CONTRALORIA GENERAL DE LA REPUBLICA

MANUAL DE AUDITORIA GUBERNAMENTAL

PARTE Nº VIII

AUDITORIA INFORMATICA

PROYECTO BID/CGR

MANAGUA – NICARAGUA
JULIO, 2009

I N D I C E

CAPITULO XXVI
VISION GENERAL DE LA AUDITORIA INFORMATICA

Capítulo XXVI
Visión General de la Auditoría Informática

La auditoría informática como técnica y herramienta de apoyo a la Organización, ha facilitado en las últimas décadas el desarrollo en el área de Sistemas, debido al auge que han tenido en estos últimos años. La Información cada vez va teniendo más realce, y se le va considerando como un activo intangible, irrecuperable e invaluable. Esta preocupación internacional ha llevado a que grandes peritos en el tema, dediquen horas de trabajo, análisis y estudio a realizar inventos que permitan el almacenamiento de los datos, acceso rápido a ellos y recuperación, entre otras

La Auditoría informática también conocida como Auditorías de Sistemas de Información es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática comprende no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La Auditoría informática debe ser realizada por un Auditor de Sistemas, miembro especialista del personal profesional designado para la ejecución de la auditoría, para ello debe tener entrenamiento apropiado y experiencias en ambientes complejos de computación, lo que en su actuación esta regulado muy estrechamente con las normas éticas de la OLACEF e INTOSAI que a nivel global están enmarcado a la fiscalización gubernamental en Centroamérica, y los asuntos relacionados tiene temas como:

- Identificación y estimación de riesgos relacionados con procesos computarizados.
- Identificación y pruebas de los controles del Computador.
- Diseño, desarrollo y utilización de técnicas de interrogación de archivos. (ACL, IDEA, CAP)
- Aplicación en estas áreas de estándares de auditorias relevantes y del enfoque de auditoria.

Un Auditor de Sistemas debe participar en las siguientes actividades de auditoria:

- Comprensión del proceso contable, incluyendo la obtención y evaluación de información que nosotros usamos para comprender el ambiente de computación y la estructura de control del computador.

- Identificación y pruebas de los controles del computador.

- Diseño de pruebas de controles y pruebas sustantivas en los sistemas de información. Ejemplo: pruebas de la integración de ingresos utilizando la pantalla del computador del cliente, dado que el cliente no imprime de forma rutinaria las historias o estados de sus ingresos en un determinado período.

1. Concepto

Consiste en el examen objetivo, crítico, sistemático y selectivo de las políticas, normas, prácticas, procedimientos y procesos, para dictaminar respecto a la economía, eficiencia y eficacia de la utilización de los recursos de tecnologías de la información, la oportunidad, confiabilidad, validez de la información y la efectividad del sistema de control interno asociado a las tecnologías de la información y a la entidad en general.

La auditoría Informática consiste en el examen de los procesos y sistemas con la finalidad de emitir una opinión sobre los procesos claves de control de los sistemas informáticos, utilizando como criterios de comparación los Principios Generales y Normas Básicas de Controles Estándares, disposiciones legales, reglamentarias, normativas y/o políticas aplicables a la Entidad u Organismo auditado, así como la evaluación de la efectividad de sus sistemas de información que integran y conforman el control interno computarizado.

2. Objetivos

La auditoría en informática es 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 debe evaluar todo (informática, organización de centros de información, hardware y software).

El objetivo general de la auditoría informática recae en emitir una opinión sobre los procesos claves de control de los sistemas informáticos, utilizando como criterios de comparación los Principios Generales y Normas Básicas de Controles Estándares, disposiciones legales, reglamentarias, normativas y/o políticas aplicables a la Entidad u Organismo auditado, así como la evaluación de a efectividad de sus sistemas de información que integran y conforman el control interno computarizado.

Los objetivos generales de la auditoria de tecnologías de la información, son:

•Comprobar el control interno de la entidad, verificando sus puntos fuertes y débiles.

•Verificar el cumplimiento de las políticas, normas y procedimientos que rigen las tecnologías de la información.

•Comprobar una seguridad razonable de los recursos (datos, tecnologías, instalaciones, personal y aplicaciones), cumpliendo con los objetivos de control y los objetivos generales del negocio.

•Comprobar si la información que se procesa es oportuna y confiable.

•Verificar el grado de privacidad del ambiente informático.

•Presentación de un informe para dar a conocer los resultados y recomendaciones.

Comprende la revisión de los controles técnicos de gestión informática referente a la seguridad, explotación de la información, interoperatividad entre sistemas, desarrollo, comunicaciones e infraestructura de tecnología.

a. Operatividad: Que el mínimo de maquinaria y sistemas informáticos se encuentren en buen funcionamiento.

b. Verificación de la observancia de las normas teóricamente existentes en el departamento de informática y su coherencia con el resto de la empresa. Aplicando:

   b.1 Las Normas Generales de la Instalación Informática: Registrar las áreas que carezcan de normatividad. Se revisa que la normatividad informática general no sea contradictoria con la Normal general de la Empresa.

   b.2 Los Procedimientos Generales Informáticos: Se verificará su existencia, al menos en los sectores más importantes.

   b.3 Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales

3. Normas de Auditoría

Las Normas de Auditoría Gubernamental de Nicaragua establecen los principios, normas generales y básicas de control interno gubernamental, emitidas bajo el enfoque proporcionado por normas de auditoría de aplicación en el ámbito OLACEFS, el Comité de Organizaciones Coauspiciadoras del Marco Integrado de Control Interno de la Comisión Treadway (COSO) que se complementa con el Marco de Referencia de Objetivos de Control y Tecnología Relacionada (COBIT), precisamente para contar con un modelo integral de control sobre la tecnología de información, que apoye a los procesos de auditoría en un marco de prácticas sanas en materia de control y seguridad

En auditoría Informática se deberán aplicar las NAGUN 2.10 a 2.90 correspondiente a las normas aplicables a todo tipo de auditoría así como las Normas específicas de Auditoría Informática NAGUN 10.10 a NAGUN 10.30

4. Proceso de Auditoría Informática

Es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones; la revisión analítica a la suficiencia de controles establecidos en el ámbito informático, con la finalidad de disminuir los riesgos y garantizar la seguridad, confiabilidad y exactitud de la información.

Como toda auditoría, se lleva a cabo en tres fases generales denominada planeación, ejecución (trabajo de campo) y comunicación de resultados. (Informes); en cada una de esas fases se ejecutan una serie de actividades, labores y tareas, las que serán tratadas en el presente Manual.

a) Planeación de la auditoría:

   Su objetivo es obtener un conocimiento de la Entidad u Organismo sobre cómo operan los sistemas de información que se han de incluir en la revisión y el ambiente de control en cuanto a ¡as fuentes de información, evaluación de riesgos inherente al control e identificación de controles claves, para definir el enfoque de auditoría que se aplicará, determinar los procedimientos de auditoría específicos a realizar, seleccionar el personal, determinar tiempo y costo y preparar los programas de auditoría respectivos.

b) Ejecución del plan:

   Su objetivo es la aplicación de las técnicas de auditoría asistidas por computador, procedimientos de pruebas y evaluación de controles para los riesgos de aplicación y del Centro de Cómputo o áreas de informática.

c) Conclusión y preparación de informe:

   Su objetivo es obtener una conclusión general de la auditoría realizada por lo que el informe debe contener:

   -Objetivos de auditoría cubiertos;
   -Naturaleza y alcance de los procedimientos aplicados;
   -Hallazgos detectados y recomendaciones de auditoría;
   -Comentarios de los Funcionarios de la Entidad u Organismo;
   -Conclusión.

CAPITULO XXVII
PLANEACION Y PROGRAMACION DE AUDITORIA

Capítulo XXVII
Planeación y programación de la auditoría

El plan de auditoría debe estar basado en la comprensión de las actividades de las entidades, sus sistemas de administración y control, la naturaleza de las transacciones que realiza y las leyes y reglamentos que le aplican. Debe ser documentado como parte integral de los papeles de trabajo y modificado, cuando sea necesario durante el transcurso de la auditoria.

La planeación es imprescindible para todo tipo de trabajo, cualquiera sea su tamaño. Sin una adecuada planeación es prácticamente imposible obtener efectividad y eficiencia en la ejecución de los trabajos, debe ser cuidadosa y creativa, positiva e imaginativa y tener en cuenta alternativas para realizar las tareas, seleccionando lo métodos más apropiados, es decir, determinando un enfoque de auditoría adecuado y práctico, acorde con las circunstancias.

Las Normas de Auditorías Gubernamentales de Nicaragua (NAGUN) establecen que "Para cada auditoría se elaborará un plan de trabajo específico" y en lo particular a la auditoría Informática indican:

NAGUN 10.10

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

a) Evaluación de los sistemas y procedimientos.
b) Evaluación de los equipos de cómputo.

1. Para que un proceso de auditoría de tecnología de la información tenga éxito debe comenzar por obtener un diagnostico con información verdadera y a tiempo de lo que sucede en la organización bajo análisis, esta obtención de la información debe ser planeada en forma estructurada para garantizar una generación de datos que ayuden posteriormente su análisis. Es un ciclo continuo en el cual se planea la recolección de datos, se analiza, se retroalimentan y se da un seguimiento.

2. Se deberá obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

3. Se deberá obtener una comprensión suficiente del ambiente total que revisará. Este conocimiento debe incluir una comprensión general de las diversas prácticas, el diseño conceptual, políticas de gestión, formas de registro, niveles de seguridad y uso de las comunicaciones para la gestión de la información y funciones de la auditoría, así como los tipos de sistemas de información que se utilizan.

El proceso de planeación comprende las siguientes etapas:

1. Planeación Previa
2. Evaluación de los sistemas
3. Comprensión del Control interno
4. Desarrollo de la estrategia de la auditoria
5. Personal
6. Programas de auditoría

1. Planeación previa

Dentro del proceso de planeación se debe obtener o actualizar el conocimiento acerca de la actividad de la Entidad u Organismo para establecer:

a) Alcance de trabajo;
b) Actividad y riesgo inherente computarizados;
d) Ambiente de control;
e) Políticas significativas.

Se deberá efectuar una investigación preliminar para observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

Administración:

Se recopila la información para obtener una visión general del área de informática por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances de la auditoría.

La información a solicitar puede ser:

a) Objetivos a corto y largo plazo.

b) Detalle de recursos materiales y técnicos disponibles tales como documentos sobre los equipos, número de ellos, localización y características.

- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

Sistemas

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Salidas.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.
Se solicita la información y se ve que:

- No tiene y se necesita.
- No se tiene y no se necesita.

Se tiene la información pero:

- No se usa.
- Es incompleta.
- No está actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de "No se tiene y no se necesita", se debe evaluar la causa por la que no es necesaria. En el caso de "No se tiene pero es necesaria", se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar porque no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

2. Información y/o documentación preliminar que se debe recopilar

2.1 Información general

- Estructura del centro de cómputos, expedientes de personal del mismo, y a nivel de usuarios.

- Estructura del ambiente de procesamiento de los sistemas de computación, plataformas, tablas de programación, paquetes enlatados, relación con proveedores, sistemas de seguridad, redes y telecomunicaciones.

- Estructura de Presupuesto, Activos con que cuentan, redes y telecomunicaciones, ciclos de operaciones

- Manuales, Políticas y procedimientos de operaciones, finanzas, contables, control gerencial.

- Expedientes de proveedores y acreedores relacionados con equipos y tecnología de la información.

- Controles gerenciales y manual de funciones de usuarios (segregaciones de funciones)

- Documentación sobres los sistemas de seguridad lógica y física y de los procesos de los Sistemas de Información.

- Manuales de Desarrollo, Adquisición y Mantenimiento de los Sistemas de Información. (Soportes Técnicos)

2.2 Seguridad

- Solicitar las Políticas de respaldos internos
- Seguridad en los ambientes de los sistemas de control en la bases de datos.
- Inventario y ubicación de los extintores e extinguidores, detectores de humos, adecuación de instalaciones, etc.
- Accesos lógicos y físicos en el centro de cómputo, así como en su ambiente computacional, redes y telecomunicaciones.

2.3 Integridad, confidencialidad y disponibilidad de los sistemas de información

- Solicitar las ordenes de Output e input utilizados en los sistemas de información y módulos de aplicación en el ambiente o uso de las computadoras del cliente.
- Conocer el período de los reportes facilitados para las gerencias de los sistemas de aplicación.
- Saber la cantidad promedio de pruebas de recorrido realizados en los sistemas computarizados.
- La utilización y almacenamiento de los códigos fuentes, licencias de los sistemas utilizados.
- Obtener los planes de contingencias y pruebas de controles de usuarios.

2.4 Desarrollo, adquisición y mantenimiento de los sistemas de información

- Solicitar los expedientes del personal de soporte técnicos.
- Los expedientes de las pruebas de recorridos y planes de mantenimiento.
- Expedientes de proveedores y acreedores de servicios y relaciones entre ellos.
- Planes de Capacitación de usuarios
- Garantías obtenidas en las adquisiciones de sistemas, equipos, software y hardware
- Manuales y guías sobre los soportes de las redes y telecomunicaciones, software y hardware y sistemas de aplicación.
- Principales operaciones de los sistemas de información

3. Evaluación de los Sistemas

Los sistemas deben ser evaluados con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

- ¿Cuáles servicios están implementados?
- ¿Están a disposición de los usuarios?
- ¿Qué características tienen?
- ¿Cuántos recursos se requieren?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

- ¿Qué aplicaciones serán desarrolladas y cuando?
- ¿Qué tipo de archivos se utilizarán y cuando?
- ¿Qué bases de datos serán utilizarán y cuando?
- ¿Qué lenguajes se utilizarán y en que software?
- ¿Qué tecnología será utilizada y cuando se implementará?
- ¿Cuántos recursos se requerirán aproximadamente?
- ¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

- ¿Qué estudios van a ser realizados al respecto?
- ¿Qué metodología se utilizará para dichos estudios?
- ¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

4. Comprensión del control interno

Se debe comprender y evaluar el control interno para identificar las áreas críticas que requieren un examen profundo y determinar su grado de confiabilidad a fin de establecer la naturaleza, alcance y oportunidad de los procedimientos de auditoría a aplicar.

