de segregación de funciones en un ambiente de microcomputadoras puede:

? permitir que queden errores sin detectar; y

? permitir que se cometa y oculte el fraude.

Controles de Aplicación del PED

36. La existencia y uso de controles apropiados de acceso al software, hardware, y archivos de datos, combinados con controles sobre la entrada, procesamiento y salida de datos pueden, en coordinación con las políticas de la administración, compensar por algunas de las debilidades en los controles generales de PED en ambientes de microcomputadoras. Los controles efectivos pueden incluir:

? un sistema de registros de transacciones y de contrapartidas por lotes;

? supervisión directa; y

? conciliación de recuentos de registros o cifras de control.

El control puede establecerse por una función independiente que normalmente:

? recibiría todos los datos para procesamiento;

? aseguraría que todos los datos sean autorizados y registrados;

? haría un seguimiento de todos los errores detectados durante el procesamiento;

? verificaría la distribución apropiada de los datos de salida; y

? restringiría el acceso físico a los programas de aplicación y archivos de datos.

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

37. En un ambiente de microcomputadoras, puede no ser factible o de costo efectivo para la administración implementar suficientes controles para reducir al mínimo los riesgos de errores no detectados. Así, el auditor puede a menudo asumir que el riesgo de control es alto en dichos sistemas.

38. En esta situación, el auditor puede encontrar que es más efectivo en costo, después de obtener una comprensión del ambiente de control y del flujo de transacciones, no hacer una revisión de controles generales del PED o controles de aplicación del PED, sino concentrar los esfuerzos de auditoría en pruebas sustantivas en o cerca del final del año. Esto puede suponer más examen físico y confirmación de los activos, más pruebas de detalles, tamaños mayores de muestras, y mayor uso de técnicas de auditoría asistidas por computadora, cuando sea apropiado.

39. Las técnicas de auditoría asistidas por computadora pueden incluir el uso de software del cliente (base de datos, hoja electrónica de cálculos, o software de utilería), que ha sido sometido a revisión por el auditor, o el uso de los propios programas de software del auditor. Dicho software puede ser usado por el auditor, por ejemplo, para añadir transacciones o saldos en los archivos de datos para comparación con registros de control o saldos de cuentas del libro mayor, para seleccionar cuentas o transacciones para pruebas de detalles o confirmación o para examinar bases de datos para partidas inusuales.

40. En ciertas circunstancias, sin embargo, el auditor puede decidir tomar un diferente enfoque. Estas circunstancias pueden incluir sistemas de microcomputadoras que procesan un gran número de transacciones cuando sería de costo efectivo desempeñar trabajo de auditoría sobre los datos en una fecha preliminar. 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; el auditor puede decidir, sobre la base de una revisión preliminar de los controles, desarrollar un enfoque de auditoría que incluya pruebas de aquellos controles en los que piensa apoyarse.

41. Los siguientes son ejemplos de procedimientos de control que un auditor puede considerar cuando piensa apoyarse en controles internos de contabilidad relacionados con microcomputadoras independientes:

    a. Segregación de obligaciones y controles de contrapartidas:

        ? Segregación de funciones según se lista en el párrafo 36.

        ? Rotación de obligaciones entre los empleados.

        ? Conciliación de saldos del sistema con cuentas de control del libro mayor.

        ? Revisión periódica por la administración del calendario de procesamiento y de informes que identifican a los individuos que usaron el sistema.

    b. Acceso a la microcomputadora y sus archivos:

        ? Colocación de la microcomputadora a la vista del individuo responsable de controlar el acceso a la misma.

        ? El uso de llaves de seguridad en la computadora y terminales.

        ? El uso de palabras clave para acceso a los programas de la microcomputadora y archivos de datos.

        ? Restricción sobre el uso de programas de utilería.

    c. Uso de software de terceras partes:

        ? Revisión de software de aplicación antes de su compra, incluyendo funciones, capacidad y controles.

        ? Pruebas adecuadas al software y las modificaciones al mismo antes de su uso.

? Evaluación continua de adecuación del software para cumplir con requerimientos del usuario.