UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

SEMINARIO DE INVESTIGACION INFORMATICA
QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

PRESENTAN:

ASESOR DEL SEMINARIO:

MEXICO, D.F. 1996

AL MAESTRO JOSE ANTONIO ECHENIQUE GARCIA.

Por su apoyo, experiencia, tiempo y confianza brindados; para el logro de la realización de este trabajo.

VERONICA BALCAZAR MOLINA
ALEJANDRO ORTEGA ZARATE

A mis padres

Con amor, respeto y agradecimiento por brindarme su ejemplo, comprensión, apoyo y aliento para superarme en cada momento de mi vida.

Y a todos aquellos amigos que me aconsejaron y brindaron su apoyo incondicional

Veronica Balcazar Molina.

INDICE

PAG

OBJETIVO

Esta tesis tiene como objetivo diseñar una guía que sirva como fuente de referencia para ayudar a equipos de trabajo a:

Planificar y ejecutar un enfoque de auditoria que responda a los riesgos en el área o áreas de cómputo en una organización.

INTRODUCCION

El avance de la tecnología y el consecuente abatimiento de costos de los bienes informáticos (hardware y software) ha originado que cada vez sea mayor el número de organizaciones del sector publico y privado que utilicen estos bienes como una herramienta para el procesamiento de información debido a las ventajas que ofrece, principalmente velocidad, exactitud, oportunidad y manejo eficiente de grandes volúmenes de datos. Esto origina que la información producida sea un elemento de suma importancia para la toma de decisiones en las organizaciones y para el control adecuado de muchas de las operaciones.

Normalmente, los recursos económicos destinados a la actividad de Procesamiento Electrónico de Datos (PED) representan cantidades importantes, lo cual hace indispensable que el rendimiento obtenido sobre dicha inversión deba ser satisfactoria, o sea, que el aprovechamiento de la capacidad instalada (personal y equipo) sea el máximo posible; a diferencia de la mayoría de la operaciones que normalmente existen en una empresa el PED tiene algunas características especiales que no se presentan en las demás operaciones. Estas caracteristicas motivan que la Auditoria en Informática incluya aspectos especiales en la ejecución y enfoque de algunas de las actividades y funciones que se realizan.

Así mismo, es cada vez mas frecuente encontrarnos con una mezcla de diversas tecnologías en donde día a día se incorporan tecnologías de Telecomunicaciones y Base de Datos. Los mini y microcomputadores son utilizados como parte integral de redes de computación mas extensas y también como sistemas independientes.

Por ello los ambientes típicos están caracterizados por una mezcla de tecnologías en donde es necesario:

- Asegurar que la separación de obligaciones exista dentro de la Organización del Procesamiento Electrónico de Datos.
- Verificar la existencia de Controles y procedimientos adecuados, tanto en las instalaciones de la computadora como en las aplicaciones para evitar accesos no autorizados.
- Asegurar la utilización efectiva de los recursos de procesamiento de información.
- Revisar las políticas y procedimientos de las funciones de Desarrollo de sistemas para asegurar los estándares adecuados para controles y reportes de manejo.

El presente trabajo tiene como tema principal la Auditoría en Informática y su aplicación en las organizaciones del sector publico y privado.

En el capitulo I podemos contemplar lo que es Auditoría, desde sus orígenes, clasificaciones y técnicas utilizadas para su realización.

El capitulo II contiene desde el origen de la Auditoria en Informática, su evolución, así como: el objetivo, la clasificación, técnicas y metodología de desarrollo de esta auditoría.

El capitulo III trata del Estudio General que se realiza a las organizaciones antes de comenzar la auditoría, ya sea de informática o cualquier otro tipo, es decir efectuar un análisis que nos proporcione un conocimiento global de la empresa, que nos llevará a poder decidir que tipo de revisión se realizará.

Del capitulo IV al VIII se muestran los diferentes tipos de revisiones que se pueden realizar en una empresa, presentando cuestionarios y procedimientos que podrán ser utilizados para llevar a cabo la auditoria.

El capitulo IX presenta una visión general de los aspectos que se deben incluir en el informe final independientemente de la revisión realizada.

I. AUDITORIA

I.1. ANTECEDENTES.

Se dice que la auditoría comenzó desde el mismo momento en que existió el comercio, ya que en este momento se llevaron a cabo auditorías de algún tipo. Las primeras auditorías fueron revisiones meticulosas y detalladas de los registros establecidos para determinar si cada operación había sido asentada en la cuenta apropiada y por el importe correcto. El propósito principal de estas auditorías era detectar desfalcos y determinar si las personas en posición de confianza estaban actuando e informando de manera responsable. Las primeras auditorías estaban encaminadas a asegurar al propietario de un negocio que los empleados contratados habían mantenido correctamente las cuentas y que existían todos los activos y se encontraban registradas a las cantidades apropiadas. Mas adelante, al intentar obtener dinero prestado, el propietario podía utilizar el balance general para mostrar a un banquero que el negocio tenía los suficientes activos para garantizar el préstamo.