Existen dos tipos de controles: el control general y el control detallado de los sistemas de información. El control general involucra a todos los sistemas de información y el control detallado está diseñado para controlar el procesamiento en sí de la información.

4.1 Evaluación de controles

Los controles claves son evaluados para decidir si son confiables corno fuente de - satisfacción de auditoría y en qué grado confiar en ellos en el desarrollo del trabajo. La evaluación se basa en el criterio de profesional e implica:

a) Identificar los controles claves potenciales;
b) Reconsiderar la evaluación inicial del riesgo de control;
c) Evaluar las debilidades.

Los principales controles a evaluar son los siguientes:

a) Controles de autenticidad:
Estos sirven para verificar la identidad del individuo o proceso que intenta realizar alguna acción en el sistema; como por ejemplo: passwords, número de identificación personal, firmas digitales, atributos físicos, etc.;

b) Controles de exactitud:

Sirven para asegurar el grado de corrección de los datos y de los procesos en un sistema; como por ejemplo: validación de campos numéricos, validación de exceso en un campo, conteo de registros, cifras de control de valores, etc.;

c) Controles de totalidad:

Sirven para asegurarse que no se ha emitido ningún dato y que el proceso se efectuó adecuadamente hasta su conclusión; por ejemplo: validación de campo en blanco, conteo de registro, cifras control de valores, validación secuencia de registros, etc.;

d) Controles de redundancia:

Sirven para asegurar que los registros son procesados una sola vez; como por ejemplo: sello de cancelación de lotes, verificación de secuencia de registros, archivo de suspenso, cifras control, etc.;

e) Controles de privacidad:

Sirven para asegurar que los datos están protegidos contra el tomar conocimiento de ellos en forma inadvertida o no autorizada; como por ejemplo: passwords, compactación de datos, inscripción de datos, etc.;

f) Controles de pistas de auditoría:

Sirven para asegurarse que se mantiene un registro cronológico de los eventos tal como ocurrieron en el sistema. Existen dos tipos de pistas de auditoría:

-Pistas de auditoría contable;
-Pistas de auditoría operacional.

g) Controles de existencia:

Sirven para asegurar la continua disponibilidad de los recursos del sistema; como por ejemplo: vaciados de la base de datos, bitácora estatus de recursos, procedimientos de recuperación, mantenimiento preventivo, puntos de verificación, puntos de reinicio, duplicación de hardware, etc.

h) Controles de protección de activos

Sirven para asegurarse que todos los recursos del sistema están protegidos contra destrucción o deterioro; como por ejemplo: extinguidores, barreras físicas, passwords, cajas fuertes contra incendio, semáforos, etc.;

i) Controles de efectividad:

Sirven para asegurar que los sistemas logran su objetivos; como por ejemplo: encuestas de satisfacción de usuarios, monitoreo de la influencias de uso, medición de los niveles de servicios, estudios de factibilidad auditorias post-implementación, etc.;

j) Controles de eficiencia:

Sirven para asegurarse que en los sistemas se hace un uso óptimo de sus recursos al lograr sus objetivos; como por ejemplo: bitácora de uso de recursos, programas monitores, análisis costo-beneficio, cargos medidos a usuarios, etc.

4.2 Comprensión de la legislación aplicable

Está relacionada con el uso adecuado de la tecnología de la información, entre ellos:

a. Propiedad intelectual

b. Contrato de licencia

c. Copia no autorizada

d. Piratería

e. Equipos personales y servidores,

f. Accesorios, unidades disponibles de disco,

g. software

5. Desarrollo de la estrategia de auditoría

En función de la naturaleza, complejidad y del objeto de auditoría, se determinarán las áreas críticas, dependiendo de éstas se definirán los objetivos o el(los) enfoque(s) y el alcance de la auditoria.

Se tiene que definir los riesgos de la auditoría como el riesgo de que la información pueda contener errores materiales o de que el auditor no detectar un error que no ha ocurrido

Entre otros aspectos, el Auditor deberá fijar su atención en la planificación en lo siguiente:

a) Si el sistema asegura en su diseño la acumulación de transacciones similares para conformar cada cuenta de los informe compartidos

b) Explicar si la tecnología de la información es centralizado o no, si usan un sistema de red, microcomputadoras independientes, unidad central, nivel de retroalimentación de información procesada.

c) Medición del desempeño sobre la adecuación de la función de T

Perfil del control de la Tecnología de la Información, relacionado con los procesos más importantes, factores críticos de éxito para el control.

El Plan Estratégico de una auditoria de sistemas representa el soporte sobre el cual estarán basadas todas las actividades requeridas para la ejecución del trabajo y para alcanzarlo de forma eficiente. A continuación se analiza cada una de sus fases:

5.1 Establecimiento de Términos de Referencia
5.2 Hechos y Transacciones
5.3 Seguimiento de Hallazgos y Recomendaciones
5.4 Programación de la Estrategia de Auditoria
5.5 Ajustes a la Planeación de la Estratégicas

5.1 Establecimiento de términos de referencia

El establecimiento de los términos de referencia consiste en definir la responsabilidad del Auditor de Sistema, logrando un claro entendimiento del alcance del trabajo o revisión especializada, por consiguiente, definiendo los objetivos que se buscan con el trabajo. Esto implica definir:

a) La naturaleza del trabajo de auditoría

Se refiere al tipo de auditoría o revisión que se efectuará y a los objetivos consecuentes, por ejemplo: Controles Generales del Computador, Controles de Aplicación, Auditorias a Procesos Informativos, Procesamiento Electrónico de Datos, otros, etc.

b) Informes de resultado y fechas de compromisos

Se deben identificar los diferentes informes que se emitirán en la fase del trabajo y las fechas máximas en que se deben ser efectivas, los que incluyen los análisis de los sistemas, el funcionamiento de los diseños del sistema, ejecución de pruebas, etc.

c) Actividades y fechas de mayor importancia

Se deben describir las actividades principales que deban cumplirse así como las fechas claves, en tal forma que se asegure cabalmente el entendimiento de responsabilidades, ejemplos:

- Visita de planeación (iniciación y terminación)
- Iniciación y terminación de visitas para auditar los sistemas
- Iniciación y terminación de visitas para realizar pruebas sustantivas
- Observación de organización del Departamento de Informática
- Presentación de resultados
- Visitas de seguimientos, implementación de recomendaciones, otro etc.

5.2 Hechos y transacciones individuales de significación

Las informaciones obtenidas en esta etapa deberán servir de base para que a manera de síntesis en el Memorando de Planeación ilustre la información sobre antecedentes con énfasis en los cambios ocurridos en el último año, al menos lo siguiente:

a) Comprensión de la Entidad y de sus Ambiente

Al planificar una auditoría, el Auditor Informático debe tener una comprensión suficiente del ambiente total que revisará. Este conocimiento debe incluir una comprensión general de las diversas prácticas y funciones de la auditoría, así como los tipos de sistemas de información que se utilizan. También, debe comprender el ambiente normativo del negocio. Ejemplo: A un banco se le exigirá requisitos de integridad de sistemas de información y de control que no están presente en una empresa comercial.

Los pasos que puede llevar a cabo un Auditor Informático para obtener una comprensión de la Entidad pueden incluir:

- Recorrer las instalaciones de la organización
- Lectura material sobre antecedentes que incluyan publicaciones sobre memorias, informes financieros independientes.
- Entrevista con gerentes claves para comprender los temas

- Estudios de los informes
- Informes de auditorías previas y planes estratégicos, etc.

b) Riesgo y Materialidad (cuantía) de auditoría

Se tiene que definir los riesgos de la auditoría como el riesgo de que la información pueda contener errores materiales o de que el auditor Informático pueda no detectar un error que no ha ocurrido

Pueden clasificar los riesgos de auditoría de la siguiente manera:

Riesgo inherente: El riesgo de que un error pueda ser material o significativo (importante) cuando se combina con otros errores encontrados durante la auditoria, no existiendo controles compensatorios relacionados.

Riesgo de control: El riesgo de existir un error material que no pueda ser evitado o detectado en forma oportuna por el sistema de control interno.

Riesgo de detección: El riesgo de que el auditor use pruebas exitosas a partir de un procedimiento de prueba inadecuado y pueda llegar a la conclusión de que no existen errores materiales cuando en realidad los hay.

Cabe señalar que la materialidad exige al auditor de SI un juicio claro, basado en que para el auditor Informático es más complicado la materialidad.

c) Otros aspectos generales

Entre otros aspectos, el Auditor Informático deberá fijar su atención en la planificación lo siguientes:

- Si el sistema de procesamiento contable es homogéneo para las regionales o unidades geográficamente separadas

- Si el sistema asegura en su diseño la acumulación de transacciones similares para conformar cada cuenta de los informe compartidos

- Explicar si el tipo de procesamiento electrónico de datos es centralizado o no, si usan un sistema de red, microcomputadoras independientes, unidad central, nivel de retroalimentación de información procesada.

- Podrían incluir una descripción de contingencias, convenios, proveedores de sistemas, respaldos, seguridad en las bases de datos, entre otros, etc.

5.3 Seguimiento de hallazgos y recomendaciones

Para evaluar los efectos sobre los Sistemas se debe dar seguimiento a los hallazgos y recomendaciones de importancia obtenidos de auditorías anteriores, las medidas correctivas realizadas, la aceptación y aporte efectuado por las auditorias de sistemas realizadas y la emisión de informes reportándose aquellas observaciones no realizadas recordando su importancia y la necesidad de corrección para propósito de determinar el enfoque, alcance, naturaleza y oportunidad de pruebas.

5.4 Programación de la estrategia de auditoría

La planeación estratégica de la auditoría debe resumirse en el memorando y debe describir como mínimo:

a) Planes de rotación (en caso de auditorías recurrentes)

En el alcance de nuestras pruebas podríamos decidir hacer revisiones en áreas que no fueron consideradas significativas o efectuar procedimientos mínimos.

b) Procedimientos generales de control

Políticas y procedimientos de seguridad lógica para asegurar la adecuada autorización de transacciones y actividades.

Políticas globales para el diseño y utilización de documentos y registros adecuados.

Accesos lógicos y seguridad, respaldos

Seguridad física para los centros de cómputos.

c) Procedimientos de control de Sistemas de Información

- Accesos de datos y programas.
- Metodologías de desarrollo de sistemas
- Operación de procesamiento de datos
- Funciones de programación de sistemas y soporte técnicos
- Control de calidad de procesamiento de datos
- Revisión técnica de la documentación de sistemas complejos
- Entrevistas con especialistas técnicos y usuarios

- Técnicas de diagramas de flujo y redes
- Fechas límites de implementación de sistemas
- Tecnologías actuales y futuras, recursos

Planes contingentes, delitos informáticos, capacitaciones, entre otros

5.5 Ajustes a la planeación de la estrategia

La planeación podrá ser ajustada básicamente por circunstancias que pueden ser:

- Resultados de la comprobación del funcionamiento de los sistemas y,
- Situaciones de error o irregularidad que aparezcan en la etapa de ejecución de las auditorias que a criterios pueden dar meritos de cambios.
- Presupuesto de tiempo y relación con otros auditores.

6 Personal participante

Una de las partes más importantes dentro de la planeación de la auditoría en informática es la designación del personal que deberá participar y sus características. Se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría.

En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

- Técnico en informática.
- Experiencia en el área de informática.
- Experiencia en operación y análisis de sistemas.
- Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

7 Programas de auditoría

Las Normas de Auditoría Gubernamental de Nicaragua establecen la obligatoriedad de elaborar programas para cada auditoría, al respecto establecen.

NAGUN 10.10 – A PROGRAMAS DE AUDITORIA

Se deberán efectuar programas a la medida que incluyan las listas de procedimientos de auditorías para examinar los Sistemas, tanto a nivel de Controles Generales del Computador como Controles Generales de Aplicación.

Los programas de auditoría deberán contemplar procedimientos para el cumplimiento de los siguientes objetivos:

1. Que la dirección y administración de las Tecnologías de Información, estén bien definidos y se cumplan las políticas y planes informáticos.

2. Que se cumplan los aspectos y contratos por servicios a terceros.

3. Que los trabajos de planeamiento, desarrollo, operación y mantenimiento de los sistemas estén documentados y controlados.

4. El aprovechamiento y rendimiento de los sistemas.

5. Evaluar los controles de acceso, modificaciones, calidad, entrada de datos, procesamiento, salidas de datos y seguridad de la información.

6. Que los controles de seguridad y continuidad estén establecidos tanto en los procesos manuales como automatizados.

7. La existencia de procedimientos efectivos para controlar los datos recibidos y los enviados.

8. Administración y seguridad de las redes

9. La transferencia electrónica de datos, valores y documentos.

10. Internet.

11. Cumplimiento del reglamento sobre seguridad informática.

12. Exactitud del procesamiento.

13. Segregación de funciones.

14. Incidencia en el Control Interno, Contable y Administrativo.

15. Cultura Organizacional.

16. Competencia Profesional del Personal Informático.

Esta etapa consiste básicamente en el proceso mediante el cual se preparan las listas de procedimientos de auditorías para examinar los Sistemas, tanto a nivel de Controles Generales del Computador como Controles Generales de Aplicación.

Los programas de auditoría detallados son los instrumentos metodológicos mediante los cuales se pone en ejecución la "Planeación General de la Auditoría" documentada en el Memorando de Planeación y su preparación es responsabilidad del Auditor de Sistemas, el cual llega ser la guía a los auditores para ejecutar los procedimientos y proporciona un registro permanente de la auditoria para facilitar la supervisión final.

Las áreas o aspectos a evaluar en una auditoría de sistemas son: la planeación de las aplicaciones, el inventario de sistemas en proceso, la situación de cada aplicación.

7.1 Evaluación de políticas y procedimientos

Se deberán elaborar programas para evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son los adecuados para la dependencia.

