TÉCNICAS PARA AUDITORÍA DE

SISTEMAS INFORMÁTICOS

ISBN: 978-9942-14-160-6
Título: Técnicas para Auditoría de Sistemas Informáticos

Autores: Quintana Sánchez, Armando Miguel
Quintanilla Romero, Marco Antonio
Ojeda Escobar, Jorge Aníbal

Editorial: Quintanilla Romero, Marco Antonio

Materia: Educación, investigación, temas relacionados con la tecnología
Publicado: 2016-03-10
NºEdición: 2
Idioma: Español

www.uceinvestigar.com

Técnicas para Auditoría de Sistemas Informáticos

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. ANTECEDENTES

En la actualidad, con los procesos de Globalización, las empresas deben adoptar estándares de integridad, calidad y seguridad de la información para poder ser competitivos. (Moore Stephens Suarez &Menendez)

En su libro de Auditoría de Sistemas(Echenique García, pág. xi) menciona:

> *Las nuevas herramientas con que se cuenta (Internet, Extranet, comunicación, base de datos, multimedia, etc.) hacen que también se pueda tener acceso a mayor información, aunque el costo total de los sistemas, así como la confiabilidad y seguridad con que se debe trabajar, sean muy altos.*
>
> *En algunas ocasiones ha disminuido el costo de las aplicaciones, pero se tiene poca productividad en relación con la información y uso que se da a éstas. También se tiene poco control sobre la utilización de los equipos, existe un deficiente sistema de seguridad tanto física como lógica y se presenta una falta de confidencialidad de la información. Lo que se debe incrementar es la productividad, el control, la seguridad y la confidencialidad, para tener la información necesaria en el tiempo y en el lugar adecuado para tomar las mejores decisiones.*

Es así como, las técnicas de auditoría se han convertido en una de las herramientas más útiles para adelantar pruebas de cumplimiento y sustantivas sobre datos, aplicaciones, equipos y programas. Estas permiten seleccionar y procesar la información necesaria para fines específicos de la auditoria, facilitando la aplicación de métodos de muestreo estadístico, el alcance de las pruebas y la verificación de la integridad de los datos obtenidos en la población auditada.

Las técnicas de auditoría informática permiten a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización.

Para aplicar las técnicas de auditoría, es necesario contar con expertos en las diferentes áreas o funciones de la informática, para que puedan "analizar y dictaminar sobre el estado del control interno del área de sistemas y de los aplicativos computarizados implantados". (Moore Stephens Suarez &Menendez)

Las técnicas de auditoría informática son de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además la evaluación debe abarcar: informática, organización de centros de información, hardware y software.

2. LA AUDITORÍA

2.1. INTRODUCCIÓN

Este manual está diseñado como una guía para aplicar técnicas de auditoría a los Sistemas de Información Basados en Computadora y hardware relacionado con su uso, aplicadas para todos los usuarios de la tecnología de información.

Con el establecimiento de normas y procedimientos se pretende lograr los siguientes beneficios:

- Proteger la información contra acciones indebidas o accidentales.
- Permitir un control adecuado sobre todo el sistema de información.
- Cumplir con los requerimientos mínimos de control.
- Garantizar al usuario el total apoyo y soporte en las actividades realizadas.

2.2. CONCEPTO DE TÉCNICAS DE AUDITORÍA

Las técnicas de auditoría son recursos investigativos que utiliza el auditor para hacer el examen de auditoría y obtener información necesaria para emitir su opinión profesional. **(Eumed.net)**

2.3. CLASES DE TÉCNICAS DE AUDITORÍA

De acuerdo a la información proporcionada en la página web (Eumed.net), el contador para emitir su opinión sobre la auditoría realizada, se ayuda de las siguientes técnicas:

- ***Estudio General***

Apreciación sobre la fisonomía o características generales de la empresa, de sus estados financieros y de los rubros y partidas importantes, significativas o extraordinarias. Esta apreciación se hace aplicando el juicio profesional del contador público que basado en su preparación y experiencia, podrá obtener de los datos e información de la empresa que va

a examinar, situaciones importantes o extraordinarias que pudieran requerir atención especial.

- ***Análisis***

Clasificación y agrupación de los distintos elementos individuales que forman una cuenta o una partida, de tal manera que los grupos constituyan unidades homogéneas y significativas. El análisis generalmente se aplica a cuentas o rubros de los estados financieros para conocer cómo se encuentran integrados y son los siguientes: Análisis de saldos y análisis de movimientos.

- ***Inspección***

Examen físico de los bienes materiales o de los documentos, con el objeto de cerciorarse de la existencia de un activo o de una operación registrada o presentada en los estados financieros.

- ***Confirmación***

Obtención de una comunicación escrita de una persona independiente de la empresa examinada y que se encuentre en posibilidades de conocer la naturaleza y condiciones de la operación y, por lo tanto, confirmar de una manera válida. Esta técnica se aplica solicitando a la empresa auditada que se dirija a la persona a quien se pide la confirmación para que conteste por escrito al auditor, dando la información que se solicita y pueda ser aplicada de diferentes formas: positiva y negativa.

- ***Investigación***

Obtención de información, datos y comentarios de los funcionarios y empleados de la propia empresa. Con esta técnica el auditor puede obtener conocimiento y formarse un juicio sobre algunos saldos y operaciones realizadas por la empresa.

- ***Declaración***

Manifestación por escrito con la firma de los interesados, del resultado de las investigaciones realizadas con los funcionarios y empleados de la empresa. Esta técnica se aplica cuando la importancia de los datos o el resultado de las investigaciones realizadas

lo ameritan. Aun cuando la declaración es una técnica de auditoría conveniente y necesaria, su validez está limitada por el hecho de ser datos suministrados por personas que participaron en las operaciones realizadas o tuvieron injerencia en la formulación de los estados financieros que se están examinando.

- ***Certificación***

Obtención de un documento en el que se asegure la verdad de un hecho, legalizado por lo general con la firma de una autoridad.

- ***Observación***

Presencia física de cómo se realizan ciertas operaciones o hechos. El auditor se cerciora de la forma como se realizan ciertas operaciones, dándose cuenta ocularmente de la forma como el personal de la empresa lo realiza.

- ***Cálculo***

Verificación matemática de alguna partida. Hay partidas en la contabilidad que son resultado de cómputos realizados sobre bases predeterminadas. El auditor puede cerciorarse de la corrección matemática de estas partidas mediante el cálculo independiente de las mismas.

2.4. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a la publicación de las **(ISO/IEC 17799, 2005, pág. 8)** menciona lo siguiente:

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear,

revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

2.5. UBICACIÓN DEL ENTORNO INFORMATICO

La Sección de Informática se encuentra ubicada bajo el Departamento Administrativo y debe ubicarse en el organigrama estructural de la empresa.

Las tres áreas claves de labor son:

Tabla 1 Áreas Claves de Labor

2.6. ESQUEMA GENERAL DE RECURSOS

Tabla 2 Esquema General de Recursos

USUARIOS	APOYO FUNCIONAL	APOYO SOFTWARE	APOYO HADWARE
Requerimientos	Comisión y Especialistas	Paquetes y Programas	Equipos de Computacion
Cartas Documentos Oficios	Comisión Informática y especialistas	Office MQR	IBM COMPAQ Oracle
Gráficos Informes Cálculos Consultas Procesos Aplicaciones especiales	CLONES de la Unidad de Sistemas	Etc.	LAN CR-RW

2.6.1. EXPLICACIÓN DEL ESQUEMA GENERAL DE RECURSOS

COMISIÓN INFORMÁTICA:

La Comisión Informática aprueba la adquisición de hardware y software, cursos de entrenamiento, movilización de equipos, reglamentos, normas, políticas, etc.

ESPECIALISTAS FUNCIONALES:

El grupo de Especialistas Funcionales está compuesto por el personal informático y los usuarios con avanzados conocimientos de DOS, Office, Netware, Windows y otros programas. Este grupo está encargado de brindar asesoría, entrenamiento, asistencia, soporte o ayuda en la utilización de paquetes, programas, equipos, unidades de respaldo (cd-rw, cintas) e impresoras.

2.7. FUNCIONES DE LA SECCIÓN INFORMÁTICA

La principal función es la de asistir a los usuarios en los siguientes puntos:

- Entrenamiento oportuno para el uso del hardware y software.
- Clarificación de problemas de operación.
- Instalación de hardware y software.
- Obtención de respaldos.
- Documentación de aplicaciones.
- Actualización de nuevas técnicas.
- Información de los recursos disponibles en hardware y software.
- Solicitudes de requerimientos, etc.

2.8. PROCEDIMIENTOS PARA USUARIOS Y SISTEMAS

Las políticas y procedimientos son la primera línea de defensa de cualquier ambiente computacional contra: pérdidas, daños, alteración, o hurto de la información, sean éstos provocados o accidentales. La falta de políticas y procedimientos deja a la organización expuesta, sin ninguna base normativa a seguir.

2.9. PROCEDIMIENTOS PARA USUARIOS

En este manual se cubre la mayoría de las posibilidades; sin embargo, en algún momento se puede presentar una situación que no se ha contemplado, para lo cual, el usuario deberá solicitar asistencia.

PROCEDIMIENTO N°1

TITULO:	**Solicitud de entrenamiento en Hardware o Software.**
DIRIGIDO A:	Usuarios de Computadores.
OBJETIVO:	Definir las normas generales para garantizar que las necesidades de entrenamiento solicitadas por usuarios de computadores, sean satisfechas oportunamente por la Sección de Informática.
DESCRIPCIÓN:	Este procedimiento se aplica para situaciones en las que un usuario requiera entrenamiento en el uso de computadores, con el fin de satisfacer y cubrir necesidades dentro de su actividad.
RESPONSABLE:	Usuarios de computadores y Dirección Administrativa.
LIMITACIONES:	Únicamente se dará entrenamiento sobre el hardware y software estandarizado y solo sobre temas relacionados con el trabajo de la persona solicitante.
RESTRICCIONES:	El solicitante no debe haber recibido con anterioridad el entrenamiento que está solicitando.

DESARROLLO:

a) El usuario solicitante de acuerdo a los requerimientos que se presentan por la necesidad de utilizar un computador o un nuevo programa para el desarrollo de sus funciones, deberá elaborar un oficio con copia adjuntando los justificativos del caso.

b) A continuación el usuario solicitante deberá enviar el original a la Sección de Informática. Deberá guardar la copia para su archivo personal.

c) La Sección de INFORMÁTICA recibe el oficio con la solicitud y lo archiva como pendiente, por fecha de solicitud.

d) La Sección de INFORMÁTICA evalúa si amerita el entrenamiento y si está planificado algún entrenamiento a nivel de grupo, relacionado con la solicitud de entrenamiento. Si el entrenamiento no amerita enviará un oficio negando la solicitud del usuario y adjuntando una copia al oficio enviado solicitando el entrenamiento, archivará los documentos.

e) Si el punto anterior es positivo, la Sección de INFORMÁTICA integra al solicitante al grupo, caso contrario, programa un entrenamiento individual, coordinando con el Jefe inmediato del usuario solicitante. Envía un oficio indicando los datos del entrenamiento solicitado y su aceptación por la Sección de INFORMÁTICA a la Dirección Administrativa. Mantiene una copia del oficio junto a la solicitud de entrenamiento.

f) La Dirección Administrativa deberá aprobar o negar finalmente la solicitud y enviar una respuesta mediante un oficio a la Sección de INFORMÁTICA.

g) La Sección de INFORMÁTICA, una vez recibido el oficio de la Dirección Administrativa, lo adjunta al trámite y comunica la decisión al usuario solicitante mediante un oficio que incluirá todos los detalles acerca del entrenamiento. Envía una primera copia al usuario solicitante, una segunda copia la Jefe inmediato y el archiva el original junto a los otros documentos por fecha de respuesta.

h) La Sección de INFORMÁTICA archiva el oficio de solicitud, la respuesta de la Dirección Administrativa, junto con la respuesta final y registra todo como procesado.

i) El usuario solicitante y su Jefe inmediato, reciben la primera y segunda copias del oficio de respuesta y archivan por fecha de respuesta.

PROCEDIMIENTO N°2

TITULO:	**Desarrollo, modificación, instalación y documentación de aplicaciones propias.**
DIRIGIDO A:	Sección de INFORMÁTICA, Jefes de Departamento y Usuarios de computadores.
OBJETIVO:	Definir las normas generales para controlar el desarrollo, modificación, documentación e instalación de aplicaciones específicas realizadas por los usuarios.
DESCRIPCIÓN:	Este procedimiento se aplica cuando un usuario requiera realizar, modificar o instalar una aplicación de computadores desarrollada internamente, con el fin de satisfacer y cubrir necesidades dentro de su actividad.
RESPONSABLE:	Usuarios de computadores, Sección de INFORMÁTICA.
LIMITACIONES:	Únicamente se desarrollarán o modificarán aplicaciones autorizadas previamente por la Sección de INFORMÁTICA mediante un oficio.

RESTRICCIONES: Antes de desarrollar o modificar una aplicación el usuario deberá consultar con su jefe inmediato y con la Sección de INFORMÁTICA, los cuales autorizarán el desarrollo o modificación de esa aplicación. No está permitido desarrollar aplicaciones para uso personal o externo. No está permitido sacar copias de los manuales y de las aplicaciones para uso externo.

DESARROLLO:

a) El usuario solicitante de acuerdo a los requerimientos que se presentan por la necesidad de automatizar su trabajo consultará con su Jefe superior y con la Sección de INFORMÁTICA el desarrollo o modificación de una nueva aplicación y la instalación de la misma. Si la aplicación ha sido ya desarrollada por otro usuario se emitirá un oficio de autorización por parte de la Sección de INFORMÁTICA, se la instalará y termina el procedimiento.

b) A continuación el usuario solicitante en coordinación con la Sección de INFORMÁTICA y con un oficio de aprobación de la misma (original para el usuario y copia para la Sección de INFORMÁTICA) procederá al desarrollo o modificación de la aplicación. Junto con la aplicación deberá desarrollarse o actualizarse un manual descriptivo de la misma y un manual de utilización tipiados en Word u otro procesador de textos.

c) Una vez finalizada la elaboración o modificación de la aplicación la Sección de INFORMÁTICA la instalará para el usuario. La Sección de INFORMÁTICA deberá guardar una copia en un disco externo (con la aplicación y los manuales tipiados en Word u otro procesador de textos) en su biblioteca.

d) La Sección de INFORMÁTICA deberá mantener un inventario actualizado de este tipo de aplicaciones.

PROCEDIMIENTO N°3

TITULO: **Adquisiciones de Equipos, Programas, Suministros, Contratos de Seguro y Mantenimiento.**

DIRIGIDO A: Comisión Informática, Sección de INFORMÁTICA, Jefes de Departamento y Usuarios de computadores.

OBJETIVO: Definir las normas generales para controlar las adquisiciones de equipos, programas, suministros y contratos de seguro y mantenimiento.

DESCRIPCIÓN: Este procedimiento se aplica cuando la Sección de INFORMÁTICA, en conversación con usuarios y jefes de departamento, establezca la necesidad de adquirir programas, equipos, suministros, contratos de seguro y mantenimiento.

RESPONSABLE: Comisión Informática y Sección de INFORMÁTICA.

LIMITACIONES: La compra de equipos y programas; y la contratación de seguro y mantenimiento deberán ser aprobadas por la Comisión de Informática. La adquisición de suministros hasta por un monto que será aprobado por el Jefe de la Sección de Informática.

RESTRICCIONES: Se comprarán preferentemente equipos de marca para mantener el estándar en hardware.

DESARROLLO:

a) La Sección de INFORMÁTICA se encargará de establecer la necesidad de comprar equipos, programas y suministros así como de contratos de seguro y mantenimiento. Esta necesidad se comunicará mediante un oficio a la comisión informática adjuntándose un análisis técnico con los justificativos, términos de referencia, y el proveedor recomendado para la adquisición. Una copia del mismo se mantendrá en la Sección de INFORMÁTICA.

b) La comisión informática autorizará o negará la compra de los equipos, programas o suministros y la contratación de seguros y mantenimiento remitiendo el respectivo oficio con la respuesta a la Sección de INFORMÁTICA con copia a los departamentos correspondientes (si la respuesta es afirmativa). Para ello y los demás puntos de este procedimiento se tomarán en cuenta las normas y políticas vigentes.

c) La Sección de INFORMÁTICA coordinará la adquisición mediante contratos o facturas (contemplando garantías y plazos de entrega) con el departamento financiero y el proveedor seleccionado.

d) La Sección de INFORMÁTICA se encargará de recibir y probar los equipos, programas y suministros adquiridos con un acta de entrega recepción o nota de entrega. Los equipos y programas deben adquirirse siempre con manuales y los discos respectivos (al comprar

programas el proveedor deberá entrenar en el manejo del mismo al personal, por lo tanto se coordinará este entrenamiento con la Sección de INFORMÁTICA. Deberá entregar un manual de utilización y un manual de desarrollo y programación del sistema con los programas fuentes en los discos), los programas y manuales se mantendrán en la biblioteca siendo de propiedad de la empresa. Los suministros se mantendrán en una bodega (con kardex e inventario mensual) dentro de la Sección de INFORMÁTICA y bajo responsabilidad de la misma. Los contratos y documentación de la compra se mantendrán en los departamentos correspondientes.

PROCEDIMIENTO N°4

TITULO: **Reporte y reparación de daños en los equipos.**

DIRIGIDO A: Comisión Informática, Sección de INFORMÁTICA, Jefes de Departamento y Usuarios de computadores.

OBJETIVO: Definir las normas generales para reportar y reparar los daños a los equipos.

DESCRIPCIÓN: Este procedimiento se aplica cuando la Sección de INFORMÁTICA, en conversación con usuarios y jefes de departamento, establezca daños en los equipos.

RESPONSABLE: Comisión Informática y Sección de INFORMÁTICA.

LIMITACIONES: Se procurará reparar siempre todo equipo dañado este o no en garantía. De ser necesario se establecerán responsabilidades sobre el mismo.

RESTRICCIONES: Se repararán únicamente en servicios técnicos autorizados.

DESARROLLO:

a) La Sección de INFORMÁTICA se encargará de establecer los daños en equipos. Estos daños se comunicarán mediante un oficio a la comisión informática adjuntándose un detalle del daño. Una copia del mismo se mantendrá en la Sección de INFORMÁTICA.

b) La comisión informática autorizará la reparación de los equipos y enviará un oficio con la respuesta a la Sección de INFORMÁTICA con copia al Departamento Financiero (Bodega).

c) La Sección de INFORMÁTICA coordinará la reparación (contemplando garantías y plazos de entrega) con el departamento financiero y el proveedor de los equipos (o el que los

arregle). Se verificará si los equipos están todavía en garantía, en cuyo caso no se procederá a ningún pago por la reparación.

d) La Sección de INFORMÁTICA se encargará de recibir y probar los equipos.

PROCEDIMIENTO N°5

TITULO:	**Reubicación de los equipos.**
DIRIGIDO A:	Comisión Informática, Sección de INFORMÁTICA, Jefes de Departamento y Usuarios de computadores.
OBJETIVO:	Definir las normas generales para trasladar de una localidad a otra los equipos.
DESCRIPCIÓN:	Este procedimiento se aplica cuando la Sección de INFORMÁTICA, en coordinación con usuarios y jefes de departamento, establezca la necesidad de trasladar los equipos a otra localidad.
RESPONSABLE:	Comisión Informática y Sección de INFORMÁTICA.
LIMITACIONES:	Los equipos los trasladará el encargado de la Sección de INFORMÁTICA únicamente. Para ello es necesario un oficio con la autorización por parte de la Comisión Informática.
RESTRICCIONES:	Se trasladará únicamente dentro de las instalaciones de la empresa.

DESARROLLO:

a) La Sección de INFORMÁTICA se encargará de establecer la necesidad de trasladar los equipos. Esta necesidad se comunicará mediante un oficio a la comisión informática adjuntándose un detalle justificativo de la acción y los requerimientos para seguridad de los equipos e instalaciones eléctricas. Una copia del mismo se mantendrá en la Sección de INFORMÁTICA.

b) La comisión informática autorizará el traslado de los equipos y enviará un oficio con la respuesta a la Sección de INFORMÁTICA, a bodega y a los demás departamentos correspondientes.

c) Si la respuesta es afirmativa la Sección de INFORMÁTICA coordinará y trasladará los equipos a la nueva localidad revisando siempre con anticipación si las instalaciones eléctricas y las seguridades son las adecuadas. Se verificará si los equipos funcionan

correctamente y luego se emitirá un acta de entrega-recepción del mismo. La documentación deberá archivar la Sección de INFORMÁTICA y Bodega.

PROCEDIMIENTO N°6

TITULO:	**Inventario de equipos, programas, aplicaciones y suministros**.
DIRIGIDO A:	Comisión Informática, Sección de INFORMÁTICA, Jefes de Departamento y Usuarios de computadores.
OBJETIVO:	Definir las normas generales para el buen manejo de equipos, programas, aplicaciones y suministros.
DESCRIPCIÓN:	Este procedimiento se aplicará en la Sección de INFORMÁTICA para mantener siempre inventarios actualizados y un buen control sobre equipos, programas, aplicaciones y suministros.
RESPONSABLE:	Comisión Informática y Sección de INFORMÁTICA.
LIMITACIONES:	Se procurará siempre mantener un inventario actualizado de todo.

DESARROLLO:

a) La Sección de INFORMÁTICA se encargará de mantener un control de la ubicación de los equipos mediante un inventario actualizado de los mismos. Este inventario deberá contener los números de serie de los equipos. Se comunicarán mediante un oficio a la comisión informática cada trimestre la situación de este inventario. Cualquier pérdida se deberá reportar inmediatamente para la acción pertinente.

b) La Sección de INFORMÁTICA se encargará de mantener un control en una biblioteca con llave de los manuales de los computadores, programas y aplicaciones además de todos los discos y cintas que contengan programas, aplicaciones o datos. Deberá mantenerse un inventario actualizado de los mismos. Este inventario deberá estar siempre detallado. Se comunicarán mediante un oficio a la comisión informática cada trimestre la situación de este inventario. Cualquier pérdida se deberá reportar inmediatamente para la acción pertinente.

c) La Sección de INFORMÁTICA llevará un control sobre el uso de suministros los cuales se entregarán mediante oficio de los jefes de departamento y con firma de quien los retira. Se deberá mantener siempre un Kardex actualizado de los mismos. Un informe con los saldos del inventario deberá entregarse tanto a la Comisión Informática como al departamento financiero cada trimestre.

2.10. ESTÁNDARES Y NORMAS DE CODIFICACIÓN

Los usuarios al escribir los nombres de sus trabajos (8 caracteres) deberán usar el siguiente esquema:

Posición 1..... Inicial del nombre del usuario
Posición 2..... Inicial del apellido del usuario
Posición 3..... Inicial del departamento o sección
Posiciones 4 a 8.... Descripción del trabajo

2.11. SEGURIDADES GENERALES

Los usuarios de los equipos computarizados deberán observar las normas de seguridad descritas a lo largo de este manual en todas sus labores.

La responsabilidad por el manejo de cada equipo recae sobre el usuario a cargo del mismo, el cual deberá tomar todas las medidas del caso para garantizar el cuidado y buen uso de los equipos.

Los procedimientos descritos en el punto 2.9 deberán observarse y respetarse siempre ya que contienen las normas de seguridad específicas para cada situación en particular.

Es responsabilidad de la Comisión de Informática y de la Sección de INFORMÁTICA establecer todas las medidas de control necesarias para garantizar la seguridad de los equipos.
Los equipos deberán siempre estar amparados por una póliza de seguros y un contrato de mantenimiento.

2.12. OBTENCIÓN DE RESPALDOS

Cada usuario deberá mantener siempre por lo menos una copia de seguridad o respaldo de su información.

La Sección de INFORMÁTICA deberá mantener tres respaldos de aquella información que sea considerada crítica en el desenvolvimiento de la actividad de la empresa.

Los respaldos se sacarán en cintas o discos verificando previamente su estado.

2.13. OBLIGACIONES Y PROHIBICIONES DE USUARIOS

Todo usuario deberá sujetarse a las normas y disposiciones emitidas por la Comisión de Informática y la Sección de INFORMÁTICA además de todas las normas contenidas en el presente documento.

Los procedimientos descritos en la sección 2.9, del presente documento constituyen normas de trabajo y deberán ser observadas siempre que se manejen equipos computarizados.

Está totalmente prohibido a los usuarios llevarse programas, manuales y suministros para uso personal o de terceros. Además se prohíbe el uso de los recursos computacionales para desarrollar tareas personales que no tienen que ver con la actividad de la empresa

2.14. CARTAS A LA GERENCIA

Uno de los propósitos de aplicar las técnicas de Auditoría es informar sobre deficiencias de control encontradas durante el examen.

Para cumplir apropiadamente con dicha finalidad es necesario evaluar el sistema de control con anterioridad al examen de los Sistemas de Información Basados en Computadora. Como resultado de dicho estudio y evaluación, el auditor deberá emitir una carta de recomendación tendiente a corregir las deficiencias encontradas siempre y cuando se consideren de importancia relativa. Esta carta o documento es comúnmente llamada "CARTA A LA GERENCIA" la misma que debe contener información que ayude a la administración a tomar acciones o decisiones correctivas, es por eso que la carta de recomendaciones, debe ser emitida y dirigida a personas que ocupen una posición tal que les permita tomar acciones correctivas inmediatas de preferencia a la Gerencia General, por cuanto es ella la responsable de mantener adecuados procedimientos de control tanto administrativos, contables y de otra índole.

Por lo tanto debería constituirse como política de una firma de auditores, que el auditor ayude al cliente o le asesore en su responsabilidad de implementar esos procedimientos de control, además considerando que el auditor, mantiene un conocimiento amplio en términos generales, sobre las operaciones de la entidad y considerando su punto de vista independiente, se considera que está más capacitado como para efectuar sugerencias constructivas.

Generalmente las cartas de recomendaciones deben ser emitidas por lo menos una vez al año, sin embargo el socio o responsable del compromiso de Auditoría, podrá tomar la decisión de emitir esta carta con mayor frecuencia. Todas las observaciones de Control Interno que realice el auditor,

ya sean éstas de naturaleza contable u operativa, deberán ser discutidas con el personal a niveles apropiados a efectos de confirmar el contenido de la carta.

2.14.1. TÉCNICAS DE PREPARACIÓN

- Cada observación debe ser titulada
- Cada observación deberá contener una breve explicación de la deficiencia, los riesgos inherentes y la corrección sugerida.
- Deberá tenerse muy presente la regla Costo-Beneficio
- Los puntos a ser incluidos no deben limitarse a aspectos netamente del entorno informático. Deberán incluir aspectos operativos, contables, impositivos y laborales.
- Incluir adjunto a las recomendaciones de ser posible, cuadros explicativos, gráficos o cuantificar el efecto de las recomendaciones.
- Cuando son extensas las cartas, incluir un índice de contenido.
- Incluir los puntos relevantes primero y los menos relevantes al último.
- Puntos de años anteriores insistir nuevamente dependiendo de su importancia, en estos casos expresiones como: "Reiteramos nuestra recomendación de años anteriores" serían apropiadas.
- En la recomendación deberán usarse frases como "Sugerimos, creemos conveniente, recomendamos" Nunca se debe imponer.
- Debe ser enviada con anterioridad a la fecha de emisión de Estados Financieros.
- Debe ser discutida antes de ser emitida formalmente.