Es importante revisar la situación en que se encuentran los manuales de análisis y si están acordes con las necesidades de la dependencia. En algunas ocasiones se tiene una microcomputadora, con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una dependencia específica.

Se debe evaluar la obtención de datos sobre la operación, flujo, nivel, jerarquía de la información que se tendrá a través del sistema. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La auditoría en sistemas debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse. Con la información obtenida podemos contestar a las siguientes preguntas:

- ¿Se está ejecutando en forma correcta y eficiente el proceso de información?
- ¿Puede ser simplificado para mejorar su aprovechamiento?
- ¿Se debe tener una mayor interacción con otros sistemas?
- ¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?
- ¿Está en el análisis la documentación adecuada?

7.2 Evaluación del diseño lógico de los sistemas

En esta etapa se deberán analizar las especificaciones del sistema.
¿Qué deberá hacer?, ¿Cómo lo deberá hacer?, ¿Secuencia y ocurrencia de los datos, el proceso y salida de reportes?; la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

El análisis del diseño lógico del sistema debe ser comparado con lo que realmente se está obteniendo en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo.

Los puntos a evaluar son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos (antes y después del proceso electrónico de datos).
- Proceso lógico necesario para producir informes.
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables.

- Número de usuarios.

7.3 Evaluación del diseño, control de los sistemas

Se deberán auditar los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema. Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza.

7.4 Evaluación de las medidas de seguridad y control de los sistemas

Se deberán diseñar programas de auditoría para evaluar las medidas de seguridad física, de respaldo, seguridad lógica, en la utilización del equipo, en la recuperación de equipos de cómputos.

En tal sentido se deberán incluir procedimientos para evaluar lo siguiente:

- Revisar la seguridad lógica de los datos y programas
- Revisar la seguridad lógica de las librerías de los programadores
- Examinar los controles sobre los datos
- Revisar procedimientos de entrada / salida
- Verificar las previsiones y procedimientos de backup
- Revisar los procedimientos de planificación, adecuación y mantenimiento del software del sistema.
- Revisar documentación del software del sistema.
- Revisar documentación del software de base.
- Revisar controles sobre paquetes externos(sw)
- Supervisar el uso de herramientas peligrosas al servicio del usuario.

Al comprobar la seguridad e integridad de la base de datos el auditor deberá verificar que:

- Existe una fase de prevención de emergencias separadas de las fases de respaldo y restauración.
- Figura responsable de la supervisión de la emergencia.
- Existencia de conjunto de normas de emergencias.
- Procedimientos sistemáticos de clasificación de emergencias.

Una vez que todos los riesgos han sido clasificados se está en condiciones de fijar los procedimientos que aseguraran la continuidad del funcionamiento del negocio.

Tipos de <u>seguros</u>:

- Todo riesgo

- Daños determinados
- Seguro contra averías
- Seguro de fidelidad
- Seguro contra interrupción del negocio; cubre las perdidas que sufrirían la empresa en el caso que las actividades informáticas se interrumpiesen.

a. Plan de desastre, respaldo y recuperación.

7.5 Respaldo en caso de desastre

Se debe revisar la existencia en cada dirección de informática un plan de emergencia el cual debe ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia, se tenga la seguridad que funcionará; por lo que se debe incluir proce3dimientos para comprobar que la información que contiene el plan de emergencia, se considere como confidencial o de acceso restringido.

Lineamientos de control que cubren los elementos de respaldo y recuperación.

- Plan de recuperación en caso de siniestro: debe existir un plan documentación de respaldo para el procesamiento de trabajos críticos.
- Procedimientos de urgencia y capacitación del personal: deben garantizar la seguridad del personal.
- Aplicaciones criticas: el plan de respaldo debe contener una prioridad preestablecida para el procesamiento de las aplicaciones.
- Recursos críticos: deben estar identificados en el plan de respaldo la producción critica, el sistema operativos y los archivos necesarios para la recuperación
- Servicios de comunicación
- Equipo de comunicación
- Equipo de respaldo
- Programación de operaciones de respaldo
- Procedimientos de respaldo de archivos
- Suministro de respaldo: considerar una fuente de abastecimiento para la recuperación de materiales especiales.
- Pruebas de plan de respaldo
- Reconstrucción del centro de sistemas de información
- Procedimientos manuales de respaldo.

Los desastres que pueden suceder podemos clasificar así:
a) Completa destrucción del centro de cómputo,
b) Destrucción parcial del centro de cómputo,
c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)
d) Destrucción parcial o total de los equipos descentralizados
e) Pérdida total o parcial de información, manuales o documentación
f) Pérdida del personal clave
g) Huelga o problemas laborales.

7.6 Contratos de mantenimiento

Como se sabe existen básicamente tres tipos de contrato de mantenimiento:

El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes.

El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es “por llamada”, en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como “en banco”, y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cuál de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación.

El Anexo muestra los modelos de programas y cuestionarios de aplicación.

8 Cronograma

El control del avance de la auditoría es fundamental para el logro eficiente de la misma por lo que se deberá elaborar un cronograma de ejecución que defina las áreas y tiempos asignados para su cumplimiento, lo cual permitirá el seguimiento a los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

CAPITULO XXVIII
EJECUCION DE LA AUDITORIA DE INFORMATICA

Capítulo XXVIII
Ejecución de la Auditoría informática

Esta etapa de la auditoría consiste en el desarrollo de los procedimientos contenidos en los programas de auditoría a través de técnicas de auditoría.

Evidencias de auditorías y papeles de trabajo

Las Normas de Auditoría Gubernamental de Nicaragua indican la obligatoriedad de Obtener Evidencia Suficiente, Competente y Pertinente" para sustentar los hallazgos de auditoría.

Los papeles de trabajo de una auditoría de sistemas constituyen el sustento del trabajo llevado a cabo por el auditor especialista, así como de los comentarios, conclusiones y recomendaciones incluidos en su informe, representado por la evidencia en ellos contenida.

La organización de centros de cómputos, seguridad de los sistemas de control y practicas de control, la administración de los sistemas de información, los procesos mismos de datos, la integridad, confiabilidad, confidencialidad y disponibilidad que brindan los sistemas computacionales, el desarrollo, adquisición y mantenimiento de los sistemas son tópicos y casi seguro de la importancia para el control de los registros que soporta la cifras y controles de cualquier reporte importante para una entidad, en su sentido amplio, constituyen un conjunto de aseveraciones o declaraciones formuladas por la administración en torno a los resultados de su gestión.

Los papeles de trabajo de la auditoría deberán mostrar los detalles de la evidencia, la forma de su obtención, las pruebas a que fue sometido y las conclusiones sobre su validez.

Los papeles de trabajo son propiedad absoluta del auditor condicionando su uso únicamente a los propósitos de su revisión y soporte de los resultados obtenidos.

1. Técnicas de Auditoría

Para la obtención de evidencias se pueden utilizar diversos tipos de técnicas y procedimientos de auditoría, de los cuales destacan el análisis de datos, ya que para las organizaciones el conjunto de datos o información son de tal importancia que es necesario verificarlos y comprobarlos; utilizando diversas técnicas para el análisis de datos, las cuales se describen a continuación:

1.1 Técnicas y procedimientos

a) Cuestionarios

El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Se envían cuestionarios preimpresos a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría. Se recomienda solo hacer preguntas necesarias, que permitan alcanzar el objetivo; preguntas sencillas y directas, no hacerlas abiertas, porque dificultan el análisis.

b) Entrevistas

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

- Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Para el caso del auditor informático, siempre tienen que ser su entrevista preparada y con preguntas sistematizadas, que en un ambiente de cordialidad le permita al usuario dar la información que el auditor requiere, de una manera sencilla.

c) Checklist

Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamados Check List, tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se pueden llegar a obtener resultados distintos a los esperados.

La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma, al método.

El profesionalismo para utilizar los checklist, pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Tipos de Check List:

- **Rango**

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido. Después se hacen preguntas, mismas a las que se les dio una ponderación y después bajo promedio aritmético, se relacionado con el rango preestablecido.

Los Checklists de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en los checklist binarios. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

- **Binaria**

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente. Los Checklists Binarios siguen una elaboración inicial mucho más ardua y compleja.

Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

d) Comparación de programas

Esta técnica se emplea para efectuar una comparación de código (fuente, objeto o comandos de proceso) entre la versión de un programa en ejecución y la versión de un programa piloto que ha sido modificado en forma indebida, para encontrar diferencias.

e) Mapeo y rastreo de programas

Esta técnica emplea un software especializado que permite analizar los programas en ejecución, indicando el número de veces que cada línea de código es procesada y las de las variables de memoria que estuvieron presentes.

f) **Análisis de código de programas**

Se emplea para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual (en cuyo caso sólo se podría analizar el código ejecutable).

g) Datos de prueba

Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

h) **Datos de prueba integrados**

Técnica muy similar a la anterior, con la diferencia de que en ésta se debe crear una entidad, falsa dentro de los sistemas de información.

i) Análisis de bitácoras

Existen varios tipos de bitácoras que pueden ser analizadas por el auditor, ya sea en forma manual o por medio de programas especializados, tales como bitácoras de fallas del equipo, bitácoras de accesos no autorizados, bitácoras de uso de recursos, bitácoras de procesos ejecutados.

j) **Simulación paralela**

Técnica muy utilizada que consiste en desarrollar programas o módulos que simulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos de forma paralela e identificar diferencias entre los resultados de ambos.

k) Trazas o Huellas

Por lo general, los auditores se apoyan en software que les permiten rastrear los caminos que siguen los datos a través del programa. Las Trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. No deben modificar en absoluto el Sistema. Permite rastrear los caminos que siguen los datos a través del programa.

Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

l) Log

Consiste en el historial que informa que fue cambiando y cómo fue cambiando la información.

i) Software de auditoría

Los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

1.2 Técnicas de auditoría asistidas por el computador

Las técnicas de auditoría asistidas por el computador son aquellas que utilizan computadores, programas y datos de computación para obtener evidencias de auditoría. Los tipos de técnicas son Programas de recuperación y análisis; técnicas de transacciones de pruebas;

a) Programas de recuperación y análisis

Son programas escritos de acuerdo con especificaciones de auditoría para organizar, combinar, calcular, analizar o extraer datos del computador, los males son dirigidos a obtener evidencia sustantiva. Las fuentes principales de estos programas son:

- Paquetes de Software de Auditoría

Estos permiten la generación de programas a través de especificaciones de la Entidad u Organismo relativamente simples. Para especificar las tareas de auditoría que el programa ejecutará se debe seleccionar la rutina o combinación de rutinas preprogramadas que se desea. Normalmente el uso de software de auditoría incluye cuatro etapas:
- Desarrollo del programa de auditoría Específica;
- Generación del programa fuente;
- Compilación del programa fuente;
- El programa objeto es ejecutado para la generación de informe.

- Software de Recuperación de Información

Es un software diseñado para la generación de reportes y recuperación de información especializada; además, existen medios o lenguaje de consulta los cuales funcionan por lo general de igual forma que los paquetes de recuperación de información o generadores de informes y generadores están presentes en sistemas de administración de bases de datos (DBMS).

- Programas Utilitarios

Son otras fuentes de software que pueden ser utilizadas para la ejecución de procedimientos de auditoría. Son diseñados para llevar a cabo tareas específicas de procesamientos de datos.

El usuario da las instrucciones al programa utilitario en forma de los que identifican los archivos de entrada y salida y la función que debe ser realizada y los criterios de selección.

Dentro de las funciones que realizan los programas utilitarios están.

- Clasificación de archivos de datos;
- Fusión de varios archivos en uno solo;
- Copia de archivos de datos;
- Impresión de todo o parte de los archivos de datos;
- Búsqueda de registros que contengan determinados valores en un campo de datos vacío.

- Lenguajes Convencionales de Programación

El uso de estos lenguajes requiere un alto nivel de conocimientos técnicos para desarrollar y correr los programas. Se requieren instrucciones de programación detalladas aun para realizar un procedimiento simple. Sin embargo, cuando no se dispone de programas de software de auditoría y otro software de recuperación de datos, un programa convencional puede ser la alternativa más conveniente.

b) Uso de programas de recuperación y análisis

- **Informe de Excepciones.**

  Un mismo programa puede seleccionar diversos tipos de excepciones. Algunos ejemplos de informes de excepciones incluyen:

  - Impresión de las cuentas por cobrar que supera un determinado monto o que están vencidas;
  - Impresión de pagos posteriores a una fecha determinada;
  - Impresión de items potencialmente obsoletos, de baja rotación o de aquellos con existencia excesiva.

- **Selección de muestras.**

  Las muestras pueden ser seleccionadas automáticamente entre diversas alternativas, incluyendo muestreos estratificados, selección sistemática o selección con probabilidad proporcional al tamaño. Los ejemplos de aplicación de muestreo incluyen:
  - Confirmaciones de cuentas por cobrar, cuentas de ahorro, cuentas de préstamos y cuentas por pagar-,
  - Análisis de desembolsos;
  - Selección de existencias para su inspección física.

- **Prueba o ejecución de cálculos.**

  Los programas de recuperación y análisis pueden ser utilizados para probar los cálculos, ya sea rehaciendo los mismos, o mediante comprobaciones globales de razonabilidad Los ejemplos de cálculos que pueden ser probados incluyen:

  - Procedimientos de manejo de depreciaciones;
  - Antigüedad de saldos de cuentas por cobrar;
  - -Ingresos o egresos por intereses;
  - -Valuación de existencia.

- **Prueba de imputaciones.**

  Los programas de recuperación y análisis pueden ser utilizados para verificar el registro de transacciones en las cuentas del mayor general, acumulando las transacciones detalladas para su conciliación con los totales resultantes del procesamiento real, como por ejemplo la distribución de:

  - Compras a cuentas por pagar y a rubros de activos, existencia y/o gastos;
  - Análisis de ventas;
  - Remuneraciones a las correspondientes cuentas de costos;

- **Totales de archivos.**

  Los programas de recuperación y análisis pueden ser utilizados para revisar las sumas y multiplicaciones en los registros individuales contenidos en los archivos, a fin de que los montos puedan ser comparados con los registros externos. Algunos ejemplos son:

  - Suma de saldos de los registros individuales de cuentas de deudores para su conciliación con el saldo del libro mayor;
  - Producto de las unidades de existencias por su costo para su conciliación con el monto de existencia registrada.