2.15. ARCHIVO DE ANÁLISIS

ÍNDICE

- SISTEMA DE CONTABILIDAD
- SISTEMA DE ACTIVOS
- SISTEMA DE CAJA
- SISTEMA DE FACTURACIÓN
- SISTEMA DE CARTERA
- SISTEMA DE INVENTARIOS
- SISTEMA DE NOMINA
- SISTEMA DE PRODUCCIÓN

CLIENTE

INDICE - ARCHIVO PERMANENTE

A) HISTORIA DE LA COMPAÑÍA

1. Escritura de constitución y estatutos
2. Accionistas
3. Directores
4. Actas de juntas de accionistas
5. Actas de juntas de directores

B) ACTIVIDADES COMERCIALES O INDUSTRIALES

1. Productos que fabrica o comercializa (indicar la importancia de cada uno sobre el total)
2. Condiciones de ventas (indicar para cada producto qué condición rige su comercialización: plazos, descuentos, garantía, etc.)
3. Materias primas (o mercaderías para reventa) principales
4. Proveedores principales

C) ORGANIZACIÓN CONTABLE

1. Principales departamentos o subdivisiones, con una breve descripción de sus funciones e indicación del número aproximado de personas en cada uno
2. Lista de las firmas o iniciales usadas por las personas responsables de autorizar documentos y firmar cheques
3. Libros y registros
4. Informes preparados periódicamente por la compañía
5. Plan de cuentas
6. Instrucciones para la utilización del plan de cuentas

D) POLÍTICA Y PROCEDIMIENTOS CONTABLES

1. Ingresos de caja
2. Desembolsos de caja
3. Ventas y cuentas por cobrar
4. Inventarios

5. Activo fijo
6. Compras y cuentas por pagar
7. Planillas
8. Sistema de costos

E) HISTORIA FINANCIERA

1. Resumen por años del balance
2. Resumen por años del estado de ganancias y pérdidas
3. Resumen por años del estado de utilidades o pérdidas acumuladas
4. Comparaciones financieras
5. Resumen del movimiento anual de reservas de capital
6. Resumen del movimiento anual de activo fijo

F) SITUACIÓN FISCAL

1. Impuestos a que está obligada la compañía
2. Exenciones tributarias de que goza la compañía
3. Copias o síntesis de las disposiciones tributarias que afecten a la compañía
4. Conciliaciones entre la utilidad contable y la utilidad fiscal (obtener copia de las declaraciones presentadas a las autoridades tributarias) - por años
5. Conciliaciones entre la utilidad declarada y utilidad revisada por las autoridades tributarias - por años
6. Situación de los años aún no revisados por las autoridades tributarias

G) SÍNTESIS O COPIAS DE CONTRATOS Y ESCRITURAS

1. Propiedades
2. Aumentos de capital
3. Royalties
4. Trabajo

ARCHIVO GENERAL

ÍNDICE

A. Informes de años anteriores
B. Cartas a la gerencia anteriores
C. Balance de prueba
D. Estados financieros del cliente
E. Carta de representación
F. Extractos de actas de directorio y junta de accionistas
G. Correspondencia relacionada con el cliente
H. Memorándums y comunicaciones internas
I. Flujogramación (incluyendo narrativas)
J. Revisión de sistemas
K. Registro de deficiencias de control y discusiones con el cliente de cartas a la gerencia
L. Prueba de funciones y organización
M. Presupuesto y estado del presupuesto de horas
N. Resumen del tiempo real utilizado

MEMORÁNDUM DE COMPROMISO

CONTENIDO:

a._ Antecedentes de la compañía
b._ Personal asignado al trabajo
c._ Presupuesto de tiempo
d._ Plan detallado de trabajo
e._ Áreas críticas descritas

2.16. RESPONSABILIDADES DE AUDITORÍA INFORMÁTICA

DESARROLLAR Y/O ADQUIRIR:

- Software de Auditoría
- Cuestionarios / Check-Lists
- Métodos/Técnicas
- Habilidad / Entrenamiento

- Asistencia externa etc.

EVALUAR LO ADECUADO DE:

- Estándares y Procedimientos establecidos y propuestos
- Políticas y Procedimientos Financieros
- Políticas y Procedimientos de los Sistema de Información
- Estándares para Control de Proyectos
- Estándares para diseño de programas y sistemas
- Estándares para documentación de sistemas, programas, manuales del usuario y operación.

EVALUAR SISTEMAS EN DESARROLLO:

Facilidades propuestas para mantener:

- Exactitud
- Confiabilidad
- Integridad
- Seguridad y Control
- Auditabilidad cuando lleguen a estar operacionales

Uso eficiente de:

- Tiempo
- Esfuerzos
- Dinero
- Otros recursos
- Efectividad en realizar resultados deseados

EVALUAR SISTEMAS OPERACIONALES:

Se debe evaluar si los Sistemas Operacionales son adecuados y si se da cumplimiento, con el uso de los mismos para obtener información que proporcione:

- Exactitud
- Confiabilidad
- Integridad

- Auditabilidad
- Seguridad y Control
- El uso eficiente de los recursos
- El grado de efectividad en satisfacer las necesidades del usuario.

REVISAR LA ADMINISTRACION DE LOS SISTEMAS DE INFORMACIÓN BASADOS EN COMPUTADOR:

Verificar si la información proporcionada, cumple con:

- Prácticas y controles administrativos y operativos.
- La forma en que se cumplen los objetivos.

EVALUAR A USUARIOS Y GRUPO DE SOPORTE:

Se deberá evaluar a los usuarios y al grupo de soporte, con la finalidad de analizar si se cumple con:

Información proporcionada con:

- Exactitud
- Confiabilidad
- Integridad
- Seguridad
- Control
- Auditabilidad de los sistemas computacionales.
- Eficiencia y eficacia de sus operaciones.

Probar y observar el cumplimiento de todas las:

- Políticas
- Procedimientos
- Estándares

Conducir investigaciones sobre:

- Déficits
- Desapariciones y destrucciones misteriosas

- Fraudes y pérdidas

Llamar la atención de la Administración y Dirección de la Institución sobre riesgos significativos en:

- El negocio
- Finanzas
- Legal
- Seguridad
- Y otros que aparezcan como imprudentes o excesivos e involucren consecuencias graves que podrían materializarse.

2.17. EL PROCESO DE AUDITORÍA

2.16.1 ESTUDIO PRELIMINAR
2.16.2 TRABAJO DE CAMPO
2.16.3 DOCUMENTACION DE EVIDENCIAS
2.16.4 PRODUCCION DEL REPORTE DE AUDITORÍA

2.17.1. ESTUDIO PRELIMINAR

- Constitución de la Organización
- Organización
- Archivo permanente de Auditoría
- Reportes previos de Auditoría
- Planes de corto y largo plazo (reportes de avances)
- Presupuestos
- Descripción de funciones
- Procedimientos de performance
- Esquemas y diagramas de flujo de procesos
- Manuales de Procedimientos
- Copias de los logs de operaciones:
- Print-log
- Resum-log
- Operator-log
- Tope/Disk-log
- Change-log
- Resúmenes de utilización de recursos

- Planes de contingencia y convenios.

FUENTES PARA ESTÁNDARES DE BUENA PRÁCTICA

- Ordenes de la Dirección
- Instructivos de trabajo en Manuales de Operación
- Requerimientos de Presupuesto
- Requerimientos regulatorios obligatorios
- Registros de Performance
- Reportes sobre experiencias en la Industria
- Publicaciones de Organizaciones profesionales con autoridad

2.17.2. TRABAJO DE CAMPO

Se han establecido los controles necesarios
Existen y se aplican Procedimientos de Control
Las excepciones son identificadas, analizadas y comunicadas a los responsables
La acción correctiva se toma prontamente:

- Controles que afecten significativamente la labor de Auditoría.
- La información concerniente a la naturaleza y extensión de controles.
- Todos los procedimientos de Control y Auditoría deben estar documentados.

2.17.3. DOCUMENTACIÓN DE EVIDENCIAS

Especificar lo concerniente a los encuentros y luego conciliar éstos con las guías y estándares establecidos.

El soporte de la evidencia por encuentros deficientes debería demostrar la existencia del defecto, proveer información concerniente a la materialidad del defecto y producir datos suficientes para dar a la administración una base adecuada para actuar.

2.17.4. PRODUCCIÓN DEL REPORTE DE AUDITORÍA

- Exacto, claro, conciso, oportuno y cortés.
- Encuentros favorables y desfavorables.
- Resumen en cápsula:

Criterio

Descripción

Causa

Efecto y recomendaciones

- Criterio Aplicado:

¿Por qué estándares fue juzgado?

- Descripción de deficiencias:

¿Qué estuvo errado?

- Causa de la deficiencia:

¿Qué sucedió?

- Efecto de la deficiencia:

¿Qué efectos tuvo?

- Recomendaciones de los Auditores para acción correctiva:

¿Cuál es la solución?

- Acciones correctivas planes.

CARACTERÍSTICAS DEL PERFIL DEL AUDITOR

Debe cumplir las siguientes características:

ENTRENAMIENTO EN AUDITORÍA

- Conoce como auditar.
- Está en posibilidad de aplicar herramientas modernas de auditoría.
- Se mantiene actualizado en las prácticas de auditoría.

ENTRENAMIENTO EN SISTEMAS DE INFORMACIÓN BASADOS EN COMPUTADORA

- Análisis y diseño de sistemas
- Programación de aplicaciones
- Programación de sistemas
- Hardware
- Base de datos/comunicación de datos

CARACTERÍSTICAS PERSONALES

- Inteligencia Analítica y sobre el promedio general
- Habilidades superiores en comunicación oral y escrita
- Escuchador y pensador
- Curioso e inquisitivo
- Político
- Profesional

2.18. ORGANIZACIÓN DE LA FUNCIÓN DE AUDITORÍA INFORMÁTICA (A.I)

La función de auditoría informática debe observar lo siguiente:

- Número de aplicaciones
- Medidas y complejidad de cada aplicación
- Frecuencia de Auditoría
- Número de Instalaciones
- Diversidad de Tecnología
- Dispersión Geográfica de Instalaciones
- Localizaciones para el Desarrollo de Sistemas
- Sitios de Preparación de Datos

2.19. SISTEMA DE REGULACIÓN DE VOLTAJE

Se debe observar que el Centro de Cómputo cuente con un sistema que regule el voltaje de la corriente eléctrica que ingresa a los computadores, para evitar que una falla en la corriente eléctrica pueda dañar el equipo y la información.

2.19.1. FUENTE DE ENERGÍA ELÉCTRICA

Se debe observar que el Centro de Cómputo cuente con una fuente de energía eléctrica (UPS), que dé energía al computador cuando no hay corriente eléctrica.

La utilización de uno de estos aparatos es necesaria debido a que muchos procesos de información al ser interrumpidos por fallas de corriente eléctrica, ocasionan la pérdida de información. Una fuente de poder puede dar la energía necesaria para terminar los procesos y apagar debidamente el equipo luego de interrumpirse la corriente eléctrica.

2.19.2. SISTEMA DE AIRE ACONDICIONADO

El Centro de Cómputo debe contar con un sistema de aire acondicionado que permita mantener a los equipos de cómputo funcionando en los límites de temperatura sugeridos por el fabricante de los equipos.

2.20. FUNCIONALIDAD DE LAS INSTALACIONES DEL DEPARTAMENTO DE P.E.D

Las instalaciones y distribución física del departamento de P.E.D. deben prestar facilidades para el trabajo del personal de dicha área, con el propósito de optimizar recursos.

2.20.1. LÍNEAS DE ALIMENTACIÓN ELÉCTRICA PARA LOS EQUIPOS DE P.E.D.

Debe existir una instalación eléctrica independiente para los equipos de Procesamiento Electrónico de Datos, con el propósito de que no se den interferencias eléctricas en los equipos del centro de cómputo causadas por los otros aparatos de la compañía.

2.20.2. CONEXIÓN A TIERRA DE LAS INSTALACIONES ELÉCTRICAS PARA EL DEPARTAMENTO DE P.E.D

Las líneas eléctricas que alimentan al departamento de P.E.D. deben contar con una conexión a tierra (neutro), puesto que ello evitará que las descargas eléctricas (muy comunes en nuestro medio) recaigan en los equipos.

2.20.3. MEDICIÓN DE VOLTAJE, TENSIÓN E INTENSIDAD DE LA CORRIENTE ELÉCTRICA

Se debe observar que el Centro de Cómputo cuente con un aparato de medición que permita controlar el voltaje, tensión e intensidad de la corriente eléctrica.

A efectos de evitar que excesivas cargas eléctricas dañen el equipo, se debe instalar un sistema de medición que permitan controlar y evitar daños al equipo por efectos de corriente eléctrica.

2.21. SISTEMA DE DETECCIÓN DE INCENDIOS

Debe existir un sistema para detección de incendios y alarma de activación manual.

Debe existir un sistema que permita detectar y avisar rápidamente un inicio de incendio. Los equipos de P.E.D. pueden estropearse en forma total con el simple contacto con fuego.

INDICACIÓN DE "NO FUMAR"

Ubicar un letrero o indicativos que señalen que está prohibido fumar en dicho lugar. La ceniza y el humo deterioran y pueden incluso causar daños graves al equipo de Procesamiento de Datos.

2.22. ACCESO AL DEPARTAMENTO DE P.E.D.

Restringir y reglamentar el acceso a dicho departamento, por lo delicado de las labores y seguridad del equipo y de los procesos de información.

2.23. PLAN DE SEGURIDAD Y EMERGENCIA

Elaborar un plan de seguridad y emergencia que permita al Departamento de P.E.D. reiniciar sus labores a la brevedad posible en casos de emergencias, daños, siniestros, etc. Este plan debe contener procedimientos escritos para cada tipo de emergencia, así como normas de seguridad física a observarse en dichos casos.

2.24. LIMPIEZA DEL DEPARTAMENTO DE P.E.D

Bajo la vigilancia del personal del departamento de P.E.D., se debe establecer un horario adecuado para que el personal de limpieza realice sus labores en este departamento. El polvo, la suciedad y la

falta de cuidado deterioran tanto los acabados externos como los dispositivos electrónicos de los equipos.

2.25. REGLAMENTO DE SEGURIDAD FISICA DEL DEPARTAMENTO DE P.E.D.

Elaborar dicho documento, en el cual se detalle las labores de cada uno de los integrantes del departamento de P.E.D. y a qué tipo de información tienen acceso (niveles de acceso). Además de horarios de entrada y salida, así como detalles sobre el uso del computador por parte de cada persona, elaboración, cambio y mantenimiento de claves de acceso, etc. En este manual es recomendable que se fijen políticas de la empresa en cuanto al manejo de la información y del departamento de P.E.D.

2.25.1. LIBRERÍA PARA MANUALES

Dotar al departamento de P.E.D. de un lugar adecuado y resguardado para mantener allí toda la documentación escrita y digital de los computadores y asignar a una persona que se responsabilice para que maneje dicha librería.

2.25.1.1. CONTROL DE ENTREGA DE MANUALES Y DOCUMENTACION DEL SISTEMA

Llevar un registro que permita conocer a quién se presta los manuales, para controlar la entrega y devolución de los mismos.

2.25.1.2. INVENTARIO DE MANUALES Y DOCUMENTACION DEL SISTEMA

Mantener siempre un inventario actualizado y completo de todos los manuales y documentos del sistema con el fin de conocer qué se tiene, dónde se tiene y quién es el responsable de ellos.

2.25.1.3. COPIAS DE MANUALES Y DOCUMENTACION

Con el objeto de salvaguardar información y documentación recogida en dichos manuales, se debe guardar una copia de los mismos en un lugar fuera de la empresa, como bancos, cajas de seguridad, sucursales, etc.

2.25.1.4. RESPALDOS DE INFORMACION

Guardar respaldos de información crítica en lugares fuera de la empresa.

2.25.1.5. ACCESO A RESPALDOS DE INFORMACION

Dar un buen uso a los medios de almacenamiento y restringir totalmente el acceso a dicho material.

2.25.1.6. INVENTARIO DE RESPALDOS DE INFORMACION

Llevar un registro de cada uno de los respaldos de información obtenida, en el cual consten: el contenido, fecha en el que fue grabado, etc. Además, etiquetar e identificar adecuadamente todo este tipo de material.

2.25.1.7. DESTRUCCIÓN DE MEDIOS MAGNÉTICOS INSERVIBLES

Destruir adecuadamente todo material magnético inservible a fin de no acumular basura en el departamento de P.E.D.

2.26. ACCESO A PROGRAMAS Y APLICACIONES

Elaborar un reglamento que restrinja el acceso a dicha información a fin de evitar que ésta se filtre a otras instituciones.

2.26.1. MATERIAL CONFIDENCIAL Y DE ALTO RIESGO

El acceso a este tipo de material debe ser controlado y observar que se encuentra claramente identificado y etiquetado.

2.26.2. POLÍTICAS DE PROPIEDAD Y DE PROTECCIÓN DE LA INFORMACIÓN

Dictaminar políticas que permitan salvaguardar la información. Se debe tener especial cuidado con los programas y de ser posible se debe registrar la propiedad de los mismos a fin de que otras instituciones no los utilicen.

2.26.3. PLAN ESCRITO PARA SACAR COPIAS DE RESPALDO DE LA INFORMACIÓN

Elaborar un plan y reglamentar la forma en que se deben sacar las copias de seguridad. Este documento debe contener: el nombre o nombres de las personas a cargo de dicho proceso, la frecuencia con que debe llevarse a cabo, a quién se deben entregar, cómo se deben almacenar, estándares de identificación, etc.

2.27. STOCKS MINIMOS DE SUMINISTROS

Calcular los stocks mínimos adecuados y mantener siempre dicha cantidad en reserva a fin de que el departamento de P.E.D. no detenga sus labores por este motivo.

2.27.1. CONTROL DEL USO DE SUMINISTROS

Se debe establecer una política para controlar el uso de todos los suministros necesarios para el departamento de P.E.D.

2.28. PROCEDIMIENTOS DE ENCENDIDO Y APAGADO DEL COMPUTADOR

Elaborar un manual de procedimientos de encendido y apagado del equipo que contemple todas las circunstancias que puedan darse en el departamento de P.E.D. e impliquen la realización de este proceso. Estos procedimientos son de carácter crucial sobre todo cuando se va la corriente eléctrica.

2.29. REGISTRO DE AVERÍAS, DAÑOS E INTERRUPCIONES

Elaborar un registro adecuado que permita conocer acerca de averías, daños e interrupciones de funcionamiento de los distintos equipos a fin de facilitar el mantenimiento y controlar de mejor manera los equipos.

2.30. PROCESOS DE EMERGENCIA EN OTRAS LOCALIDADES

Buscar una institución que posea el mismo tipo de equipo y convenir la continuación de los procesos en dicho lugar en caso mide que se dañe el equipo.

2.31. SOLICITUD DE PROCESOS DE INFORMACIÓN Y HOJA DE RUTA

Establecer un formulario diseñado que detalle quién solicitó procesos y cuál es el usuario final de la información procesada por el departamento de P.E.D. La hoja de ruta permite conocer inclusive por qué personas ha pasado la información.

2.32. CRONOGRAMAS DE TRABAJO

Elaborar continuamente un cronograma de trabajo que permita asignar el uso de los recursos y la buena labor del departamento de P.E.D.

2.33. DOCUMENTACIÓN DE LOS PROGRAMAS

Revisar, adecuar y completar la documentación que acompaña a los programas, esto es, análisis, diseño, descripción, flujo gramas, listados, etc. Esta información es indispensable para hacer cambios a programas, mantenimiento de sistemas, etc. y el momento en que el personal de P.E.D. deja de laborar en la empresa es el único soporte para seguir utilizando y adecuando cada programa.

2.33.1. AUTORIZACIÓN DE CAMBIOS DE PROGRAMAS

La Gerencia debe intervenir directamente aprobando los cambios o modificaciones a programas. Un cambio inadecuado puede resultar en pérdida de información.

2.33.2. REVISIÓN Y VERIFICACIÓN DE LOS CAMBIOS DE PROGRAMAS

Probar detenida y adecuadamente los programas modificados y documentar al detalle dichas pruebas como referencia futura. El riesgo de no probar adecuadamente un programa es el de perder información.

2.33.3. PRUEBAS EN CONJUNTO DE PROGRAMAS Y APLICACIONES NUEVAS O MODIFICADAS

Efectuar pruebas que garanticen el que un nuevo programa o aplicación o un cambio o modificación de las mismas no altere o afecte al resto del sistema.

2.33.4. DOCUMENTACIÓN DE CAMBIOS Y MODIFICACIONES A PROGRAMAS

Con el propósito de mantener una historia de la vida de cada programa, añadir a la documentación correspondiente a cada programa todos los cambios o modificaciones que éstos hayan sufrido. Dicha documentación deberá detallar todo lo referente al proceso de cambio.

2.33.5. MANTENIMIENTO DE PROGRAMAS Y APLICACIONES

Con el propósito de tener siempre los sistemas funcionando correctamente elaborar un plan de trabajo con la finalidad de verificar como están trabajando los programas y sugerir modificaciones que permitan optimizar los recursos disponibles.

2.33.6. DESTRUCCIÓN DE PRUEBAS DE PROGRAMAS

Destruir todo rezago inservible proveniente de las pruebas de programas y se guarde únicamente lo indispensable para documentar adecuadamente dichas pruebas.

2.33.7. INTEGRACIÓN DE PROGRAMAS Y APLICACIONES

Integrar en un todo todos los programas con el fin de que ciertos procesos no sean repetidos y que la información ingresada al sistema sea procesada en forma óptima.

2.33.8. PROCEDIMIENTOS ACERCA DEL USO DE CADA PROGRAMA Y APLICACIÓN

Elaborar un documento que detalle objetivos, usuario final, etc., de cada programa y aplicación.

2.33.9. ESTÁNDARES PARA LA ELABORACIÓN DE PROGRAMAS, APLICACIONES Y DOCUMENTACIÓN

Fijar dichos estándares con el fin de que toda la información sea presentada en forma clara y sobre todo uniforme.

2.33.10. CONTROL DE FALLAS DE FUNCIONAMIENTO DE PROGRAMAS Y APLICACIONES

Implantar controles ya que de él se desprenden una serie de criterios para mejorar el sistema entero evitando que se repitan errores que muchas veces detienen y dificultan los procesos.

2.34. PROCEDIMIENTOS ESCRITOS PARA GRABAR Y RESTAURAR INFORMACIÓN

Elaborar un documento en que se detalle la forma de grabar y restaurar la información que se requiere.

2.35. TIEMPO DE UTILIZACIÓN DEL COMPUTADOR POR PARTE DE LOS USUARIOS

Elaborar listados que el mismo computador puede producirlos, que detallen el tiempo de uso de cada terminal por cada usuario con el fin de tomar criterios para optimizar el uso de tan importante recurso.

Este tipo de listados ayudan a determinar intentos fallidos de ingreso al computador por parte de personas no autorizadas.

2.36. MESA DE CONTROL

Implantar una mesa de control que ayude a garantizar la calidad de la información procesada, además que pueda controlar la entrega y utilización final de la información.

2.37. PARTICIPACIÓN DE AUDITORÍA INTERNA EN EL DESARROLLO, MODIFICACIÓN Y REVISIÓN DE PROGRAMAS Y APLICACIONES

Es indispensable que la Auditoría Interna participe en estos procesos a fin de sugerir y prevenir errores.

(Guachi Aucapiña, 2012) Menciona que las Norma ISO 27001 garantiza los controles de seguridad contribuyendo a salvaguardar los activos de información, "Dada la evolución de la Tecnología de la información y su relación directa con los objetivos del negocio de las Organizaciones, el universo de amenazas y vulnerabilidades crece por lo tanto es necesario proteger uno de los activos más importantes de la Organización, la información, garantizando siempre la disponibilidad, la confidencialidad e integridad de la misma. La forma más adecuada para proteger los activos de información es mediante una correcta gestión del riesgo, logrando así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentren más expuestos."

2.37.1. PLAN PARA DESARROLLO FUTURO

Elaborar un plan de desarrollo futuro de aplicaciones y programas, en el cual se detallen las perspectivas a futuro del departamento de P.E.D., su expansión futura, planes y proyectos.

2.37.2. PARTICIPACIÓN DE AUDITORÍA INTERNA EN LAS LABORES DE P.E.D.

En vista de que la intervención de Auditoría Interna es siempre conveniente, debe participar en el desarrollo, pruebas y revisión de programas y aplicaciones así como una revisión del cumplimiento de normas y procedimientos por parte del departamento de P.E.D. Es importante que se hagan inspecciones regulares y por sorpresa a dicho departamento.

2.38. PALABRAS CLAVES Y CÓDIGOS SECRETOS

Controlar y variar las claves con regularidad a fin de evitar ingresos irregulares y no autorizados por descuido o descubrimiento de dichas claves o códigos.

Es indispensable también que cada usuario tenga su propia clave de acceso y que cada uno sea responsable en forma individual del uso de dicha clave.

2.39. ORGANIZACIÓN DEL DEPARTAMENTO DE P.E.D.

Organizar adecuadamente el departamento y segregar las funciones de cada persona del departamento. Para ello es aconsejable elaborar un manual de organización donde se describan responsabilidades, obligaciones, etc.

2.39.1. SELECCIÓN Y EVALUACIÓN DEL PERSONAL DE P.E.D.

Elaborar políticas y mecanismos que permitan seleccionar y evaluar adecuadamente al personal de P.E.D.

(PriteshGupta, 2012), menciona la norma Iso 27002 y sus cláusulas en el siguiente esquema relacionados con el talento humano:

"ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en seguridad de la información.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo"

Al revisar estas cláusulas, se puede obtener los parámetros para realizar la contratación de personal, como indica en (PriteshGupta, El portal de ISO 27002 en Español, 2012): Antes de la contratación

"Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles.

Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.

Conjuntamente con RRHH, de debería asegurar que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc."

2.39.2. CAPACITACIÓN DEL PERSONAL DE P.E.D.

Elaborar un plan de capacitación para el personal que labora en esta área con el fin de que estén siempre al día en una ciencia que avanza muy rápido como es la informática.

2.39.2.1. FORMACIÓN DEL PERSONAL DE P.E.D. EN TÉCNICAS DE HARDWARE

Capacitar al personal en técnicas de manejo del equipo y control de averías, a fin de que conozcan cómo proceder cuando éstas se presenten.

(PriteshGupta, El portal de ISO 27002 en Español, 2012), en la cláusula 7.2 Durante la contratación menciona: "Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.

A todos los usuarios empleados, contratistas y terceras personas se les debería proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

Se debería establecer un proceso disciplinario normal para gestionar las brechas en seguridad.

La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc.

Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información."

2.39.3. MOTIVACIÓN DEL PERSONAL DE P.E.D.

Trazar políticas que mantengan a dicho personal siempre motivado y dispuesto a brindar todo su esfuerzo en favor de la institución.

Para el personal, una causa de motivación es la capacitación que la organización le pueda ofrecer.

2.39.4. PERSONAL DE SEGURIDAD

El personal de seguridad de la Empresa debe estar informado acerca de medidas y cuidados específicos que se deben tener en cuenta con relación al departamento de P.E.D.

2.39.4.1. SEGURIDAD DE LA INFORMACIÓN AL TERMINAR RELACIONES LABORALES CON PERSONAL DE P.E.D.

Elaborar políticas que permitan salvaguardar la información cuando cesa la relación laboral con alguna persona de dicho departamento.

En el cese de las funciones menciona (PriteshGupta, El portal de ISO 27002 en Español, 2012) lo siguiente: "7.3.1 Cese o cambio de puesto de trabajo: Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente."

2.39.5. VACACIONES OBLIGATORIAS

Definir políticas que obliguen al personal de P.E.D. a tomar vacaciones a fin de optimizar su rendimiento.

2.40. MICROCOMPUTADORAS

Una microcomputadora es un tipo de computadora que utiliza un microprocesador como unidad central de procesamiento (CPU). Generalmente son computadoras que ocupan espacios físicos pequeños, comparadas a sus predecesoras históricas, las mainframes y las minicomputadoras.