- **Resumen y clasificación de datos.**

  A menudo la forma en que la información es almacenada o presentada no es conveniente para la ejecución de los procedimientos de auditoría. Se pueden preparar programas de recuperación y análisis para resumir y reordenar la información de la manera más conveniente; como por ejemplo

  - Reordenamiento y resumen de los pagos a proveedores, ordenados por proveedor y listados en orden descendente;
  - Reordenamiento y resumen de cobranzas de deudores para su comparación con los créditos registrados en las cuentas individuales de cada deudor;
  - Estratificación de datos para la selección de muestras o revisiones analíticas.

- **Comparación de datos en archivos separados.**

  Esta función puede proporcionar una manera eficiente de relacionar la información utilizada por diversos sistemas de aplicación. Como ejemplo tenemos:
  -Archivos de desembolsos con archivos maestros para establecer sí los pagos se efectúan solo a proveedores autorizados;
  -Archivos de remuneraciones del período corriente y anterior para identificar altas y bajas de personal;
  Resultados de inventarios físicos con registros permanentes de existencias para identificar discrepancias.

- Comparación de datos con registros contables.
  Los programas de recuperación y análisis deben ser utilizados para comparar la evidencia de auditoría con los registros contables. Un ejemplo podría ser 1 comparación de existencias con los registros permanentes de existencias y la comparación de las respuestas a circularización de las cuentas por cobrar.
- Preparación de informes.
  Además de los informes producidos como resultados de los procedimientos descritos anteriores se pueden preparar muchos otros informes,

c) Técnicas de transacciones de prueba

Estas técnicas permiten verificar la operación correcta de los controles computarizados y funciones procesamiento de los sistemas de aplicación.

Suponen el ingreso (o intento de ingreso) de pruebas.
Los resultados obtenidos del procesamiento son posteriormente comparados con los resultados predeterminados.

Existen varios mecanismos los cuales se describen a continuación:

- **Procedimientos de Prueba Integrado**

Este procedimiento es también conocido como la técnica de mini empresas o empresas simuladas. En este procedimiento las transacciones de pruebas son procesadas a través del sistema de un modo productivo o sea utilizando los mismos procedimientos que se emplean para la transacciones reales; pero se deberá tener la precaución de excluir la empresa simulada de la información real al final del trabajo.

Aunque el procedimiento de prueba integrado puede ser implantado para cualquier sistema de aplicación, esta técnica es más efectiva cuando se ha perdido el rastro de auditoría o cuando la complejidad del sistema dificulta el seguimiento del flujo de las transacciones.

- **Datos o Lotes de Pruebas**

Se utilizan para determinar si las rutinas de edición y otros controles de procesamiento computarizados funcionan de acuerdo con lo previsto. Una vez finalizado el procesamiento los resultados reales de la prueba son comparados con los resultados predeterminados.

Al emplear la técnica de datos de prueba debe tenerse en cuenta los siguientes aspectos:

-Una vez desarrollados los lotes de pruebas pueden volver a ser usados en ocasiones futuras, siempre y cuando los programas no hayan sido modificados;
Cuando los lotes de pruebas deban cubrir un amplio alcance su desarrollo y ejecución pueden requerir una considerable inversión de tiempo;

Se debe estar seguro de que se prueban las copias adecuadas de los programas de producción.

- **Pruebas On Line (Pruebas en Línea)**

Esta técnica es útil cuando la información es capturada en sistemas interactivos y los registros se actualizan en forma inmediata o son almacenados temporalmente para procesarlo en forma posterior sin intervención del usuario.

Las características comunes de esta técnica son las siguientes:

- Se usa la edición y validación de datos para prevenir la captura de transacciones erróneas o no autorizadas;

- La mayoría de los sistemas con captura interactiva están diseñados para rechazar transacciones inválidas sin dejar huellas de dicho rechazo;

- - Es fácil de usar y las pruebas en ser instaladas con un mínimo de interrupción en los sistemas de aplicación;

- Las pruebas en líneas pueden ser usadas para evaluar los controles en contra de accesos no autorizados.

d) Uso de técnicas de transacciones de pruebas

A continuación se describen procedimientos de auditoría específicos que se en llevar a cabo con las técnicas de transacciones de pruebas:

- **Verificación de los controles de edición y validación.**

La mayoría de los sistemas de aplicación computarizados incorporan controles de edición y validación que informan o rechazan transacciones faltantes, duplicadas o potencialmente erróneas. Se pueden probar tales controles ingresando transacciones de pruebas.

- **Prueba de informe de excepción.**

La revisión y solución de las excepciones o items en suspenso informados en contribuir a evitar errores de importancia. Mediante el procesamiento de pruebas que contengan excepciones, se puede determinar si las excepciones incorrectas son rechazadas o incluidas en archivos de items en suspenso y en los informes de error correspondientes.

- **Prueba de los cambios a los datos permanentes.**

Los controles sobre los cambios a los datos permanentes permiten confirmar la corrección de la información, al impedir o detectar las modificaciones erróneas o no autorizadas.

- **Prueba de comparaciones, cálculos, registros y acumulaciones.**

Las transacciones de prueba pueden ser preparadas y sometidas a cálculos, imputaciones y acumulaciones. Si los resultados reales concuerdan con lo previsto existirá una razonable seguridad de que las funciones de procesamiento computarizadas funcionan adecuadamente.

- **Prueba de totales de control.**

  Se puede utilizar recuentos de registros y otros totales de control generados durante el procesamiento para detectar transacciones no autorizadas, faltantes, duplicadas o erróneas. Se pueden usar transacciones de pruebas ingresadas y procesadas como un lote separado para verificar que los totales de control generados por el sistema sean correctos.

e) El downloading como herramienta de auditoria

Las conexiones de microcomputadores y computadoras centrales facilitan el acceso de los datos y permiten flexibilidad en la ejecución de los procedimientos de auditoría. Permiten que el microcomputador se transforme en un mecanismo de ingreso,. Procedimiento y salida de datos, además de ser una unidad independiente.

A continuación se enumeran posibles procedimientos de auditoría realizando Downloading:

- Transferencia de datos trimestrales seleccionada al microcomputador para revisiones periódicas;

- Datos financieros y operativos significativos para su revisión analítica por categoría de gastos, centro de costo, división o línea de producto, con el objeto de realizar: -Comparaciones de saldos; -Análisis de tendencia lústrica; -Análisis de índices; -Análisis de variaciones.

- Cartera de inversiones para verificar los precios a través de conexiones con base de datos públicas;

- Selección en el computador central de las cuentas para circularización, impresión de las cartas de confirmación y resumen de los resultados;

- Transferencia a microcomputadores de los datos sobre existencia para crear una base de datos y usar el software de micro computación para:
  -Seleccionar los items a recontar;
  -Examinar los Usados para identificar iteras inusuales;
  -Reordenar los items utilizando condiciones;
  -Detectar niveles excesivos de existencias;
  -Detectar ¡tema de poco movimiento.

- Transferencia al microcomputador de los precios y cantidades de existencias de las líneas de productos más significativas para compararlas con períodos anteriores y el uso proyectado;

- Para Entidades u Organismo financieros

- Transferencias de los saldos de préstamos, tasas de interés e información de unidades monetaria a fin de crear una base de dato de los préstamos en el microcomputador y emplear el software para:
  -Calcular índices;
  -Calcular tasas de retorno;
  -Calcular por unidad monetaria o por tasa de interés;
  -Seleccionar préstamos para su confirmación.

- Transferencia de datos financieros de importancia a un modelo en el microcomputador a fin de comprobar si se están cumpliendo cláusulas complejas de los contratos- de préstamos;

- Selección en el computador central de items de cuentas por pagar a fin de transferirlos al microcomputador para imprimir las confirmaciones y resumir los resultados;

- Transferencia de los saldos de cuentas significativas a un modelo en el microcomputador para hacer cálculos de:
  - Previsión para vacaciones;
  - Distribución de utilidades;
  - Planes de pensiones etc.

- Transferencia de los montos de previsiones impositivas, incluyendo impuestos diferidos y prueba de cálculos;

- Transferencia de los balances de saldos en moneda extranjera por país para realizar su conversión;

- Para Compañías de Seguros, transferencia de los datos históricos y financieros necesarios para analizar las reservas.

f) Software de análisis y extracción (interactive data extraction and analisis - i. d. e. a)

IDEA es un programa de aplicación para microcomputadores diseñado para ayudar al auditor en la revisión de las características de los registros de computador de manera fácil, consistente y rápida.
Esta revisión está constituida por las siguientes funciones:

- Importar o encadenar los registros de un determinado ambiente al ambiente estándar del IDEA para propósito de extracción y análisis mediante procedimientos preprogramados;

- Extraer un conjunto de registros utilizando las siguientes modalidades:

- -Procedimientos de muestreo;
- -Definiendo el criterio de selección de los registros;
- Analizar las características de los registros seleccionados utilizando diversas técnicas predeterminadas;
- Crear reportes de registros seleccionados en diversas modalidades;
- Exportar los registros seleccionados a diferentes ambientes para otros tipos de análisis y/o presentaciones.

2. Evidencia sobre información procesada por medios electrónicos.

En el entorno actual, el uso de equipos para procesamiento electrónico de datos en los sistemas computarizados cada día es más rápido y generalizado, aún en entidades de tamaño mediano o pequeño.

La mayoría de los Delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos.
- Adicionar Datos.
- Alterar datos.
- Duplicar procesos.

Al respecto, el uso de computadoras también afecta el proceso de la auditoría. Su empleo puede dar como resultado sistemas que proporcionen menos evidencia que aquellos que utilicen procedimientos manuales. Las características de estos sistemas pueden incluir:

a) Ausencia de documentos de entrada, los datos pueden ser alimentados directamente al sistema sin documentos que lo soporten, inclusive las autorizaciones de entrada de datos puede ser reemplazada por otros contenidos en los programa de la computadora (Ej. Límite de transacción).

b) Falta de rastro visible de transacciones, ciertos datos son mantenidos sólo en los archivos de la computadora, o sólo parcialmente legible y por un período limitado de tiempo.

c) Falta de datos de salida visible, ciertas transacciones o resultados de procesamiento pueden no ser impresos o sólo en datos resumidos, lo que da como resultado la necesidad de tener acceso a datos retenidos en archivos legibles sólo por la computadora.

d) Facilidades de acceso de datos y programas de computadora. Se puede tener acceso a los datos y programas y además pueden ser alterados, desde lugares distantes. En ausencia de controles apropiados existe un potencial acceso no autorizado y la alteración de datos por personal dentro y fuera de la entidad.

Un sistema con deficiencias de sistemas y/o procedimientos puede dar lugar a errores en cuanto a:

a) Procesamiento de transacciones y otros datos.

b) Procedimientos de control.

c) Los saldos de diversas cuentas, por un ingreso erróneo de datos.

d) Vulnerabilidad de datos y medios de almacenamiento

Si la información de la Entidad u Organismo Auditado es procesada mediante Equipos de tecnología informática y ella constituye parte importante de la auditoría, el auditor deberá cerciorarse de su relevancia y confiabilidad. Los auditores pueden aplicar los criterios siguientes:

Cuando el auditor utiliza información proveniente de sistemas de procesamiento informático de datos, o la incluye en su reporte con fines informativos o como antecedentes y ella no es significativa para comunicar los hallazgos y observaciones de su informe, bastará citar la fuente de la información incluida y expresar que ella no fue verificada. De esta manera se satisfacen las normas para la presentación de informes, en lo que respecta a exactitud e integridad.

3. Tipos de procedimientos

3.1 Pruebas de cumplimiento

El objetivo de la prueba de cumplimiento es determinar si el control interno es adecuado y si está funcionando en la forma que se planeó en el área de informática.

Las pruebas de cumplimiento deben apoyarse en el alcance que se determinó, pudiendo soportarlo a través de:

- Documentación.
- Manuales de usuario, técnicos y procedimientos.
- Cambios en los programas.
- Solicitud por escrito.
- Pruebas por parte de los usuarios.

- Actualización de los manuales técnicos y de usuarios
- Verificar que los cambios en los programas sean realizados por el personal de informática o por el proveedor de la aplicación.
- Copias de respaldo y recuperaciones.
- Contenidos de las copias.
- Periodicidad de las copias.
- Persona responsable.
- Custodia, almacenamiento, inventario, rotación de la cinta.
- Acceso a datos y programas.
- Verificar la lista de usuarios que tiene acceso.
- Revisar el procedimiento para otorgar y eliminar los accesos.
- Analizar la periodicidad de los cambios de los passwords (clave).
- Capacitación de los usuarios
- Controles en la entrada, proceso y salida

3.2 Pruebas sustantivas

El objetivo de las pruebas sustantivas es obtener la suficiente evidencia para que el auditor pueda juzgar si ha habido pérdidas materiales o podrían ocurrir en el ambiente de procesamiento de datos.

A continuación se enumeran algunas pruebas sustantivas que deben ser usadas:

a) Pruebas para identificar procesos erróneos;

b) Pruebas para evaluar la calidad de los datos;

c) Pruebas para identificar datos inconsistentes;

d) Pruebas para comparar datos con conteos físicos;

e) Confirmación de datos con fuentes externas.

3.3 Pistas de auditoría informática

Es recomendable que toda la información que se necesita para revisar datos con fines de auditoría contable, se guarde en una base de datos, la cual deberá contener por lo menos la siguiente información:

a) Identidad del usuario del sistema;

b) Autenticidad de la información proporcionada;

c) Recursos solicitados;

d) Privilegios solicitados;

e) Identificación para la terminal;

e) Tiempo de inicio y de fin de la sección;

f) Número de intentos antes de lograrse conectarse;

g) Recursos proporcionados y negados;

h) Privilegios proporcionados y negados.