2.40.1. RESPALDOS DEL DISCO DURO

Respaldar la información contenida en el disco duro de los microcomputadores.

(PriteshGupta, El portal de ISO 27002 en Español, 2012), indica la cláusula 5.1.1 Conjunto de políticas para la seguridad de la información: "Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes."

2.40.2. PROGRAMAS ORIGINALES

Utilizar programas originales, es decir comprar las licencias respectivas para evitar problemas legales.

2.40.3. INFORMACIÓN ALMACENADA EN EL DISCO DURO

En el artículo sobre Discos Duros (Publiespe) indica: *"El disco duro (hard disk) es una unidad de almacenamiento magnético de la información. Es un disco metálico (normalmente de aluminio) recubierto con una capa de material magnetizable por sus dos caras (usualmente níquel)."*

Ilustración 1: Almacenamiento de información

El Commodore 64 fue uno de los más famosos microordenadores de su época, y el modelo mejor vendido de las computadores caseras de todos los tiempos.

2.40.4. PÓLIZA DE SEGUROS DE MICROCOMPUTADORAS

Antes de hablar de pólizas, es necesario, saber que es una **microcomputadora**, entonces en la página web (WIKIPEDIA, 2015) indica:

> *La microcomputadora es una computadora pequeña, con un microprocesador como su Unidad Central de Procesamiento (CPU). Generalmente, el microprocesador incluye los circuitos de almacenamiento (o memoria caché) y entrada/salida en el mismo circuito integrado (o chip). Las microcomputadoras se hicieron populares desde 1970 y 1980 con el surgimiento de microprocesadores más potentes. Los predecesores de estas computadoras, las supercomputadoras y las minicomputadoras, eran mucho más grandes y costosas (aunque las supercomputadoras modernas, como IBM System, utilizan uno o más microprocesadores como CPUs). Muchas microcomputadoras (cuando están equipadas con un teclado y una pantalla para entrada y salida) son también computadoras personales (en sentido general). La abreviatura micro fue comúnmente utilizada durante las décadas de 1970 y de 1980, aunque actualmente esté en desuso.*

No existe una póliza de seguros para microcomputadoras, por lo que, se sugiere contratar a la brevedad posible dicha póliza, con el fin de salvaguardar los intereses de la empresa y su inversión en este tipo de equipos.

Ilustración 2: Microcomputadoras

Una colleción de las primeras microcomputadoras: Processor Technology SOL-20, un MITS Altair 8800, a TV Typewriter, y una Apple I

Microcomputadoras

2.40.5. MANUALES DE LOS MICROCOMPUTADORES

Es responsabilidad del personal leer los manuales con instrucciones, sobretodo, acerca del cuidado de estos documentos a fin de evitar pérdidas a futuro.

Considerando que para mejorar el Control Interno, cada formulario debe contener lo siguiente:

Tabla 3: Personal responsable

REALIZADO POR: ……FECHA:……
REVISADO POR: ……FECHA:……
APROBADO POR: ……FECHA:……

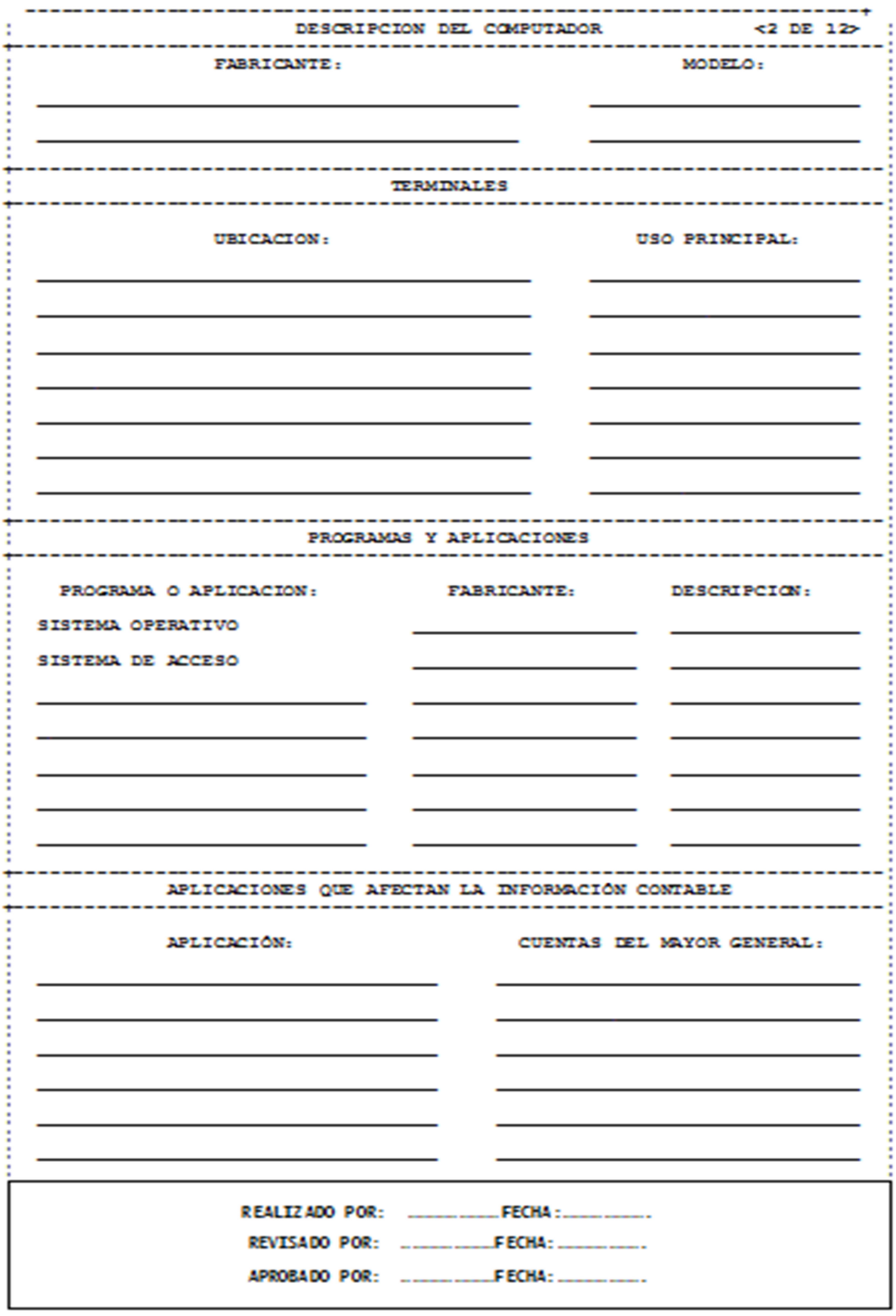
Cuestionario de Control Interno para Sistemas Computarizados

Tabla 4: Cuestionario de Control Interno para Sistemas Computarizados

CUESTIONARIO DE CONTROL INTERNO PARA SISTEMAS COMPUTARIZADOS	MQR <1 DE 12> págs.
CLIENTE : _____	PERIODO : _____
REALIZADO POR : _____	FECHA : _____
REVISADO POR : _____	FECHA : _____
APROBADO POR : _____	FECHA : _____
INSTRUCCIONES GENERALES	
OBJETIVO:	
El objetivo de este cuestionario es ayudar al auditor en la evaluación del control interno en compromisos en que usan equipos de procesamiento electrónico de datos en los procesos contables importantes.	
La evaluación de control interno del ambiente de procesamiento electrónico de datos determinará el enfoque de auditoría a seguir y la confiabilidad en los controles internos.	
Este estudio y evaluación tienen como meta el determinar la confiabilidad en los estados financieros preparados por el departamento de procesamiento electrónico de datos y ofrecer recomendaciones sobre el control interno de dicho departamento al cliente, las cuales pueden incluirse en la carta a la gerencia o en un informe independiente.	
CUANDO DEBE USARSE:	
Este cuestionario debe usarse en todos los compromisos en que se usan equipos de procesamiento electrónico de datos para llevar a cabo operaciones contables importantes. Es aplicable en compromisos donde dichos procesos se llevan a cabo ya sea en las propias instalaciones del cliente o en un servicio de cómputo externo. Su aplicación es obligatoria.	
QUIEN DEBE PREPARARLO:	
Los procedimientos descritos en este cuestionario pueden ser llevados a cabo por el contador encargado o por la colaboración de un especialista en PED. En aquellos procesos en que el contador encargado tenga dificultad, debe acudir al especialista en PED. En la aplicación de este cuestionario, se espera que cada contador aplique su juicio profesional con el fin de alcanzar los objetivos propuestos.	
COMO DEBE PREPARARSE	
Este cuestionario consta de varias preguntas las cuales tienen tres posibles respuestas; éstas son SI, NO ó N/A. Debe contestarse en el casillero correspondiente. Adicionalmente, existe una columna para incluir comentarios los que deben especificarse claramente. De ser necesario pueden añadirse a este cuestionario hojas adicionales que aclaren cualquier comentario.	
Al final de cada pregunta aparece el interrogante: "¿CARTA A LA GERENCIA?"; esto se refiere a que, a criterio de la persona que está evaluando, se debe o no incluir dicho comentario en la carta a la gerencia.	
Si fuera necesario, se pueden añadir preguntas a este cuestionario con el objetivo de aclarar la evaluación.	
ADVERTENCIA:	
Este cuestionario es de uso exclusivo de	
No puede ser reproducido ni utilizado, sin una autorización escrita por parte de los	
propietarios. DERECHOS RESERVADOS.	

Descripción del Computador

Tabla 5: Descripción del Computador



DESCRIPCION DEL COMPUTADOR <2 DE 12>

FABRICANTE: MODELO:

TERMINALES

UBICACION: USO PRINCIPAL:

PROGRAMAS Y APLICACIONES

PROGRAMA O APLICACION: FABRICANTE: DESCRIPCION:

SISTEMA OPERATIVO

SISTEMA DE ACCESO

APLICACIONES QUE AFECTAN LA INFORMACIÓN CONTABLE

APLICACIÓN: CUENTAS DEL MAYOR GENERAL:

REALIZADO POR: _____ FECHA: _____.

REVISADO POR: _____ FECHA: _____.

APROBADO POR: _____ FECHA: _____.

Seguridades y Controles Físicos

Tabla 6: Seguridades y Controles Físicos

SEGURIDADES Y CONTROLES FÍSICOS			<3 DE 12>	
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
1.¿Cuenta el sistema con un regulador de voltaje?				
¿Carta a la gerencia?				
2.Si la respuesta a la pregunta anterior es sí,¿está funcionando adecuadamente?				
¿Carta a la gerencia?				
3.¿Cuenta el sistema con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica?				
¿Carta a la gerencia?				
4.Si la respuesta a la pregunta anterior es sí, ¿está funcionando adecuadamente? Indique en observaciones cuántos minutos de energía le da al computador.				
¿Carta a la gerencia?				
5.¿Existe en el centro de cómputo un extinguidor de incendios? ¿Carta a la gerencia?				
6.Si la respuesta al pregunta anterior es sí, ¿está dentro del período de carga y con la presión adecuada?				
¿Carta a la gerencia?				
7.¿Cuenta el sistema con un equipo de aire acondicionado adecuado?				
¿Carta a la gerencia?				
8.¿Se mide con frecuencia la temperatura y la humedad?				
¿Carta a la gerencia?				
9.¿Las instalaciones de PED se encuentran en un lugar funcional?				
¿Carta a la gerencia?				
10.¿Las líneas eléctricas de PED son independientes del resto de la instalación eléctrica?				
¿Carta a la gerencia?				
11.¿Se mide con frecuencia la tensión e intensidad de la corriente eléctrica?				
¿Carta a la gerencia?				
12.¿La instalación eléctrica de PED tiene conexión a tierra?				
¿Carta a la gerencia?				
13.¿Existe algún sistema de detección de incendios?				
¿Carta a la gerencia?				
14.¿Existe algún letrero o indicador de que está prohibido fumar convenientemente escrito o difundido?				
¿Carta a la gerencia?				
15.¿Está restringido el acceso al departamento de PED?				
¿Carta a la gerencia?				
16.¿Existe algún sistema de alarma que permita detectar intrusos en el departamento PED?				
¿Carta a la gerencia?				
17.¿Tiene el departamento PED alguna puerta de escape?				
¿Carta a la gerencia?				

SEGURIDADES Y CONTROLES FÍSICOS (CONTINUACION) <4 DE 12>				
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
18.- ¿Existe algún equipo de control de acceso al departamento de PED? Si existe alguno, descríbalo brevemente en observaciones.				
¿Carta a la gerencia?				
19.- ¿Existe algún plan de seguridad o de emergencias escrito y aprobado?				
¿Carta a la gerencia?				
20.- ¿Se ha contratado alguna póliza de seguros?				
¿Carta a la gerencia?				
21.- Si la respuesta a la pregunta anterior es sí, ¿cubre ésta todo riesgo?				
¿Carta a la gerencia?				
22.- Si la respuesta a la pregunta anterior es sí, ¿cuál tipo de riesgo?				
¿Carta a la gerencia?				
23.- ¿Se limpia regularmente el centro de PED?				
¿Carta a la gerencia?				
24.- Si la respuesta a la pregunta anterior es sí, ¿se controla al personal de limpieza?				
¿Carta a la gerencia?				
25.- ¿Está alfombrado el centro de PED?				
¿Carta a la gerencia?				
26.- Si la respuesta a la pregunta anterior es sí, ¿se le ha dado algún tratamiento a la alfombra para evitar la energía estática?				
¿Carta a la gerencia?				
27.- ¿Se hace mantenimiento periódico a los equipos de computación?				
¿Carta a la gerencia?				
28.- ¿Se destruye adecuadamente todo papel, listado, etc. al que no se le va a dar uso?				
¿Carta a la gerencia?				
29.- ¿Cuenta el centro de cómputo con una destructora de papeles?				
¿Carta a la gerencia?				
30.- Si la respuesta a la pregunta anterior es sí, ¿funciona ésta adecuadamente?				
¿Carta a la gerencia?				
31.- ¿Existe algún manual o reglamento que trate acerca de la seguridad física del centro de PED?				
¿Carta a la gerencia?				
32.- ¿Existe algún tipo de librería con llave para guardar los manuales y documentación de los programas y aplicaciones?				
¿Carta a la gerencia?				
33.- ¿Se controla la entrega de dichos manuales y documentación así como la recepción de los mismos?				
¿Carta a la gerencia?				
34.- ¿Existe un inventario actualizado de los manuales y documentación de los programas y aplicaciones?				
¿Carta a la gerencia?				

SEGURIDADES Y CONTROLES FÍSICOS (CONTINUACION) <5 DE 12>				
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
35.- Si la respuesta a la pregunta anterior es sí, ¿se encuentran estas copias bajo llave y custodia?				
¿Carta a la gerencia?				
36.- ¿Están los discos, cintas y cualquier otro medio magnético convenientemente almacenados en salas o armarios especiales?				
¿Carta a la gerencia?				
37.- ¿Se guarda en una localidad distinta a la de la empresa una copia de los discos y cintas?				
¿Carta a la gerencia?				
38.- Si la respuesta a la pregunta anterior es sí, ¿se encuentran estas copias bajo llave y custodia?				
¿Carta a la gerencia?				
40.- ¿Está restringido el acceso a manuales, documentación, librerías, discos, cintas y medios magnéticos?				
¿Carta a la gerencia?				
41.- ¿Está marcado o identificado perfectamente el material confidencial?				
¿Carta a la gerencia?				
42.- ¿Se sacan suficientes copias de seguridad de los archivos principales, sobre todo los del área contable?				
¿Carta a la gerencia?				
43.- ¿Existe algún plan escrito para sacar copias de respaldo periódicamente?				
¿Carta a la gerencia?				
44.- ¿Existe un inventario actualizado de cintas y discos que permita controlar su ubicación y antigüedad?				
¿Carta a la gerencia?				
45.- ¿Se destruyen los discos y cintas que están dañados o fuera de uso?				
¿Carta a la gerencia?				
46.- ¿Existe un stock mínimo o de seguridad de los suministros (papel, cintas, discos, etc.) en el departamento de PED?				
¿Carta a la gerencia?				
47.- ¿Existe procedimientos de operación escritos para encender y apagar el computador ya sea en operaciones normales o cuando se va la energía eléctrica?				
¿Carta a la gerencia?				
48.- En caso de que el equipo sufra un daño, ¿hay la posibilidad de continuar los procesos en alguna otra institución o empresa que tenga el mismo equipo?				
¿Carta a la gerencia?				
50.- ¿Existe control adecuado sobre el uso de suministros de PED?				
¿Carta a la gerencia?				

SEGURIDADES Y CONTROLES FÍSICOS (CONTINUACION) <6 DE 12>				
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
51.- ¿Se lleva un registro adecuado de averías e interrupciones en el funcionamiento del equipo de computación?				
¿Carta a la gerencia?				
52.- ¿Se evita la operación del computador por personas no autorizadas?				
¿Carta a la gerencia?				
53.- ¿Está el centro de cómputo alejado de zonas peligrosas?				
¿Carta a la gerencia?				
54.- ¿El techo y suelo del centro de cómputo están hechos de algún material incombustible?				
¿Carta a la gerencia?				
55.- ¿Existe algún conducto de agua que atraviese el centro de PED?				
¿Carta a la gerencia?				
56.- ¿Pasan los cables de corriente eléctrica cerca de material combustible?				
¿Carta a la gerencia?				
57.- ¿Las puertas del centro de cómputo se cierran solas mediante algún mecanismo?				
¿Carta a la gerencia?				
58.- ¿Existe alguna alarma de incendios de activación manual?				
¿Carta a la gerencia?				
59.- ¿Está la información en discos y cintas magnéticas correctamente etiquetados y ordenados?				
¿Carta a la gerencia?				
60.- ¿Existe algún mecanismo de control que permita conocer a quién se le entrega la información procesada por el computador?				
¿Carta a la gerencia?				
61.- ¿Existe algún tipo de solicitud para la emisión de listados e información por parte de PED?				
¿Carta a la gerencia?				
62.- ¿Tiene la información y listados emitidos por PED una hoja de ruta que permita conocer el destino y utilización de dicha información?				
¿Carta a la gerencia?				
63.- ¿Están las ventanas del centro de cómputo protegidas contra intrusos?				
¿Carta a la gerencia?				
64.- ¿Existen cronogramas de trabajo para el uso del equipo?				
¿Carta a la gerencia?				
65.- ¿Se retienen copias de la información el tiempo necesario para satisfacer requisitos operacionales y legales?				
¿Carta a la gerencia?				
REALIZADO POR : _____ FECHA : _____				
REVISADO POR : _____ FECHA : _____				
APROBADO POR : _____ FECHA : _____				

Tabla 7: Seguridades y Controles en Programas a Aplicaciones

SEGURIDADES Y CONTROLES EN PROGRAMAS Y APLICACIONES <7 DE 12>				
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
1.- ¿Es adecuada la documentación de los programas?				
¿Carta a la gerencia?				
2.- ¿Los cambios, modificaciones o nuevos programas son autorizados antes de proceder a su realización?				
¿Carta a la gerencia?				
3.- ¿Se revisan y se prueban adecuadamente los programas antes de entregarlos a los usuarios?				
¿Carta a la gerencia?				
4.- ¿Se documenta adecuadamente cualquier cambio o modificación a un programa?				
¿Carta a la gerencia?				
5.- ¿Participan los auditores internos en el desarrollo y revisión de los programas y aplicaciones?				
¿Carta a la gerencia?				
6.- ¿Existe un plan para el desarrollo futuro de programas y aplicaciones para y la adquisición del equipo necesario para ello?				
¿Carta a la gerencia?				
7.- ¿Existen políticas en cuanto a la propiedad de datos y protección de los mismos?				
¿Carta a la gerencia?				
8.- ¿El acceso a los programas está restringido y reglamentado para el departamento de PED?				
¿Carta a la gerencia?				
9.- ¿Se preparan manuales de cada programa para el usuario?				
¿Carta a la gerencia?				
10.- ¿Se da mantenimiento a los programas y aplicaciones en forma regular?				
¿Carta a la gerencia?				
11.- ¿Están integrados los programas y aplicaciones en un todo?				
¿Carta a la gerencia?				
12.- ¿Existe una mesa de control que revise que los listados e información emitida por el computador estén correctos?				
¿Carta a la gerencia?				
13.- ¿Existen procedimientos escritos y detallados con instrucciones concretas acerca del uso de cada programa y aplicación?				
¿Carta a la gerencia?				
14.- ¿Está cada usuario o grupo de usuarios provisto de una palabra clave o código secreto de seguridad que restrinja su acceso al computador?				
¿Carta a la gerencia?				
15.- ¿Se varía con suficiente frecuencia la tabla de palabras claves secretos?				
¿Carta a la gerencia? está restringido?				
16.- ¿Se varía con suficiente frecuencia la tabla de palabras códigos secretos?				
¿Carta a la gerencia? está restringido?				
17.- ¿Existen otros procedimientos de seguridad física adicionales (llaves, tarjetas magnéticas, etc.) para restringir el acceso al computador?				
¿Carta a la gerencia?				

SEGURIDADES Y CONTROLES EN PROGRAMAS Y APLICACIONES (CONTINUACION) <8 DE 12>				
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
18.- ¿Las fallas de funcionamiento en los programas son documentadas y revisadas adecuadamente?				
¿Carta a la gerencia?				
19.- ¿Los programas y aplicaciones son autorizados por gerencia antes de ser puestos en operación?				
¿Carta a la gerencia?				
20.- ¿Existen procedimientos escritos para descargar o restaurar información al computador?				
¿Carta a la gerencia?				
21.- ¿Se controla el tiempo de utilización del computador por parte de los usuarios?				
¿Carta a la gerencia?				
22.- ¿Los documentos fuente de las transacciones son detenidos en el centro de PED?				
¿Carta a la gerencia?				
23.- ¿Emite el sistema un listado de control donde se especifique la hora, la fecha, el tiempo de utilización, los programas usados, el usuario, etc.?				
¿Carta a la gerencia?				
24.- ¿Se hacen inspecciones regulares y por sorpresa del contenido de programas y aplicaciones?				
¿Carta a la gerencia?				
25.- ¿Existen estándares establecidos para la elaboración y documentación de los programas?				
¿Carta a la gerencia?				
26.- ¿Se destruyen las pruebas de los programas?				
¿Carta a la gerencia?				
27.- ¿Existen procedimientos para probar programas modificados de manera que aseguren el no dañar a los demás?				
¿Carta a la gerencia?				
28.- ¿Hay procedimientos y controles para detectar un intento de ingresar al computador por parte de personas no autorizadas?				
¿Carta a la gerencia?				
29.- ¿Tienen acceso los usuarios a la documentación y a los programas de manera que puedan modificarlos?				
¿Carta a la gerencia?				
30.- ¿Existe algún contrato o convenio para procesar información fuera de las instalaciones del cliente?				
¿Carta a la gerencia?				

REALIZADO POR : _____ FECHA : _____

REVISADO POR : _____ FECHA : _____

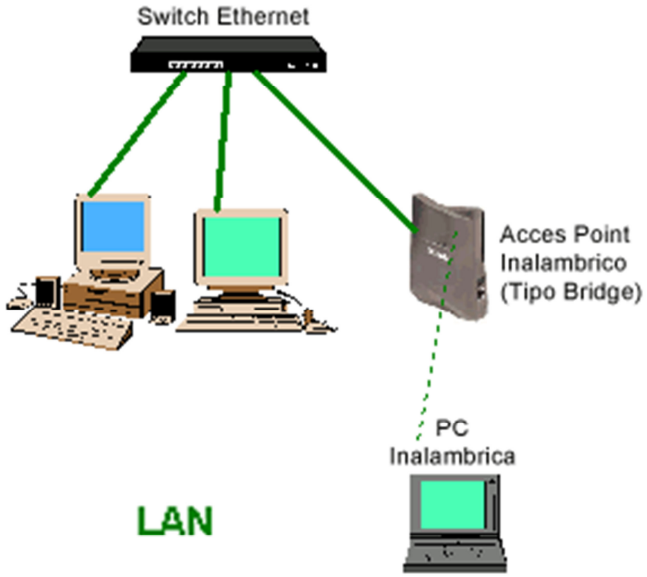
APROBADO POR : _____ FECHA : _____

Tabla 8: Seguridades y Controles en la Organización

SEGURIDADES Y CONTROLES EN LA ORGANIZACIÓN <9 DE 12>				
PREGUNTAS:	SI	NO	N/A	OBSERVACIONES:
1.- ¿Está adecuadamente organizado el departamento de PED? Elabore un organigrama.				
¿Carta a la gerencia?				
2.- ¿Existe separación de funciones y de responsabilidades en el departamento de PED?				
¿Carta a la gerencia?				
3.- ¿Se selecciona adecuadamente al personal de PED?				
¿Carta a la gerencia?				
4.- ¿Se capacita continuamente al personal de PED?				
¿Carta a la gerencia?				
5.- ¿Se motiva adecuadamente al personal de PED?				
¿Carta a la gerencia?				
6.- ¿Está el personal de operación del computador adecuadamente formado en técnicas de determinación de problemas y averías?				
¿Carta a la gerencia?				
7.- ¿Está informado el personal de seguridad sobre medidas y cuidados específicos relativos a la seguridad del departamento de PED?				
¿Carta a la gerencia?				
8.- ¿Existe un manual de organización en el cual se describa responsabilidades y posiciones del departamento de PED?				
¿Carta a la gerencia?				
9.- ¿Existen políticas para mantener la seguridad cuando termina la relación laboral con un empleado?				
¿Carta a la gerencia?				
10.- ¿Se evalúa y supervisa al personal de PED con regularidad?				
¿Carta a la gerencia?				
11.- ¿Existen políticas de vacaciones obligatorias para el personal de PED?				
¿Carta a la gerencia?				
12.- ¿Tiene auditoría interna un alcance sin restricciones para investigar cualquier aspecto referente al departamento de PED?				
¿Carta a la gerencia?				
REALIZADO POR : _____ FECHA : _____				
REVISADO POR : _____ FECHA : _____				
APROBADO POR : _____ FECHA : _____				

DIAGRAMAS <10 DE 12>

Ilustración 3: Organigrama de Ped



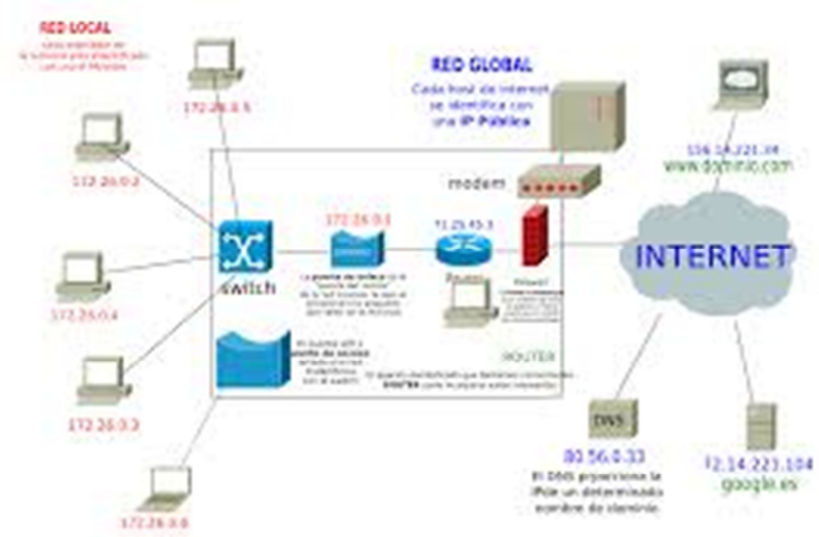
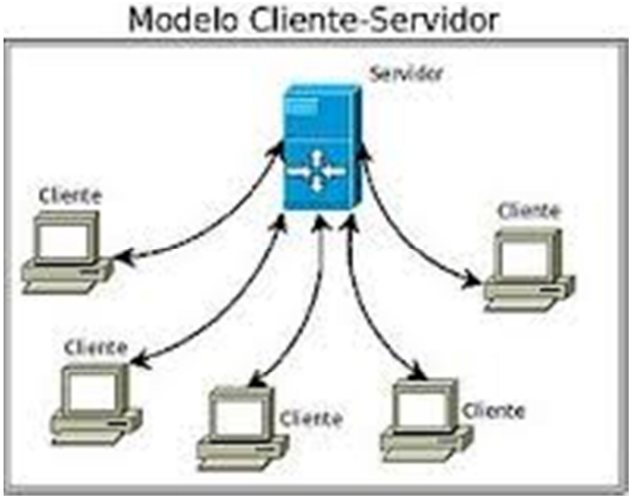