Esta información le será de utilidad al auditor gubernamental para detectar cualquier debilidad en el sistema.

Si se usa la captura con documentos, la constancia de la auditoría debe estar presente en los documentos otros debe identificarse:

a) Quién elabore el documento;

b) Quién lo autorizó.

c) Cuando se elaboró;

d) Cuál cuenta contable se afectará;

e) Qué información se actualizará,

f) Número del lote.

3.4 Otras pistas de auditoría

Algunas otras pistas de auditoría que debe revisarse son:

a) Tiempo invertido para teclear documentos fuente en una terminal;

b) Número de errores leídos por un dispositivo de lectura óptica;

c) Número de errores de dedo que hubo durante la captura;

d) Frecuencia con la cual se utiliza una instrucción;

e) El tiempo que toma en ejecutar la misma instrucción usando una pluma magnética Vs. ratón.

CAPITULO XXIX
INFORME DE AUDITORIA INFORMATICA

Capítulo XXIX
Informe de Auditoría

Las normas relativas al informe de auditoría definen que se prepare un informe por escrito que contenga los resultados obtenidos por la auditoría, con sus conclusiones, observaciones, recomendaciones y comentarios procedentes, especificando los criterios técnicos para su elaboración, contenido y presentación.

Siendo el informe el documento formal, y el producto final de la Auditoria de SI, en el cual se establecen la naturaleza, alcance y resultados de nuestros procedimientos de auditoria, su importancia es fundamental, pues resulta ser el documento que le interesa a la Entidad Auditada.

Las Normas de Auditoría Gubernamental de Nicaragua en lo que respecta a la Auditoría de Informática indican:

NAGUN 10.30 INFORME DE AUDITORIA

El informe de auditoría deberá comprender:

1. Carta de envío

2. Resumen Ejecutivo que contenga

   2.1 Antecedentes,

   2.2 Fundamento legal;

   2.3 Los objetivos y alcance de la auditoria, los procedimientos más importantes aplicados y cualquier limitación al alcance de la auditoria,

   2.4 Un breve resumen de los resultados de auditoria, control interno, cumplimiento con las leyes y regulaciones aplicables, y estado de las recomendaciones anteriores;

   2.5 Identificación de los hechos que originan responsabilidades;

   2.6 Comentarios de la administración de la entidad respecto a la aceptación del informe.

3. Informe de Auditoría informática que debe contener:

   a) Los antecedentes, acciones o circunstancias que dieron origen a la auditoría.

   b) Los objetivos, que identificarán los propósitos específicos que se cubrirán durante la misma.

c) El alcance, se referirá al sujeto, objeto y período examinados; así como a la cobertura del trabajo realizado.

d) Se debe especificar en el alcance, que la auditoría se realizó de acuerdo con las normas de auditoría gubernamental.

e) Limitaciones que no permitieron al auditor gubernamental cumplir con los objetivos previstos, estas deben ser mencionadas en el informe de manera expresa.

f) La metodología, explicará las técnicas y procedimientos que fueron empleados para obtener y analizar la evidencia; asimismo, se mencionarán los criterios y normas aplicadas durante el desarrollo del examen.

g) Resultados de Auditoría que expondrán los hallazgos significativos que tengan relación con los objetivos de auditoría, los que incluirán la información suficiente que permita una adecuada comprensión del asunto que se informa; además, la exposición de la misma debe ser objetiva y convincente, redactados conforme los atributos señalados en la NAGUN 2.80.

h) Las conclusiones, que son inferencias lógicas sobre el objeto de auditorías basadas en los hallazgos, deben ser expresadas explícitamente de manera convincente y persuasiva, evitando el riesgo de interpretaciones por parte de los lectores.

1. Evaluación de los hallazgos y conclusiones de auditoría

El análisis de los resultados de la auditoría es particularmente importante para el Auditor Informático antes de la formalización de sus informes, debido a las consecuencias legales que pueden llegar a tener tales resultados.

Las anteriores circunstancias en términos de Normas de Auditoria, requieren que el auditor informático ejerza el debido cuidado profesional con doble diligencia, obteniendo la seguridad razonable de que la información obtenida es comprobatoria, cerciorándose de su competencia y suficiencia.

Para que la evidencia sea competente, tiene que ser válida y relevante; estas cualidades dependen tanto de las circunstancias en la que se obtiene como de la confiabilidad inherente a cada tipo de evidencia, por ejemplo:

La evidencia obtenida de fuentes independientes fuera de la Entidad es más confiable que la obtenida dentro de la misma Entidad.

La evidencia producida por un sistema de administración y control interno eficaz por su diseño y cumplimiento es más confiable en el centro de cómputo que la que se obtiene de un sistema que no esta integrado en el.

Las evidencias obtenidas directamente por el auditor de sistema en la aplicación de procedimientos como la inspección, observación y cálculos es más confiable que la información obtenida indirectamente, como por ejemplo, a través de la confianza en los usuarios de los sistemas de computación o de empleados del Centro de Cómputo.

La suficiencia de la evidencia, consiste en la cantidad de información de prueba que a juicio del auditor sea necesaria para formarse una opinión sobre lo que examina. No existe como ya se dijo, rigidez en la condición de la evidencia, este es un asunto de criterio, el cual puede ser influido por el muestreo y el riesgo correlativo que asume el auditor.

Si los papeles de trabajo han sido preparados en tal forma que no haya duda sobre la procedencia de la evidencia (fuente) y si existe claridad sobre el problema (hay ejemplos considerados representativos o materiales) incluyendo verificaciones, discusiones con funcionarios autorizados, observaciones físicas, testimonios de terceros, etc.

En conclusión, el juicio del auditor de sistema sobre la suficiencia y competencia de la evidencia incluirá reflexionar en cada caso, si una persona prudente al conocer tal evidencia sin tener conocimiento profundo del asunto, puede llegar a su misma conclusión.

2. Tipos de informes

Por los objetivos de la auditoría practicada los informes pueden emitirse:

- Informe de Auditoría Informático sobre todo el Sistema Computarizado como tal, aplicado a los controles generales del Computador
- Informe de Auditoría a los Controles de Aplicación
- Informe de Auditoría Informático sobre un programa específico, ejemplo de Recursos Humanos, de control de llamadas telefónicas, etc.

3. Discusión de informes

Las recomendaciones para mejorar la eficacia de los Sistemas y la tecnología de la información, auditados, serán explicadas al máximo ejecutivo de la Entidad al hacer entrega del informe respectivo.

La discusión de informes no es solo al intercambio verbal que se haga con el mencionado ejecutivo de la Entidad al hacerle entrega del Informe preliminar, sino que también deberá considerarse como discusión al proceso de intercambio verbal y en ocasiones escrito sobre los hallazgos de auditoría, entre los miembros del equipo de auditoría y funcionarios pertenecientes a niveles apropiados de la Entidad, de tal forma que sus comentarios tengan la credibilidad necesaria para ser tomados en cuenta en el informe.

La discusión de los hallazgos previa a la presentación del informe ante la máxima autoridad, debe hacerse con los siguientes objetivos:

Indagar o completar la información sobre las causas de los hallazgos y ampliar conocimientos sobre los problemas.

Obtener los puntos de vista de los empleados con responsabilidad sobre los hallazgos, en cuanto a la manera como ellos podrían solucionar los problemas.

Disminuir la resistencia de los empleados a las recomendaciones de la auditoría vinculándolos al proceso de cambio.

La información verbal cuando es obtenida por los auditores de sistemas a medida que identifican las deficiencias y excepciones mediante entrevistas informales, suele quedar documentada en los papeles de trabajo como parte de cada hallazgo; en cada caso deberá especificarse al responsable de tal información y si ella es corroborable, el auditor debe hacerlo y dejar constancia de ello.

Cuando la información verbal es obtenida en reuniones específicas para el efecto, se debe asegurar que el auditor informático y por parte de los empleados involucrados de la Empresa, cuando menos dos funcionarios autorizados para tal fin, entre los cuales deberá estar presente el responsable del Centro de Computo y de la unidad operativa sobre la que versarán los hallazgos a discutir.

Al comienzo y durante la entrevista se mantenga un tono cordial y constructivo, ello significa que la actitud del auditor debe orientarse a obtener información y no a entrar en conflicto o debate.

Se promueva un ambiente mutuo de cooperación y entendimiento de los hechos reales, de sus causas y de las medidas correctivas.

ANEXOS

ANEXOS

Esta sección presenta modelos de cuestionarios y programas de auditoría que el Auditor Informático puede utilizar como guía en la preparación de Cuestionarios, entrevistas y programas a la medida.

1. Cuestionarios

1.1 Revisión de Control Interno General

REF	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
	1. ¿Actualmente se cuenta con una gráfica de la organización? 2. ¿Las funciones de control de inventarios, asignación de equipos, definición de funciones, otorgamiento de licencias están separadas? 3. ¿De quién depende directamente el jefe de departamento de inventarios, de software, de contratación, de mantenimiento de pequeño y grande equipo? 4. ¿Tiene la compañía auditor interno? ¿De quién depende? Describir brevemente el trabajo del auditor interno. 5. ¿Se usa un catálogo de equipo, software y funciones del personal? 6. ¿Actualmente hay algún manual o instructivo de asignación de equipo, de software, de mantenimiento, de operación? 7. ¿Se preparan y entregan a la alta gerencia mensualmente reportes de los activos tangibles o intangibles tecnológicos de la empresa? 8. ¿Se tiene control presupuestal de los costos y gastos?				

	9. ¿Quién autoriza las compras de nuevos equipos, licencias y actualización del hardware y software? 10. ¿Se hacen estudios y se documenta todo aquello que sirve para la determinación de una adquisición? 11. ¿Ha definido el consejo de administración la política general con respecto a seguros y monto de los mismos? ¿Se revisa pro algún funcionario público responsable, el monto y la cobertura de los seguros? 12. ¿Existe una revisión periódica de los mantenimientos preventivos? ¿En el área hay alguna persona encargada de supervisarlos y aprobarlos?				

1.2 Cuestionario sobre Planes generales

REF	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
	1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro? 2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia? 3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios? 4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo? 5. Escribir la lista de proyectos a corto plazo y largo plazo. 6. Escribir una lista de sistemas en proceso periodicidad y usuarios. 7. Quién autoriza los proyectos? 8. Cómo se asignan los recursos? 9. ¿Cómo se estiman los tiempos de duración? 10. ¿Quién interviene en la planeación de los proyectos? 11. ¿Cómo se calcula el presupuesto del proyecto? 12. ¿Qué técnicas se usan en el control de los proyectos? 13. ¿Quién asigna las prioridades? 14. ¿Cómo se asignan las prioridades? 15. ¿Cómo se controla el avance del proyecto?				

	16. ¿Con qué periodicidad se revisa el reporte de avance del proyecto? 17. ¿Cómo se estima el rendimiento del personal? 18. ¿Con que frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado? 19. ¿Qué acciones correctivas se toman en caso de desviaciones? 20. ¿Qué pasos y técnicas siguen en la planeación y control de los proyectos? Enumérelos secuencialmente. • Determinación de los objetivos. • Señalamiento de las políticas. • Designación del funcionario responsable del proyecto. • Integración del grupo de trabajo. • Integración de un comité de decisiones. • Desarrollo de la investigación. • Documentación de la investigación. • Factibilidad de los sistemas. • Análisis y valuación de propuestas. • Selección de equipos. 21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados? De análisis De programación Observaciones 22. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual.				

1.3 Cuestionario para la evaluación del diseño y prueba de los sistemas:

REF	PREGUNTAS	SI	NO	N/A
	1. ¿Quiénes intervienen al diseñar un sistema? • Usuario. • Analista. • Programadores. • Operadores. • Gerente de departamento. • Auditores internos. • Asesores. • Otros. 2. ¿Los analistas son también programadores? 3. ¿Qué lenguaje o lenguajes conocen los analistas? 4. ¿Cuántos analistas hay y qué experiencia tienen? 5. ¿Qué lenguaje conocen los programadores? 6. ¿Cómo se controla el trabajo de los analistas? 7. ¿Cómo se controla el trabajo de los programadores? 8. Indique qué pasos siguen los programadores en el desarrollo de un programa: • Estudio de la definición • Discusión con el analista • Diagrama de bloques • Tabla de decisiones • Prueba de escritorio • Codificación • ¿Es enviado a captura o los programadores capturan? • ¿Quién los captura? • Compilación ( ) • Elaborar datos de prueba • Solicitar datos al analista • Correr programas con datos • Revisión de resultados • Corrección del programa • Documentar el programa • Someter resultados de prueba • Entrega del programa 9. ¿Qué documentación acompaña al programa cuando se entrega?			

1.4 Cuestionario sobre control de información

Permite evaluar la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información, para lo cual se puede utilizar el siguiente cuestionario:

1. Indique el porcentaje de datos que se reciben en el área de captación

_____

2 Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos:

Número de folio _____
Número(s) de formato(s) _____
Fecha y hora de Nombre, Depto. _____
Recepción Y Usuario _____
Nombre del documento _____
Nombre responsable _____
Volumen aproximado _____
Clave de cargo de registro _____
Número de cuenta Número de registros _____
Fecha y hora de entrega de Clave del capturista _____
documentos y registros captados _____
Fecha estimada de entrega _____

3 Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:

Firmas de autorización _____
Recepción de trabajos _____
Control de trabajos atrasados _____
Revisión del documento Avance de trabajos _____
Fuente (legibilidad, verificación de datos completos, etc.)_____
Prioridades de captación _____
Errores por trabajo _____
Producción de trabajo _____
Corrección de errores _____
Producción de cada operador _____
Entrega de trabajos _____
Verificación de cifras _____
Costo Mensual de trabajo de control de entrada con las de salida_____

4 ¿Existe un programa de trabajo de captación de datos?

a) ¿Se elabora ese programa para cada turno? Diario ( ) Semanalmente ( ) mensual ( )
b) La elaboración del programa de trabajos se hace:
Internamente ( ) ; Se les señalan a los usuarios las prioridades ( )

c) ¿Que acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?

5. ¿Quién controla las entradas de documentos fuente?