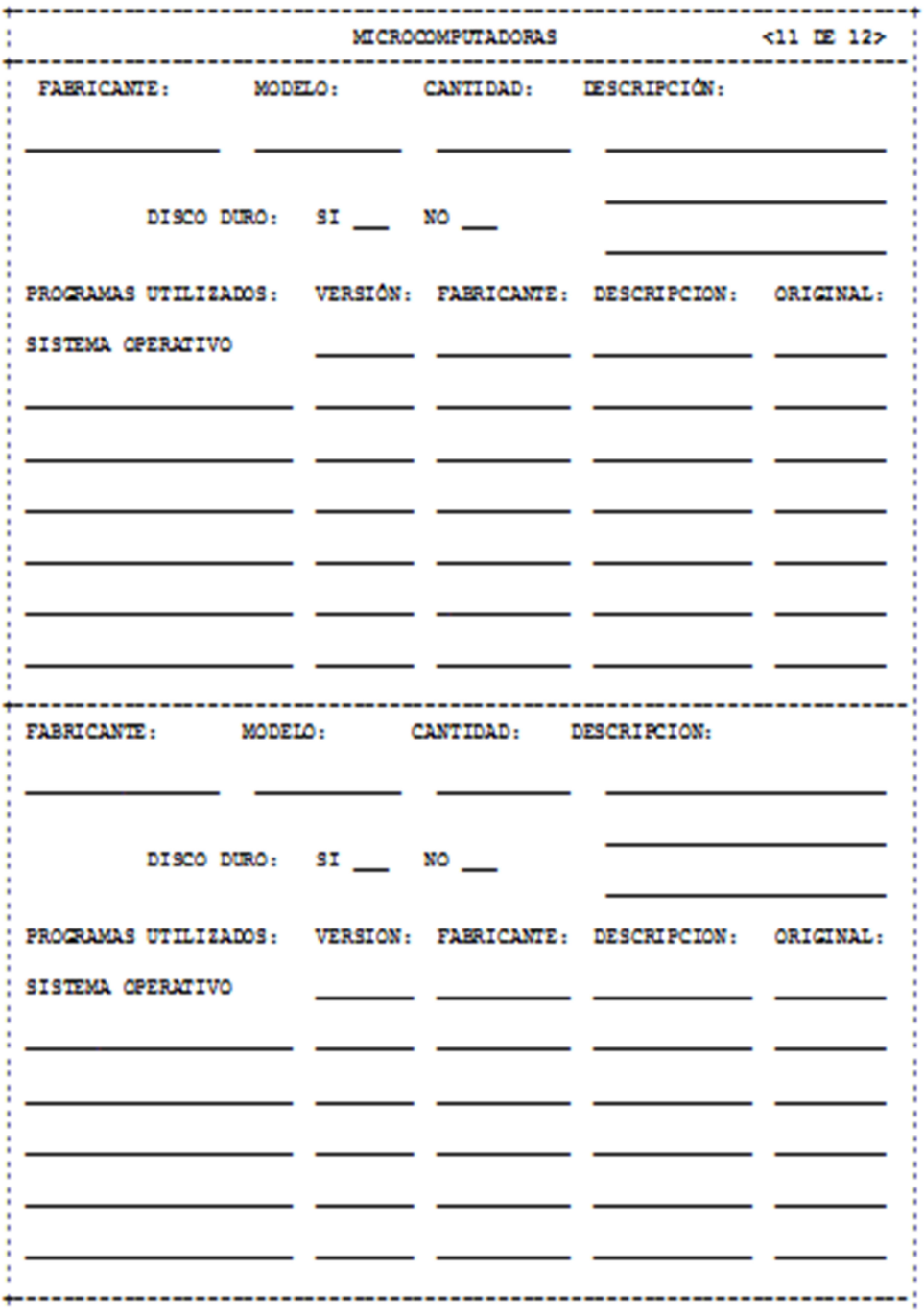
Ilustración 4: Computadoras Terminales

Ilustración 5: Modelo Cliente - Servidor



Formulario de Registro de Microcomputadoras

Tabla 9: Formulario de Registro de Microcomputadoras



MICROCOMPUTADORAS <11 DE 12>

FABRICANTE: MODELO: CANTIDAD: DESCRIPCIÓN:

DISCO DURO: SI ___ NO ___

PROGRAMAS UTILIZADOS:	VERSIÓN:	FABRICANTE:	DESCRIPCION:	ORIGINAL:
SISTEMA OPERATIVO				

FABRICANTE: MODELO: CANTIDAD: DESCRIPCION:

DISCO DURO: SI ___ NO ___

PROGRAMAS UTILIZADOS:	VERSION:	FABRICANTE:	DESCRIPCION:	ORIGINAL:
SISTEMA OPERATIVO				

MICROCOMPUTADORAS <12 DE 12>

FABRICANTE:	MODELO:	CANTIDAD:	DESCRIPCION:

DISCO DURO: SI ___ NO ___

PROGRAMAS UTILIZADOS:	VERSION:	FABRICANTE:	DESCRIPCION:	ORIGINAL:
SISTEMA OPERATIVO				

FABRICANTE:	MODELO:	CANTIDAD:	DESCRIPCION:

DISCO DURO: SI ___ NO ___

PROGRAMAS UTILIZADOS:	VERSION:	FABRICANTE:	DESCRIPCION:	ORIGINAL:
SISTEMA OPERATIVO				

REALIZADO POR: _____FECHA:_____.

REVISADO POR: _____FECHA:_____.

APROBADO POR: _____FECHA:_____.

OBSERVACIONES:

REALIZADO POR: _____FECHA:_____.

REVISADO POR: _____FECHA:_____.

APROBADO POR: _____FECHA:_____.

3. GLOSARIO

1. **Algoritmo:** Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema

2. **Árbol:** En ciencias de la informática, un árbol es una estructura de datos ampliamente usada que imita la forma de un árbol (un conjunto de nodos conectados).

3. **Árbol binario:** Un árbol binario es una estructura de datos en la cual cada nodo siempre tiene un hijo izquierdo y un hijo derecho. No pueden tener más de dos hijos (de ahí el nombre "binario").

4. **Arquitectura de Computadores:** Trata del diseño interno de los componentes de un computador y la comunicación entre ellos en un lenguaje llamado ensamblador, que es el lenguaje propio de la máquina

5. **Auditoría de sistemas informáticos:** examen riguroso al sistema con el fin de evaluar su situación.

6. **Antivirus:** programas cuyo objetivo es detectar y/o eliminar virus informáticos.

7. **Archivos:** conjunto de bits almacenado en un dispositivo.

8. **Aplicaciones:** Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo.

9. **Base de Datos:** Un banco de datos similar a una biblioteca que contiene documentos y textos indexados para su consulta, pero esta base de datos tiene un formato electrónico, que ofrece muchas más soluciones al problema de almacenar datos.

10. **BIOS:** un programa registrado en una memoria no volátil (antiguamente en memorias ROM, pero desde hace tiempo se emplean memorias flash). Este programa es específico de la placa base y se encarga de la interfaz de bajo nivel entre el microprocesador y algunos periféricos. Recupera, y después ejecuta, las instrucciones del MBR (Master Boot Record), o registradas en un disco duro o SSD, cuando arranca el sistema operativo.

11. **Bit:** (acrónimo: Binary digit. En inglés Dígito Binario.) Un bit es un dígito del sistema de numeración binario.

12. **Byte:** secuencia de bits contiguos, equivalente a un octeto, es decir, a ocho Bits)

13. **Blog:** Bitácora digital o bitácora, es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente.

14. **Computación:** Básicamente, el tratamiento de la información, mediante un computador.

15. **CD-ROM:**(En inglés: Compact Disc - Read Only Memory) Es un prensado disco compacto que contiene los datos de acceso, pero sin permisos de escritura, un equipo de almacenamiento y reproducción de música.

16. **Compiladores:** Son aquellos programas que traducen órdenes de un usuario, mediante un programa computacional o una orden dada por consola, que están conformados por letras y números, a un lenguaje de máquina conformado por secuencias de impulsos eléctricos.

17. **Computación para las Ciencias:** Rama de la computación orientada al desarrollo de modelos matemáticos y computacionales que representan problemas científicos o tecnológicos, para su manipulación y control.

18. **CD-RW:**(En inglés: Compact Disc ReWritable) Es un soporte digital óptico utilizado para almacenar cualquier tipo de información. Este tipo de CD puede ser grabado múltiples veces, ya que permite que los datos almacenados sean borrados.

19. **Cintas Magnéticas:** Es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato. El tipo de información que se puede almacenar en las cintas magnéticas es variado, como vídeo, audio y datos.

20. **Circuitos Integrados:** Es conocido como chip o microchip, es una pastilla pequeña de material semiconductor, de algunos milímetros cuadrados de área, sobre la que se fabrican circuitos electrónicos generalmente mediante fotolitografía y que está protegida dentro de un encapsulado de plástico o cerámica.

21. **Complemento o Plug-in:** Es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica.

22. **Computador:** También denominada ordenador, es una máquina electrónica que recibe y procesa datos para convertirlos en información útil

23. **CPU (Unidad Central de Procesos):**(Acrónimo en inglés de central processing unit), Conocido como procesador o microprocesador, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

24. **Dato:** El dato es una representación simbólica (numérica, alfabética, algorítmica etc.), un atributo o una característica de una entidad

25. **Depuración de programas:** es el proceso de identificar y corregir errores de programación. En inglés se le conoce como debugging, ya que se asemeja a la eliminación de bichos (bugs), manera en que se conoce informalmente a los errores de programación.

26. **Diagrama de flujo (Tipo de Algoritmo):** Es una representación gráfica de un algoritmo o proceso.

27. **Dirección IP:** Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

28. **Disco Duro:** (En inglés Hard Disk Drive, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales.

29. **Disco Óptico:** Es un formato de almacenamiento de datos digital, que consiste en un disco circular en el cual la información se codifica, se guarda y almacena, haciendo unos surcos microscópicos con un láser sobre una de las caras planas que lo componen.

30. **Dispositivos:** Son componentes que leen o escriben datos en medios o soportes de almacenamiento, y juntos conforman la memoria o almacenamiento secundario de la computadora.

31. **DVD:** (En inglés Digital Versatile Disc) (DiscoVersátil Digital) Es un disco óptico de almacenamiento de datos.

32. **DVD-RW:** Es un DVD regrabable en el que se puede grabar y borrar la información varias veces. La capacidad estándar es de 4,7 GB.

33. **Enlaces:** el enlace, un navegador web de código abierto en modo de texto.

34. **Estructuras de datos:** Relativo a cómo se ordenan u organizan los datos en computador para ser utilizados por los programas computacionales.

35. **Gadget:** Es un dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso.

36. **GPU (Unidad de Procesamiento Gráfico):** (Acrónimo del inglés graphics processing unit) es un procesador dedicado al procesamiento de gráficos u operaciones de coma flotante, para aligerar la carga de trabajo del procesador central en aplicaciones como los videojuegos y/o aplicaciones 3D interactivas.

37. **Graficar por Computadora:** Campo de la informática visual, donde se utilizan computadoras para generar imágenes visuales sintéticamente o manejar la información visual y espacial obtenida del mundo real.

38. **Hardware:** Soporte físico del sistema computacional., todo lo tangible del computador, corresponde al Hardware.

39. **Hipervínculo:** Es un elemento de un documento electrónico que hace referencia a otro recurso, por ejemplo, otro documento o un punto específico del mismo o de otro documento.

40. **Ícono:** Es una imagen, cuadro o representación; es un signo que sustituye al objeto mediante su significación, representación o por analogía, como en la semiótica.

41. **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

42. **Informática:** es el estudio de la computación y métodos para el procesamiento de datos.

43. **Internet:** Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

44. **Intranet:** Es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

45. **Ingeniería de Software:** Asignatura que introduce en los métodos y técnicas para la creación de *software así como el empleo de herramientas de apoyo para cada etapa de su creación.

46. **Ingeniería de Software:** Asignatura que introduce en los métodos y técnicas para la creación de *software así como el empleo de herramientas de apoyo para cada etapa de su creación

47. **Inteligencia Artificial:** Ciencia que intenta la creación de programas para máquinas que imiten el comportamiento y la comprensión humana.

48. **KDD:** (Knowledge Discovery from Databases) es el proceso no trivial de identi car patrones válidos, novedosos, potencialmente útiles y en última instancia, comprensibles a partir de los datos.

49. **Lenguaje de Programación:** Lenguaje que intenta estar relativamente próximo al lenguaje humano o natural y enlazar con las computadoras que operan siguiendo las indicaciones de programas escritos en lenguaje de máquina, que es un sistema de códigos que la máquina interpreta directamente y lleva a cabo las acciones solicitadas.

50. **Lenguaje Ensamblador:** (En inglés assembly language) es un lenguaje de programación de bajo nivel para los computadores, microprocesadores, microcontroladores, y otros circuitos integrados programables.
51. **Links:** Es un navegador web de código abierto en modo texto —y gráfico a partir de su versión 2 en modo terminal.

52. **LOOP:** Es una sentencia que se realiza repetidas veces a un trozo aislado de código, hasta que la condición asignada a dicho bucle deje de cumplirse.