_____

_____

6. ¿En qué forma las controla?

_____

_____

7. ¿Qué cifras de control se obtienen?

Sistema Cifras que se obtienen

_____

8. ¿Qué documento de entrada se tienen?

Sistemas Documentos que proporciona_____
Depto._____
Periodicidad_____
Observaciones _____

9. ¿Se anota que persona recibe la información y su volumen? SI_____ NO _____

10. ¿Se anota a que capturista se entrega la información, el volumen y la hora? SI_____ NO ____

11. ¿Se verifica la cantidad de la información recibida para su captura? SI _____ NO_____

12. ¿Se revisan las cifras de control antes de enviarlas a captura? SI _____ NO _____

13. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida? SI _____ NO _____

14. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?

_____

_____

15. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?_____

16. Si se queda en el departamento de sistemas, ¿Por cuánto tiempo se guarda?

_____

17. ¿Existe un registro de anomalías en la información debido a mala codificación?

_____

18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?

_____

19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?

_____
_____

20. ¿Se hace una relación de cuándo y a quién fueron distribuidos los listados?

_____
_____

21. ¿Se controlan separadamente los documentos confidenciales?

_____

22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?

_____

23. ¿Existe un registro de los documentos que entran a capturar?

_____
_____

24. ¿Se hace un reporte diario, semanal o mensual de captura?

_____

25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?

_____
_____

26. ¿Se lleva un control de la producción por persona?

_____
_____

27. ¿Quién revisa este control?

_____
_____

28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

_____
_____

1.5 Cuestionario sobre Control de Operación

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

El objetivo del llenado de este cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

PREGUNTAS:

1. ¿Existen procedimientos formales para la operación del sistema de computo? SI ( ) NO ( )

2. ¿Están actualizados los procedimientos? SI ( ) NO ( )

3. Indique la periodicidad de la actualización de los procedimientos: Semestral ( ) Anual ( )
   Cada vez que haya cambio de equipo ( )

4. Indique el contenido de los instructivos de operación para cada aplicación:
   Identificación del sistema
   Identificación del programa
   Periodicidad y duración de la corrida
   Especificación de formas especiales
   Especificación de cintas de impresoras
   Etiquetas de archivos de salida, nombre, archivo lógico, y fechas de creación y expiración
   Instructivo sobre materiales de entrada y salida
   Altos programados y las acciones requeridas
   Instructivos específicos a los operadores en caso de falla del equipo
   Instructivos de reinicio
   Procedimientos de recuperación para proceso de gran duración o criterios
   Identificación de todos los dispositivos de la máquina a ser usados
   Especificaciones de resultados (cifras de control, registros de salida por archivo, etc.)

5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)? SI ( ) NO ( )

6. ¿Son suficientemente claras para los operadores estas órdenes? SI ( ) NO ( )
7. ¿Existe una estandarización de las ordenes de proceso? SI ( ) NO ( )

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados. SI ( ) NO ( )

9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo? Primero que entra, primero que sale, se respetan las prioridades, Otra (especifique)

10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?
SI ( ) NO ( )

11. ¿Quién revisa este reporte en su caso?

_____
_____

12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.

_____
_____

13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?

_____
_____

14. ¿Cómo se actúa en caso de errores?

_____
_____

15. ¿Existen instrucciones especificas para cada proceso, con las indicaciones pertinentes?

_____
_____

16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

_____
_____

17. ¿Puede el operador modificar los datos de entrada?

_____
_____

18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?

_____
_____

19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?

_____
_____

20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?

_____
_____

21. ¿Las intervenciones de los operadores:
a) Son muy numerosas? SI ( ) NO ( ); b) Se limitan los mensajes esenciales? SI ( ) NO( )
Otras (especifique)_____

22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?
SI ( ) NO ( )

23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?

24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?
SI ( ) NO ( )

25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos? SI ( ) A MAQUINA ( ) MANUAL ( ) NO ( )

26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.

_____
_____

27.¿Existen procedimientos para evitar las corridas de programas no autorizados?
SI ( ) NO ( )

28. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.

_____
_____

29. Verificar que sea razonable el plan para coordinar el cambio de turno.

_____
_____

30. ¿Se hacen inspecciones periódicas de muestreo? SI ( ) NO ( )

31. Enuncie los procedimientos mencionados en el inciso anterior:

32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo? SI ( ) NO ( )

33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias? SI ( ) NO ( )
¿Cómo?_____

34. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.

_____
_____

35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos? SI ( ) NO ( )

_____
_____

36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores? SI ( ) NO ( )

_____
_____

37. ¿Durante cuanto tiempo?

_____
_____

38. ¿Que precauciones se toman durante el periodo de implantación?

_____
_____

39. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.

_____
_____

40. ¿Se catalogan los programas liberados para producción rutinaria? SI ( ) NO ( )

_____
_____

41. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.

_____
_____

42. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.

_____
_____

43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo? SI ( ) NO ( )

_____
_____

44. Indique como está organizado este archivo de bitácora.
Por fecha ( ) por fecha y hora ( ) por turno de operación ( ) Otros ( )

45. ¿Cuál es la utilización sistemática de las bitácoras?

_____
_____

46. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?

_____
_____

47. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.

_____
_____

48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización? SI ( ) NO ( )

_____
_____

49. ¿Cómo se controlan los procesos en línea?

_____
_____

50. ¿Se tienen seguros sobre todos los equipos? SI ( ) NO ( )

_____
_____

51. ¿Conque compañía? Solicitar pólizas de seguros y verificar tipo de seguro y montos.

_____
_____

52. ¿Cómo se controlan las llaves de acceso (Password)?.

_____
_____

1.6 Cuestionario sobre controles de salida

1. ¿Se tienen copias de los archivos en otros locales?

_____

2. ¿Dónde se encuentran esos locales?

_____
_____
_____

3. ¿Que seguridad física se tiene en esos locales?

_____
_____
_____

4. ¿Que confidencialidad se tiene en esos locales?

_____
_____
_____

5. ¿Quién entrega los documentos de salida?

_____
_____

6. ¿En que forma se entregan?

_____
_____

7. ¿Que documentos?

_____
_____
_____

8. ¿Que controles se tienen?

_____
_____
_____

9. ¿Se tiene un responsable (usuario) de la información de cada sistema? ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

_____

10. ¿Se destruye la información utilizada, o bien que se hace con ella?
Destruye ( ) Vende ( ) Tira ( ) Otro_____

1.7 **Cuestionario de control de medios de almacenamiento masivo**

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además se deben tener perfectamente identificados los archivos para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cintoteca y discoteca tienen:
   - Aire acondicionado ( )
   - Protección contra el fuego ( )
   - (señalar que tipo de protección)_____
   - Cerradura especial ( )
   - Otra
   -

2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego? SI ( ) NO ( )
   (señalar de que tipo)_____

3. ¿Qué información mínima contiene el inventario de la cintoteca y la discoteca?
   - Número o clave del usuario _____
   - Número del archivo lógico _____
   - Nombre del sistema que lo genera _____
   - Fecha de expiración del archivo _____
   - Fecha de expiración del archivo_____
   - Número de volumen _____
   - Otros _____

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?
   SI ( ) NO ( )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias? SI ( ) NO ( )

6. ¿Que tan frecuentes son estas discrepancias?

_____

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo inadvertidamente destruido? SI ( ) NO ( )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso? SI ( ) NO ( )
¿Cómo?_____

9. ¿Existe un control estricto de las copias de estos archivos? SI ( ) NO ( )

10. ¿Que medio se utiliza para almacenarlos? Mueble con cerradura ( ); Bóveda ( )
Otro (especifique)_____

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?
SI ( ) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos? SI ( ) NO ( )

14. ¿Se realizan auditorías periódicas a los medios de almacenamiento? SI ( ) NO ( )

15. ¿Qué medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

---

16 ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado? SI ( ) NO ( )

17. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?
SI ( ) NO ( )

18. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán? SI ( ) NO ( )

20. ¿Se lleva control sobre los archivos prestados por la instalación? SI ( ) NO ( )

21. En caso de préstamo ¿Conque información se documentan?

- fecha de recepción ( )
- fecha en que se debe devolver ( )
- archivos que contiene ( )
- formatos ( )
- cifras de control ( )
- código de grabación ( )
- nombre del responsable que los presto ( )
- otros (

22. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo? SI ( ) NO ( )

23. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos? SI ( ) NO ( )

24. ¿Estos procedimientos los conocen los operadores? SI ( ) NO ( )

25. ¿Con que periodicidad se revisan estos procedimientos? MENSUAL ( ) ANUAL ( ) SEMESTRAL ( ) OTRA ( )

26. ¿Existe un responsable en caso de falla? SI ( ) NO ( )

27. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

---

28. ¿Existe un procedimiento para el manejo de la información? SI ( ) NO ( )

1.8 **Cuestionario de Control de mantenimiento**

Como se sabe existen básicamente tres tipos de contrato de mantenimiento:

El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes.

El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es "por llamada", en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como "en banco", y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cuál de los tres tipos es el más conveniente y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales. Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación.

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

PREGUNTAS

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).

_____
_____

2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computo? SI ( ) NO ( )

3. ¿Se lleva a cabo tal programa? SI ( ) NO ( )

4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos? SI ( ) NO ( )

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido? SI ( ) NO ( )

5. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.- SI ( ) NO ( )

6. ¿Cómo se notifican las fallas?

_____
_____

9. ¿Cómo se les da seguimiento?

_____
_____

1.9 Cuestionario Sobre el orden y cuidado del centro de cómputo

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de informática o cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

PREGUNTAS

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:

   Semanalmente ( ) Quincenalmente ( )
   Mensualmente ( ) Bimestralmente ( )
   No hay programa ( ) Otra (especifique) ( )

2. Existe un lugar asignado a las cintas y Archivos de discos? SI ( ) NO ( )

3. ¿Se tiene asignado un lugar especifico para papelería y utensilios de trabajo?
   SI ( ) NO ( )

4. ¿Son funcionales los muebles asignados para el archivo de a cintas, discos y otros?
   SI ( ) NO ( )

5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.? SI ( ) NO ( )

6. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo? SI ( ) NO ( )

6. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición? SI ( ) NO ( )

7. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática? SI ( ) NO ( )

8. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo:

_____

_____

1.10 Cuestionario para la Evaluación de la configuración del sistema de cómputo

Los objetivos son evaluar la configuración actual tomando en consideración las aplicaciones y el nivel de uso del sistema, evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de la instalación y revisar las políticas seguidas por la unidad de informática.

Esta sección está orientada a:

a) Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo actual o de comparar la capacidad instalada con los planes de desarrollo a mediano y largo plazo.
b) Evaluar las posibilidades de modificar el equipo para reducir el costo o bien el tiempo de proceso.
c) Evaluar la utilización de los diferentes dispositivos periféricos.

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo y diferentes áreas de la Entidad. ¿existe equipo?
   ¿Con poco uso? SI ( ) NO ( )
   ¿Ocioso? SI ( ) NO ( )
   ¿Con capacidad superior a la necesaria? SI ( ) NO ( )

Describa cual es _____

2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro más lento y de menor costo? SI ( ) NO ( )

3. Si la respuesta al inciso anterior es negativa, ¿el equipo puede ser cancelado? SI ( ) NO ( )

4. De ser negativa la respuesta al inciso anterior, explique las causas por las que no puede ser cancelado o cambiado. _____

5. ¿El sistema de cómputo tiene capacidad de teleproceso? SI ( ) NO ( )

6. ¿Se utiliza la capacidad de teleproceso? SI ( ) NO ( )

7. ¿En caso negativo, exponga los motivos por los cuales no utiliza el teleproceso? SI ( ) NO ( )

7. ¿Cuántas terminales se tienen conectadas al sistema de cómputo?
   _____

8. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios? SI ( ) NO ( )

9. ¿La capacidad de memoria y de almacenamiento máximo del sistema de cómputo es suficiente para atender el proceso por lotes y el proceso remoto? SI ( ) NO ( )

1.11 Cuestionario de Evaluación de la Seguridad física

El objetivo es comprobar que se han establecido políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.

Entre las precauciones que se deben revisar están:

* Los ductos del aire acondicionado están limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
* En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
* En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.
* Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
* Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
* También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
* Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.
* Los materiales mas peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

PREGUNTAS

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información? SI ( ) NO ( )

2. ¿Existen una persona responsable de la seguridad? SI ( ) NO ( )

3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad? SI ( ) NO ( )

4. ¿Existe personal de vigilancia en la institución? SI ( ) NO ( )

4. ¿La vigilancia se contrata?
   a) Directamente ( )
   b) Por medio de empresas que venden ese servicio ( )

5. ¿Existe una clara definición de funciones entre los puestos clave? SI ( ) NO ( )

7. ¿Se investiga a los vigilantes cuando son contratados directamente? SI ( ) NO ( )

7. ¿Se controla el trabajo fuera de horario? SI ( ) NO ( )

9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?. SI ( ) NO ( )

10. ¿Existe vigilancia en el departamento de cómputo las 24 horas? SI ( ) NO ( )

11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas? a) Vigilante ? ( ) b) Recepcionista? ( ) c) Tarjeta de control de acceso ? ( ) d) Nadie? ( )

12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores? SI ( ) NO ( )

13. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización? SI ( ) NO ( )

14. El edificio donde se encuentra la computadora está situado a salvo de:
a) Inundación? ( )
b) Terremoto? ( )
c) Fuego? ( )
d) Sabotaje? ( )

15. El centro de cómputo tiene salida al exterior al exterior? SI ( ) NO ( )

16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.

17. ¿Existe control en el acceso a este cuarto?
a) Por identificación personal? ( )
b) Por tarjeta magnética? ( )
c) por claves verbales? ( )
d) Otras? ( )

18. ¿Son controladas las visitas y demostraciones en el centro de cómputo? SI ( ) NO ( )

19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática? SI ( ) NO ( )

20. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude? SI ( ) NO ( )

21. ¿Existe alarma para
a) Detectar fuego(calor o humo) en forma automática? ( )

b) Avisar en forma manual la presencia del fuego? ( )
c) Detectar una fuga de agua? ( )
d) Detectar magnéticos? ( )
e) No existe ( )

22. ¿Estas alarmas están:
a) En el departamento de cómputo? ( )
b) En otro lugar? ( )

23. ¿Existe alarma para detectar condiciones anormales del ambiente?
a) En el departamento de cómputo? ( )
b) En otros lados ( )

24. ¿La alarma es perfectamente audible? SI ( ) NO ( )

25.¿Esta alarma también está conectada
a) Al puesto de vigilancia ? ( )
b) A la estación de Bomberos? ( )
c) A ningún otro lado? ( )
Otro_____

26. Existen extintores de fuego
a) Manuales? ( )
b) Automáticos? ( )
c) No existen ( )

27. ¿Se ha adiestrado el personal en el manejo de los extintores? SI ( ) NO ( )

28. ¿Los extintores, manuales o automáticos a base de

TIPO	SI	NO
a) Agua,	( )	( )
b) Gas?	( )	( )
c) Otros	( )	( )

29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores? SI ( ) NO ( )

30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego? SI ( ) NO ( )

31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause más daño que el fuego? SI ( ) NO ( )

32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause mas daño que el fuego? SI ( ) NO ( )

33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal

a) Corte la acción de los extintores por tratarse de falsas alarmas? SI ( ) NO ( )
b) Pueda cortar la energía Eléctrica SI ( ) NO ( )
c) Pueda abandonar el local sin peligro de intoxicación SI ( ) NO ( )
d) Es inmediata su acción? SI ( ) NO ( )

34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos? SI ( ) NO ( )

35. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego? SI ( ) NO ( )

36. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)? SI ( ) NO ( )

37. ¿Existe salida de emergencia? SI ( ) NO ( )

38. ¿Esta puerta solo es posible abrirla:
a) Desde el interior ? ( )
b) Desde el exterior ? ( )
c) Ambos Lados ( )

39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen? SI ( ) NO ( )

40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia? SI ( ) NO ( )

41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
a) Evitando artículos inflamables en el departamento de cómputo? ( )
b) Prohibiendo fumar a los operadores en el interior? ( )
c) Vigilando y manteniendo el sistema eléctrico? ( )
d) No se ha previsto ( )

42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo? SI ( ) NO ( )

43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe? SI ( ) NO ( )

44. ¿Se controla el acceso y préstamo en la
    a) Discoteca? ( )
    b) Cintoteca? ( )
    c) Programoteca? ( )

45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.

_____
_____

46. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora? SI ( ) NO ( )

47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.

_____
_____

48. ¿Se tienen establecidos procedimientos de actualización a estas copias? SI ( ) NO ( )

49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

_____
_____

50. ¿Existe departamento de auditoria interna en la institución? SI ( ) NO ( )

51. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?
SI ( ) NO ( )

52. ¿Que tipos de controles ha propuesto?

_____
_____

53. ¿Se cumplen? SI ( ) NO ( )

54. ¿Se auditan los sistemas en operación? SI ( ) NO ( )

55.¿Con que frecuencia?
    a) Cada seis meses ( )
    b) Cada año ( )
    c) Otra (especifique) ( )

56.¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?

a) Usuario ( )
b) Director de informática ( )
c) Jefe de análisis y programación ( )
d) Programador ( )
e) Otras (especifique) _____

57.¿La solicitud de modificaciones a los programas se hacen en forma?

a) Oral? ( )
b) Escrita? ( )

En caso de ser escrita solicite formatos,

58.Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
SI ( ) NO ( )

59.¿Existe control estricto en las modificaciones? SI ( ) NO ( )

60.¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
SI ( ) NO ( )

61.¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?
SI ( ) NO ( )

62.Se verifica identificación:

a) De la terminal ( )
b) Del Usuario ( )
c) No se pide identificación ( )

63.¿Se ha establecido que información puede ser acezada y por qué persona? SI ( ) NO ( )

64.¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella? SI ( ) NO ( )

65.¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores? SI ( ) NO ( )

66.¿Existen controles y medidas de seguridad sobre las siguientes operaciones?
¿Cuáles son? ( )
Recepción de documentos_____
( ) Información Confidencial_____
( ) Captación de documentos_____
( ) Cómputo Electrónico_____
( ) Programas_____
( ) Discotecas y Cintotecas_____
( ) Documentos de Salida_____

( ) Archivos Magnéticos_____
( ) Operación del equipo de computación_____
( ) En cuanto al acceso de personal_____
( ) Identificación del personal_____
( ) Policia_____
( ) Seguros contra robo e incendio_____
( ) Cajas de seguridad_____
( ) Otras (especifique)_____

1.12 Cuestionario sobre Control de inventarios

REF	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
	1. ¿Se almacenan las existencias en una forma sistemática?				
	2. ¿Están protegidas de modo adecuado para evitar su deterioro físico contándose con seguros contraincendio, daños, robo, etc.?				
	3. ¿Están bajo el control directo de almacenistas responsables por las cantidades en existencia?				
	4. ¿Están construidos y segregados los almacenes y áreas de almacenaje de manera de evitar el acceso a personas no autorizadas?				
	5. ¿Se llevan los registros de los inventarios constantes por personas que no tengan a su cargo los almacenes?				
	6. ¿Las actas de resguardo están actualizadas?				
	7. ¿Se tiene un procedimiento para detectar o permitir la sugerencia de mantenimiento del equipo cuando ha tenido alguna falla?				
	8. ¿Se sigue el procedimiento de investigación de la falla del equipo para hacer el cargo de responsabilidad a quien tiene el resguardo, cuando ha sido por descuido personal?				
	9. ¿Informan los almacenistas a sus superiores cuando han recibido el equipo? ¿Informan el estado en que fue entregado y recibido? ¿Se lleva algún reporte al respecto?				
	10. Se entregan los abastecimientos, licencias, accesorios, equipo personal, suministros, mediante requisiciones, vale de salida o indicación precisa pero escrita y con firma de autorización?				
	11. En tal caso, son las requisiciones o vales: ¿Preparados por otra persona que no sea el almacenista? ¿Hechos en formas prenumeradas y controlando el orden numérico?				
	12. Si algún equipo ya es obsoleto, o no se está utilizando, ¿Existe algún procedimiento para sustituirlo o para fomentar que el usuario informe y lo entregue?				

1.13 Cuestionario Activo Fijo (planta y equipo informático)

REF	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
	1. ¿Dónde está ubicado el site? ¿Dónde están ubicados los respaldos? ¿Dónde están ubicados los bienes de activo fijo? 2. ¿Existe descripción breve de los bienes de activo fijo? 3. ¿Existen políticas definidas sobre la autorización de inversiones en activo fijo, y que estén a cargo de determinadas personas o comités? 4. ¿Las erogaciones en demasía de lo autorizado están sujetas a la misma aprobación que la autorización original? 5. ¿Los registros del activo fijo contienen la suficiente información y detalle, según las necesidades de la entidad? 6. ¿Se hace periódicamente un inventario físico del activo fijo y se compara con los registros respectivos? 7. ¿Las personas que tienen a su cuidado el activo fijo, están obligadas a reportar cualquier cambio habido como baja, obsolescencia, traspasos? 8. ¿El traspaso a otros centros, unidades o áreas de trabajo dentro de la entidad requiere de la autorización de los Directivos del área administrativa e informática? 9. ¿Se encuentran debidamente controladas las licencias en documento físico contra quienes realmente la tienen en uso? 10. ¿Se hacen investigaciones y avalúos periódicos para fines de aseguramiento? 11. ¿Se hace periódicamente levantamiento de información para detectar las necesidades en cuanto a equipo personal?				

1.14 Cuestionario sobre Uso del Correo electrónico; asignación de licencia

REF	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
	1. . ¿Cuál es su categoría profesional? ¿Alto mando, medio mando, operativo, analista, secretaria, otro? 2. ¿Cuál es su actitud hacia los medios de comunicación?: Desconfianza, Positiva, Reticencia, Completamente positiva, Indiferencia 3. ¿Cuál es su actitud hacia el correo? 4. ¿Qué ventajas observa sobre el uso del correo para desempeñar su trabajo? 5. ¿Cuáles son los principales problemas en el uso del correo? 6. ¿Sabía de la existencia de empresas que controlan los mensajes de sus empleados? 7. ¿Considera adecuada o justificada su actuación? 8. ¿Existen en su ámbito de trabajo normativas relativas a la utilización del correo electrónico? 9. ¿Qué medidas de seguridad especifica? 10. ¿Cuánto tiempo utiliza diariamente su correo electrónico? 11. ¿Cuál es el número de mensajes que envía diariamente? 12. ¿Cuál es el porcentaje de mensajes cuyo contenido es estrictamente laboral?				

2. Programas de auditoría

2.1 Programa de análisis de Software

		HECHO	INDICE	FECHA
	I. Objetivos Verificar la seguridad, control de los sistemas, seguridad, calidad de la información y sistemas en uso para determinar la efectividad y eficiencia de los mismos. **II. Procedimientos** **Software del Sistema** 1. Software del sistema (software de base) se deberá comprobar que: a) Existan control de modificaciones al sistema operativo b) Que se evite realizar cambios no autorizados y el uso incontrolable de herramientas potentes c) Revisión de los procedimientos de obtención de backup. d) Existencia de la Metodología de selección de paquetes de software e) Evaluación de herramientas de desarrollo de sistemas y software de gestión de la base de datos. 2. Efectúe revisión del Software de la base de datos y verifique que: a) La integridad de la base de datos b) Que se hayan establecido estándares de documentación c) Existencia de backup d) Uso de utilitarios y modificaciones de los métodos de acceso. 3. Efectúe medición de los Riesgos en una base de datos: a) Inexactitud de los datos b) Inadecuada asignación de responsabilidades c) Acceso no autorizado a datos d) Documentación no actualizada e) Adecuación de las pistas de auditoría.			

	Sistemas de procesamiento distribuido y redes 4. Revise el sistema de distribución y redes y compruebe: a) Provee abastecimiento de información sobre una base descentralizada. b) Existen planes de implantación, conversiones y pruebas de aceptación adecuadas de la red. c) Existen estándares y políticas para el control de la red. d) Poseen facilidades de control del hardware y el software e) Existe compatibilidad, en la integridad y el uso de datos. f) Existe control de acceso a datos g) Existe un Software de comunicación y sistema operativo de red – control de rendimiento de la red. **Sistemas basados en microcomputadoras** 5. Efectúe revisión de los equipos de microcomputadores existentes y compruebe: a) Los Criterio de adquisición, y políticas de asignación de equipos b) Software aplicativo, de desarrollo y sistema operativo, en uso. c) Documentación de programas d) Procedimientos para la creación y mantenimiento de archivos. e) Seguridad física f) Compartir recursos / autorización g) Programas de mantenimiento **Sistemas Online** 6. Realice revisión de los sistemas Online y compruebe: a. Que el usuario tiene acceso directo al sistema y lo controla de algún modo a través de terminales del software disponible. b. Existen sistemas de consultas c. Procedimientos de Entrada de datos Online (validaciones) d. Actualización de datos Online (actualización de archivos maestros) e. Remote Job Entry (un punto remoto actúa con control total del ordenador central)			

	f. Programación Online, permite a los programadores trabajar desde puntos remotos del equipo central 7. Realice análisis del acceso Online y compruebe que ningún usuario puede acceder a datos que no debería o realizar procesos no permitidos, en este caso verifique: a. Que las passwords de los usuarios posean cambios periódicos b. Perfiles de usuarios (acceso limitado a archivos) c. Bloqueo de terminales (time out o intentos de acceso) d. Logueo de actividades del usuario e. Encriptación de datos. 8. Del Análisis de las consultas Online, verifique que el usuario no pueda modificar datos de los archivos, para ello investigue:. a) Control de acceso al sistema b) Uso de la información obtenida. c) Tiempo de respuesta. 9. Realice análisis de la introducción de datos Online y determine la existencia de problemas son de control, validación y corrección de los mismos, compruebe:. a) Control de acceso al sistema b) Existencia de procedimientos previos a la entrada de datos, tratamiento de documentación, autorización adecuada. c) Sistema de control que permita verificar la totalidad de los datos de entrada. d) Controles que protejan contra omisiones o duplicaciones de datos. e) Calidad de la validación f) Existencia de registros de las correcciones efectuadas en caso de fallo del sistema: g) Métodos que determinen que transacciones se ha perdido h) Procedimientos Batch de reemplazo. i) Procedimientos para comprobar el estado del sistema (luego del reinicio) 10. Verifique los procedimientos de actualización online y compruebe: a. Existencia de Controles de acceso al sistema b. Se establecen puntos de control en la entrada c. Mantiene logs de actualizaciones			

	d. Se realizan validaciones sobre los registros actualizados e. Existe la autoridad necesaria para la actualización del usuario. f. Proveen oportunamente la corrección de errores y su impacto. g. Mantienen una relación de los archivos maestros que se hayan modificado, indicando el movimiento antes y después de la modificación. 11. Realice análisis de la seguridad Online a. Disponibilidad de equipos alternativos para cubrir necesidades mínimas. b. Existencia de planes de emergencia, documentados y practicados. c. Seguridad de archivos, backup, etc. d. Medidas de seguridad contra accesos no autorizados. 12. Compruebe el control de la entrada de remote Job entry, los niveles de autorización del usuario. Se deberá comprobar que: a) Acceso de programadores autorizados b) Registro del uso del sistema con emisión de informes periódicos c) Trabajos de programación autorizados y controlados. 13. Compruebe el desarrollo de aplicaciones Online sobre: a. Asegurar rutinas de validación b. Existencia de ayudas en las terminales c. Procedimientos de corrección y modificación Online d. Control de acceso simultanea a registros .			