53. **Malware:** (En inglés Malicius Software) Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

54. **Memoria:** También llamada almacenamiento, se refiere a parte de los componentes que forman parte de una computadora. Son dispositivos que retienen datos informáticos durante algún intervalo de tiempo.

55. **Memoria Caché:** Un caché es un sistema especial de almacenamiento de alta velocidad. Puede ser tanto un área reservada de la memoria principal como un dispositivo de almacenamiento de alta velocidad independiente.

56. **Memoria RAM:** (Acrónimo: Random Acces Memory, memoria de acceso aleatorio) Es un memoria volátil, no permanente, corresponde a la memoria de trabajo que almacena los datos hasta su proceso o bien hasta que son destino a una memoria secundaria.

57. **Memoria ROM:** (Acrónimo: de read-only memory) Es una memoria de lectura de carácter permanente del fabricante de la placa madre, almacena datos de arranque y verificación de los dispositivos del Pc, no puede ser alterado y es físicamente un chip.

58. **Memoria Volátil:** Es aquella memoria cuya información se pierde al interrumpirse la energía eléctrica.

59. **Memoria No Volátil:** Es aquella memoria cuya información se pierde al interrumpirse la energía eléctrica.

60. **Microcontrolador:** es un circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria.

61. **Microprocesador:** Es el circuito integrado central y más complejo de un sistema informático; a modo de ilustración, se le suele asociar por analogía como el «cerebro» de un computador.

62. **Microsoft:** Empresa multinacional que desarrolla, fabrica, licencia y produce software y equipos electrónicos, siendo sus productos más usados el sistema operativo Microsoft Windows y la suite Microsoft Office, los cuales tienen una importante posición entre los ordenadores personales.

63. **Mouse:** Es un dispositivo apuntador utilizado para facilitar el manejo de un entorno gráfico en una computadora.

64. **Multimedia:** Se refiere a cualquier objeto o sistema que utiliza múltiples medios de expresión (físicos o digitales) para presentar o comunicar información. De allí la expresión «multimedios». Los medios pueden ser variados, desde texto e imágenes, hasta animación, sonido, video, etc.

65. **Minería de Datos:** Estudio de algoritmos para buscar y procesar información en documentos y bases de datos, muy relacionada con la adquisición de información

66. **Navegador Web:** Es una aplicación que opera a través de Internet, interpretando la información de archivos y sitios web para que podamos ser capaces de leerla, (ya se encuentre ésta alojada en un servidor dentro de la World Wide Web o en un servidor local).

67. **Netbook:** Es una categoría de ordenador portátil de bajo costo y generalmente reducidas dimensiones, lo cual aporta una mayor movilidad y autonomía.

68. **Notebook:** Un ordenador portátil es un ordenador personal móvil o transportable, que pesa normalmente entre 1 y 3 kg.

69. **Página Web:** Es el nombre de un documento o información electrónica adaptada para la World Wide Web y que puede ser accedida mediante un navegador para mostrarse en un monitor de computadora o dispositivo móvil.

70. **PC (Computador Personal):** (sigla en inglés de personal computer), es una microcomputadora diseñada en principio para ser usada por una sola persona a la vez.

71. **Periféricos:** Son aparatos o dispositivos auxiliares e independientes conectados a la unidad central de procesamiento de una computadora.

72. **Procesos Paralelos y Distribuidos:** Son modelos para resolver problemas de computación masiva, utilizando una organización conformada por un gran número de ordenadores.

73. **Programación:** es el proceso de diseñar, escribir, depurar y mantener el código fuente de programas computacionales

74. **Protocolos:** Reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre un sitio y otro. Estos son programas computacionales o dispositivos electrónicos que interactúan en el camino de comunicación.

75. **Pseudocódigo:** el pseudocódigo (o falso lenguaje) es una descripción de un algoritmo de programación informático de alto nivel compacto e informal que utiliza las convenciones estructurales de un lenguaje de programación verdadero, pero que está diseñado para la lectura humana en lugar de la lectura en máquina, y con independencia de cualquier otro lenguaje de programación

76. **Queue:** Conjunto de paquetes en espera de ser procesados

77. **RAM:** Memoria de acceso aleatorio, cuyo acrónimo es RAM, en inglés: random-access memory; es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

78. **Recursividad:** es la forma en la cual se especifica un proceso basado en su propia definición.

79. **Redes de Computadores:** Conjunto de dos o más computadoras de diferentes tipos y tecnologías interconectadas entre sí.

80. **Robótica:** Estudio del diseño y construcción de máquinas capaces de desempeñar tareas físicas realizadas por el ser humano o que requieren del uso de inteligencia.

81. **Simulación:** Representación del funcionamiento de un sistema por otro. Por ejemplo, la representación de un sistema físico por un modelo matemático.

82. **Sistemas Computacionales:** conjunto de *Hardware y *Software.

83. **Sistemas de Numeración:** es un conjunto de símbolos y reglas que se utilizan para la representación de datos numéricos o cantidades. Cada sistema de numeración se va a caracterizar por su base que es el número de cada símbolo distinto que utiliza, y además determina el valor de cada símbolo, dependiendo de la posición que ocupe.

84. **Sistemas Digitales:** Análisis y diseño de circuitos lógicos que conforman el sistema computacional. Son circuitos que funcionan basados en la lógica matemática.

85. **Sistemas Expertos:** Son programas de ordenador que tienen el mismo nivel de conocimientos que un experto humano sobre un tema particular y extraen conclusiones razonadas sobre un grupo de conocimientos y son capaces de comunicar al usuario, la línea de razonamiento seguida.

86. **Sistemas Operativos:** Software o conjunto de programas dedicados al funcionamiento interno del computador e interpretación de las órdenes dadas por el usuario.
87. **Software:** Programas y datos del sistema computacional.

88. **Software de aplicación:** Programas orientados a la realización de una determinada tarea de interés del usuario, tal como programas procesadores de textos, programas financieros, científicos, tecnológicos, etc.

89. **Software de Base:** Programas computacionales cuya labor es atender tareas de funcionamiento del computador.

90. **Stack (pila):** Conjunto de elementos de memoria, organizados en pila, para guardar una información transitoria, como las direcciones de retorno de las sub-rutinas; por extensión, zona de memoria para guardar información transitoria.

91. **Teoría de Autómata & lenguajes formales:** Estudio de los lenguajes formales, características y clasificación de sus gramáticas y construcción de programas autómatas que son programas capaces de reconocer dichos lenguajes, fundamental para comprender los principios de funcionamiento de los *compiladores e intérpretes.

92. **UAL (Unidad Aritmética Lógica):** Es un circuito digital que calcula operaciones aritméticas (como suma, resta, multiplicación, etc.) y operaciones lógicas (si, y, o, no), entre dos números.

93. **UC (Unidad de Control):** Su función es buscar las instrucciones en la memoria principal, decodificarlas (interpretación) y ejecutarlas, empleando para ello la unidad de proceso.

94. **UMP (Unidad de Memoria Principal):** Realiza la sesión de trabajo. Es una unidad dividida en celdas que se identifican mediante una dirección.

95. **UMS (Unidad de Memoria Secundaria):** Es el conjunto de dispositivos (aparatos) y medios (soportes) de almacenamiento, que conforman el subsistema de memoria de una computadora, junto a la memoria principal.

96. **Unidad de Disco Óptico:** Es un formato de almacenamiento de datos digital, que consiste en un disco circular en el cual la información se codifica, se guarda y almacena, haciendo unos surcos microscópicos con un láser sobre una de las caras planas que lo componen.

97. **USB:** (En inglés: Universal Serial Bus) (bus universal en serie), abreviado comúnmente USB, es un puerto que sirve para conectar periféricos a un ordenador.

98. **Usuario:** Es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina, un programa, etc.

99. **Variables:** las variables son espacios reservados en la memoria que, como su nombre indica, pueden cambiar de contenido a lo largo de la ejecución de un programa. Una variable corresponde a un área reservada en la memoria principal del ordenador pudiendo ser de longitud fija o variable.

100. **Windows:** es el nombre de una familia de sistemas operativos desarrollados por Microsoft

4. PREGUNTAS

1. ¿Para qué está diseñado el manual de técnicas para la auditoría informática?

   _____
   _____
   _____

2. Indique 2 objetivos del manual de técnicas para la auditoría informática

   _____
   _____
   _____

3. ¿En la ubicación del entorno informático cuales son las tres áreas claves de labor?

   _____
   _____
   _____

4. ¿Explique en sus propias palabras las normas generales para reportar los daños en un equipo informático?

   _____
   _____
   _____

5. ¿Enumere los responsables del traslado de los equipos informáticos dentro de las instalaciones de trabajo?

   _____
   _____
   _____

6. ¿Cómo aplicaría usted seguridades generales a los equipos informáticos de la empresa?

   _____
   _____
   _____

7. ¿Enumere dos prohibiciones que comúnmente aplican las empresas a sus trabajadores en el uso de equipos informáticos?

   _____
   _____
   _____

8. Cuál es el alcance de la responsabilidad que tiene un auditor cuando realiza una auditoría informática?

   _____
   _____
   _____

9. Cuáles son las etapas del proceso de una auditoría informática?

   _____
   _____
   _____

10. Cuáles son las características que debe poseer un auditor informático?

    _____
    _____
    _____

11. En que nos ayuda tener un respaldo del sistema, una imagen o copia exacta del disco duro?

    _____
    _____
    _____

12. Porque es importante el determinar el tiempo de utilización del computador por parte de los usuarios?

    _____
    _____
    _____

13. Mantener un control de fallas de funcionamiento de programas y aplicaciones en que ayuda a las empresas?

_____
_____
_____

14. ¿Cuáles son las características personales que debe poseer un auditor informático dentro del Departamento de procesamiento electrónico de datos?

_____
_____

15. ¿Qué se recomienda utilizar para asegurar el ingreso solo de personal autorizado al departamento de P.E.D.?

_____
_____
_____

16. ¿Qué procedimientos y normas se debe considerar para definir y establecer un adecuado plan de seguridad y emergencia?

_____
_____
_____

17. ¿Qué se deberá considerar para el manejo, inventario y control de manuales dentro del departamento de P.E.D.?.

_____
_____

5. BIBLIOGRAFÍA

- Piattinni, G. M & Peso del E. Auditoría Informática. Un enfoque práctico. Alfaomega.
- ALONSO RIVAS, GONZALO Auditoria Informática. Díaz de Santos. Madrid 1998. 187 págs.
- JUAN RIVAS, ANTONIO DE y PÉREZ PASCUAL, AURORA. La Auditoria en el desarrollo de Proyectos Informáticos. Díaz de Santos. Madrid 1998. 178 págs.
- MILLS, DAVID. Manual de Auditoria de la calidad. Gestión 2000. Barcelona 1997. 242 págs.
- PIATTINIVELTHUIS, MARIO y OTROS. Auditing Information Systems. Idea Group Publishing. Hershey, London 2000. 246 págs.
- PIATTINIVELTHUIS, MARIO y DEL PESO NAVARRO EMILIO (Editores) Auditoria Informática: Un enfoque práctico. Alfaomega. México 1998. 609 págs. PIATTINIVELTHUIS, MARIO y DEL
- PIATTINIVELTHUIS, MARIO y DEL PESO NAVARRO EMILIO (Editores) Auditoria Informática: Un enfoque práctico (2ª Edición).Ra-ma. Madrid 2001. 660 págs.
- PLANS, JOSE La práctica de la Auditoria Informática. Instituto de Censores Jurados de Cuentas de España. Madrid 1986. 159 págs.
- THOMAS, A.J. y DOUGLAS I. J. Auditoria Informática. Paraninfo. Madrid 1987. 214 págs.
- http://www.slideshare.net/Andrea_Mendoza/manual-auditoria-de-sistemas- informatica1
- LIBRO: AUDITORÍA EN SISTEMAS COMPUTACIONALES, Pearson Education Auditoría en Sistemas Computacionales Carlos Muñoz Razo Pearson Pentice Hall. www.gubiz.com/ Articulo.aspx?id=502174001278
- http://fec.uh.cu/CUGIO/1%20acciones/ProyectosProtocolos/15/Mireya%20Benchardl.pdf
- http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/tecnicas_auditoria.pdf
- http://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf
- http://www.aecid.org.ar/administrador/imagenes/auditoria%20de%20sistemas.pepepe.pdf
- Echenique García, J. A. Auditoría en Informática. México: MacGraw-Hill.

- Eumed.net. (s.f.). Eumed.net. Recuperado el 26 de Julio de 2015, de Eumed.net: http://www.eumed.net/libros-gratis

- Guachi Aucapiña, T. V. (07 de 2012). Repositorio Universidad Tecnica de Ambato. Obtenido de http://repositorio.uta.edu.ec/handle/123456789/2361

- ISO/IEC 17799. (15 de Junio de 2005). Tecnología de la Información – Técnicas de seguridad- Código para la práctica de la gestión de la seguridad de la información. Tecnología de la Información – Técnicas de seguridad- Código para la práctica de la gestión de la seguridad de la información .

- Moore Stephens Suarez &Menendez. (s.f.). www.suarez-menendez.com. Recuperado el 25 de Julio de 2015, de www.suarez-menendez.com: http://www.suarez-menendez.com

- PriteshGupta. (2012). El portal de ISO 27002 en Espanol. Obtenido de http://www.iso27000.es/iso27002.html

- PriteshGupta. (2012). El portal de ISO 27002 en Español. Obtenido de http://www.iso27000.es/iso27002_7.html

- PriteshGupta. (2012). El portal de ISO 27002 en Español. Obtenido de http://www.iso27000.es/iso27002_5.html

- Publiespe. (s.f.). Publiespe. Recuperado el 3 de Agosto de 2015, de Publiespe: http://publiespe.espe.edu.ec/articulos/sistemas/disco-duro/disco-duro.htm

- WIKIPEDIA. (22 de Junio de 2015). WIKIPEDIA. Recuperado el 3 de Agosto de 2015, de WIKIPEDIA: https://es.wikipedia.org/wiki/Microcomputadora