2.2 Programas de Apoyo al Software del Sistema

		HECHO	INDICE	FECHA
	I. **Objetivos** Determinar la efectividad de los procedimientos para adquirir, implementar y mantener el software del sistema (es decir, el sistema operativo y otro software que no se relaciona directamente con los sistemas de aplicación), incluyendo las funciones y responsabilidades de cualesquier individuos o grupos involucrados en este proceso. II. **Procedimientos** 1. Efectúe pruebas del software de sistemas nuevos y/o modificaciones al software existente 2. Evalúe el impacto del software de sistemas nuevos o modificados en el procesamiento de los sistemas de aplicación 3. Compruebe la aprobación de la implementación del software de sistemas nuevos y/o modificaciones al software existente (v. gr., nuevas versiones de dicho software) 4. Verifique si se efectúan traslados del software de los sistemas nuevos a las bibliotecas de producción (es decir, implementación de los programas nuevos o modificados) 5. Compruebe la Validación de la integridad y exactitud del procesamiento del software de los sistemas nuevos o modificados.			

2.3 Programa de Verificación del Hardware

		HECHO	INDICE	FECHA
	I. Objetivos Comprobar la seguridad, calidad y uso eficiente de los Hardware de la Entidad **II. Procedimientos** **1.** Para el sistema central de la computadora y otras computadoras o servidores importantes soportados por este ambiente de procesamiento de la computadora, proporcione la siguiente información: a) Marca, modelo b) Sistema Operativo, versión c) Ubicación d) Años de instalación **2.** Investigue cómo se da mantenimiento al equipo de la computadora? 3. Asegúrese de que cualesquier cambios a los sistemas de aplicación se documenten adecuadamente. **4.** Que exista controlo y registro de las adquisiciones, cambios o disposiciones de hardware			

2.4 Programas de Evaluación del diseño lógico de los sistemas

		HECHO	INDICE	FECHA
	I. Objetivos Determinar las especificaciones del sistema, como opera, la secuencia y ocurrencia de los datos, el proceso y salida de reportes; la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión. **II. Procedimientos** 1. Efectúe comparación del diseño lógico del sistema con lo que realmente se está obteniendo en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo. Los puntos a evaluar son: a) Entradas. b) Salidas. c) Procesos. d) Especificaciones de datos. e) Especificaciones de proceso. f) Métodos de acceso. g) Operaciones. h) Manipulación de datos (antes y después del proceso electrónico de datos). i) Proceso lógico necesario para producir informes. j) Identificación de archivos, tamaño de los campos y registros. k) Proceso en línea o lote y su justificación. l) Frecuencia y volúmenes de operación. m) Sistemas de seguridad. n) Sistemas de control. o) Responsables. p) Número de usuarios.			

	2. Solicite información de los sistemas y evalúe: a) Manual del usuario. b) Descripción de flujo de información y/o procesos. c) Descripción y distribución de información. d) Manual de formas. e) Manual de reportes. f) Lista de archivos y especificaciones. 3. Determine los procedimientos de los sistemas: a) ¿Quién hace, cuando y como? b) ¿Qué formas se utilizan en el sistema? c) ¿Son necesarias, se usan, están duplicadas? d) ¿El número de copias es el adecuado? e) ¿Existen puntos de control o faltan? 4. Investigue si el flujo de información: a) Es fácil de usar? b) ¿Es lógica? c) ¿Se encontraron lagunas? d) ¿Hay faltas de control? 5. Compruebe el diseño existe y se ajusta la herramienta al procedimiento?			

2.5 Programa de Evaluación del desarrollo del sistema

		HECHO	INDICE	FECHA
	I. Objetivos Evaluar los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema. Si el sistema de información proporciona información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. **II. Procedimientos** 1. Determinar las características de los sistemas comprobando si estos son: a) Dinámicos (susceptibles de modificarse). b) Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo) 2. Compruebe si los sistemas son Integrados en un solo objetivo. Si existen sistemas que puedan ser interrelacionados y no programas aislados. 3. Compruebe si los sistemas son: a) Accesibles (que estén disponibles). b) Necesarios (que se pruebe su utilización). c) Comprensibles (que contengan todos los atributos). d) Oportunos (que esté la información en el momento que se requiere). e) Funcionales (que proporcionen la información adecuada a cada nivel). f) Estándar (que la información tenga la misma interpretación en los distintos niveles). g) Modulares (facilidad para ser expandidos o reducidos). h) Jerárquicos (por niveles funcionales). 4. Compruebe los niveles de seguridad si sólo las personas autorizadas tienen acceso y que no se duplique información.			

2.6 Evaluación de los instructivos de operación

		HECHO	INDICE	FECHA
	I. Objetivos Evaluar los instructivos de operación de los sistemas para evitar que los programadores tengan acceso a los sistemas en operación, y el contenido mínimo de los instructivos de operación se puedan verificar mediante el siguiente cuestionario. **II. Procedimientos** 1. Comprobar que el instructivo de operación contiene a) Diagrama de flujo por cada programa. b) Diagrama particular de entrada/salida c) - Mensaje y su explicación d) - Parámetros y su explicación e) - Diseño de impresión de resultados f) - Cifras de control g) Fórmulas de verificación h) Observaciones i) Instrucciones en caso de error j) Calendario de proceso y resultados			

2.7 Programa de Evaluación de los Controles

		HECHO	INDICE	FECHA
	I. Objetivos Comprobar el control de los datos de la entidad como recursos valiosos, la responsabilidad de los mismos, clasificación, y relación con las bases de datos. II. **Procedimientos** 1. Los responsables de la captura y modificación de la información están definidos, con claves de acceso de acuerdo a niveles: a) Primer nivel de consultas b) Segundo nivel: captura y consultas c) Tercer nivel: consultas, captura y baja de datos 2. Evaluación de las entradas de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información, 3. Verificar que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. 4. Comprobar el uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos. 5. Comprobar que existan un método eficaz para proteger sistemas de computación es el software de control de acceso, tales como claves de acceso. .			

	6. Comprende el sistema integral de seguridad: a) Elementos administrativos b) Definición de una política de seguridad c) Organización y división de responsabilidades d) Seguridad física y contra catástrofes(incendio, terremotos, etc.) e) Prácticas de seguridad del personal f) Elementos técnicos y procedimientos g) Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales. h) Aplicación de los sistemas de seguridad, incluyendo datos y archivos i) El papel de los auditores, tanto internos como externos j) Planeación de programas de desastre y su prueba. 7. Se ha clasificado la instalación en términos de riesgo a) Se clasifican los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación. b) Se han identificado la información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones. 8. Se han tomado las precauciones, del riesgo que tenga la información y del tipo y tamaño de la organización. a) El personal que prepara la información no debe tener acceso a la operación. b) Los análisis y programadores no tiene acceso al área de operaciones y viceversa. c) Los operadores no debe tener acceso irrestringido a las librerías ni a los lugares donde se tengan los archivos almacenados; d) Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.			

2.8 Programa de verificación de la seguridad física

		HECHO	INDICE	FECHA
	I. Objetivos Determinar si se han establecido políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo. **II. Procedimientos** 1. Compruebe que los ductos del aire acondicionado están limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego. 2. Verifique lo siguiente: a) En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso. b) Revisar el número de extintores, su capacidad, fácil acceso, peso y tipo de producto que utilizan. c) Investigar si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso. d) Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.			

2.9 Seguridad en la utilización del equipo

		HECHO	INDICE	FECHA
	I. Objetivos Comprobar los medios de seguridad en la utilización de los equipos, accesos restringidos a programas, archivos y el monitoreo. II. **Procedimientos** 1) Compruebe la existencia de medidas de seguridad siguientes: a) Se han restringido el acceso a los programas y a los archivos. b) Los operadores trabajan con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos. c) Se aseguran en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados. d) No se permite la entrada a la red a personas no autorizadas, ni a usar las terminales. e) Se realiza periódicamente una verificación física del uso de terminales y de los reportes obtenidos. 2) Verifique que los datos recolectados sean procesados completamente, por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema. a) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema. b) Se controla la distribución de las salidas (reportes, cintas, etc.). c) Se guardan copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos. d) Se tiene un estricto control sobre el acceso físico a los archivos.			

	e) En el caso de programas, se asigna a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión. 3) Compruebe la seguridad en el manejo de información: a) Que no se obtengan fotocopias de información confidencial sin la debida autorización. b) Sólo el personal autorizado debe tener acceso a la información confidencial. c) Control de los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta. d) Control del número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales. 4) Verifique que la entidad cuente con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia. * Equipo, programas y archivos * Control de aplicaciones por terminal * Definir una estrategia de seguridad de la red y de respaldos * Requerimientos físicos. * Estándar de archivos.			

2.10 Seguridad al restaurar el equipo

		HECHO	INDICE	FECHA
	I. Objetivos Comprobar la existencia de medidas de seguridad en la restauración de equipos en casos de contingencias que permita la recuperación de datos II. Procedimientos 1. Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes: a) Se guardan copias periódicas de los archivos que permita reanudar un proceso a partir de una fecha determinada. b) Se analizan el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia. c) Se puede reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones. 2. Además de los procedimientos de recuperación y reinicio de la información, se contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares.			

2.11 Seguridad de la Información

Políticas y Procedimientos de Seguridad

Describa brevemente la naturaleza y alcance de las políticas y procedimientos de seguridad de la información:

¿Están por escrito las políticas y procedimientos de seguridad de la información del cliente?

¿Tiene el cliente un programa para hacer del conocimiento del usuario las políticas, procedimientos y prácticas de seguridad

Seguridad Lógica

En la tabla siguiente, relacione los métodos que usa el cliente para restringir el acceso lógico a los sistemas de aplicación y a la información:

	Método de Restricción de Acceso

¿Están centralizados o descentralizados el soporte y la administración de los métodos de restricción de acceso lógico?

En la tabla siguiente, relacione las técnicas que el cliente usa para autentificar la identidad de los usuarios que intentan acceder al sistema:

	Técnicas de Autentificación

Describa brevemente los procesos del cliente para autorizar el acceso a la información y para asignar los privilegios de acceso a los usuarios:

¿Se ha definido explícitamente la propiedad de la información?

¿Se ha clasificado la información para efectos de la autorización del acceso?

	¿Quién es el responsable de autorizar el acceso a la información (es decir, de aprobar una solicitud para que se le otorgue a un individuo el acceso a información específica o tipos de información)?

	¿Quién es el responsable de asignar los privilegios de acceso a los usuarios (es decir, de fijar los parámetros de software que restringen o permiten ciertos tipos de acceso a cierta información)?

	¿A quién se le permite actualizar el acceso a los datos de producción?

¿Permite el cliente el acceso externo a/desde sus sistemas de la computadora (por ejemplo, por vía de marcación telefónica o por redes externas)?

¿Permite el cliente el acceso de Internet a /desde sus sistemas de la computadora?

Describa el acceso de Internet a/desde los sistemas de la computadora del cliente. Considere lo siguiente:

- Usuarios internos y externos a quienes se les ha otorgado dicho acceso
- El propósito de tal acceso

¿Tiene el cliente una dirección World Wide Web (w.w.w.)?

¿Tienen los usuarios acceso al software escritor de informes?

¿Tienen los usuarios la capacidad de recibir datos (to download) y manipular la información del sistema de aplicación?

¿Tienen los usuarios la capacidad de transmitir datos (to up load) a los sistemas de aplicación, fuera del sistema de aplicación normal de entrada de datos?

Seguridad Física

	¿Qué métodos usa el cliente para restringir el acceso físico a esta ubicación de procesamiento?

En la tabla siguiente, relacione todos los grupos (internos y externos) cuyo acceso físico está permitido a este ambiente de procesamiento de la computadora. Por cada grupo, indique si se le ha otorgado acceso completo o restringido e indique la naturaleza de las restricciones.

	Grupo	**Naturaleza de las Restricciones de Acceso Físico, Si las Hay**

	¿Qué tipo de controles ambientales se tienen establecidos en esta ubicación de procesamiento para prevenir daños al equipo de la computadora?

Implementación y Mantenimiento de los Sistemas de Aplicación

Describa la naturaleza de la metodología del desarrollo de sistemas y mantenimiento del cliente:	Se han implementado por escrito normas, políticas y procedimientos para el desarrollo y mantención de sistema

¿Utiliza el cliente algunos sistemas de apoyo de decisiones y/o sistemas de información ejecutiva?	

¿De qué fuentes obtiene el cliente los sistemas de aplicación?

		Ciclo de Negocios	**Nombre del Sistema de Aplicación**	**Fuente**

Refiérase a la tabla anterior:

Si la fuente de alguno de los sistemas de aplicación arriba relacionados es "software comprado, con poco o sin grado de adaptación" o "software comprado, con grado importante de adaptación," verifique aquí:	

Si la fuente de alguno de los sistemas de aplicación arriba relacionados es "software de patente provisto por la organización de servicio" o "software desarrollado internamente," verifique aquí:	

¿Tiene el cliente acceso a una copia actual del código fuente para todos los sistemas de aplicación importantes?	

Implementación y Soporte de la Base de Datos

Describa la arquitectura de datos de los sistemas de aplicación soportados por esta ubicación de procesamiento.	Base de datos integrada, utilizada por todos los módulos de aplicación

En la tabla siguiente, relacione el software de administración de la base de datos usado por los sistemas de aplicación soportados por este ambiente de procesamiento de la computadora y los sistemas de aplicación correspondientes.

	Software de Administración de la Base de Datos	**Sistemas de Aplicación**

¿Mantiene el cliente uno o más diccionarios de datos?	
Describa las responsabilidades para la administración de la base de datos del cliente.	

Apoyo a la Red

Describa brevemente el uso de redes del cliente, incluyendo las ubicaciones conectadas a la red, los ciclos y actividades de negocios y que están soportados por los sistemas de aplicación en la red, y las interrelaciones dentro de la red. Considere adjuntar un diagrama general de la red, si hay alguno disponible.

En la tabla siguiente, relacione el software del sistema de administración de la red usado por el cliente:

	Software del Sistema de Administración de la Red

	¿Quién actualiza el acceso a la configuración de datos del Software del Sistema de Administración de la Red?

	¿Quién es el responsable de modificar la configuración de datos del Software del Sistema de Administración de la Red?