Después de la revolución industrial el alcance y la complejidad de los negocios se amplio notablemente. Al aumentar en tamaño las compañías emplearon mayor número de personas y sus sistemas contables se volvieron mucho mas desarrollados, con esto, resulto posible dividir las tareas dentro de la compañía. Ninguna persona tenía la responsabilidad de manejar la totalidad de una operación; las funciones de custodia de activos, y su registro fueron separadas y se establecieron otros controles internos efectivos para proteger los activos y prevenir y detectar los desfalcos. Los auditores internos también se convirtieron en una parte importante de los sistemas de control interno. Además se comprendió que la meta de descubrir errores se podía llevar a cabo con mayor efectividad mediante un sistema adecuado de control interno. El papel de auditor cambio de la búsqueda de desfalcos y de certificar la exactitud de un balance general a la revisión del sistema y comprobación de las evidencias a fin de poder emitir una opinión sobre la presentación correcta de todos los estados financieros.

La creciente separación de la propiedad de las corporaciones estimulo el desarrollo de la auditoría moderna. Las bolsas de valores a principio de siglo establecieron requisitos mínimos para la presentación de informes de compañías cuyas acciones estaban registradas en las mismas. La legislación federal sobre valores de 1933 y 1934 creo la Security and Exchange-Comission (SEC), amplio los requisitos de presentación de informes y exigió que los estados financieros fueran dictaminados por auditores independientes.

I.2. CONCEPTO

Auditoría, en un sentido amplio, equivale a examen (o revisión) efectuado por alguien independiente de la elaboración de los elementos objeto de examen.

Cualquier aspecto de la empresa es susceptible de auditoría y hay tantas formas de ella como áreas pueden ser objeto de revisión.

El examen efectuado le proporciona al auditor las evidencias para que pueda emitir un informe que resuma su opinión sobre los elementos revisados. Dicho informe constituye, en consecuencia, la conclusión del trabajo de auditoría.

La auditoría es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos por la organización.

Como la auditoría es un *proceso sistemático* de obtener evidencia, tienen que existir conjuntos de procedimientos lógicos y organizados que sigue el auditor para recopilar la información. Aunque los procedimientos apropiados varían de acuerdo con cada compañía, el auditor siempre tendrá que apegarse a los estándares generales establecidos por la profesión.

La definición señala que la evidencia se obtiene y evalúa de *manera objetiva*. Por consiguiente el auditor debe emprender el trabajo con una actitud de independencia mental neutral.

La *evidencia* examinada por el auditor consiste en una amplia variedad de información y datos que apoyen los informes elaborados. La definición no es restrictiva en cuanto a la naturaleza de la evidencia revisada, mas bien implica que el auditor tiene que usar su criterio profesional en la selección de la evidencia apropiada. El debe considerar cualquier elemento que le permita hacer una evaluación objetiva y expresar un dictamen de naturaleza profesional.

Los informes sobre actividades económicas y otros acontecimientos toman por lo general la forma de informes financieros, especialmente estados financieros, pero esta definición de auditoría es lo bastante general como para incluir informes que pueden tomar la forma de declaraciones de impuestos, convenios contractuales, informes de funcionamiento, estudios de factibilidad y muchos otros tipos de informes.

El papel del auditor es determinar el *grado de correspondencia* entre la evidencia de los que ocurrió en realidad y los informes que se han presentado de esos sucesos. Los usuarios del informe que por lo general no conocen directamente lo que aconteció en realidad,

quieren que el auditor les asegure que la información presentada es una declaración objetiva de los sucesos reales y sus resultados.

La medición y el informe de los acontecimientos económicos debe estar de acuerdo con *principios establecidos*, el auditor tiene que estar familiarizado con los principios aplicables para cada situación de informes, y debe tener la capacidad suficiente para determinar si dichos principios han sido aplicados de manera apropiada. Lo mas común es que el auditor utilizará como principios los *"Principios de Contabilidad Generalmente Aceptados"*, pero en algunas ocasiones los principios apropiados podrán ser las leyes, los reglamentos del impuesto sobre la renta, convenios contractuales, manuales de procedimientos, requisitos fijados por el gobierno, y otras disposiciones establecidas.

I.3 CLASIFICACION

Existen numerosos conceptos y clasificaciones desarrolladas por los contadores públicos en relación con la auditoría. Ocasionalmente surgen confusiones que se acentúan porque se carece de una terminología universalmente aceptada y de uso uniforme.

Las discrepancias en el empleo de términos elementales como reserva, provisión y fondo son indiscutibles; es frecuente encontrar reportes de prestigiadas firmas de contadores públicos que incluyen el manejo equivocado de dichos conceptos, o clasificaciones de los rubros de los estados financieros que se apartan de las normas de revelación suficiente promulgadas por los organismos colegiados.

Cuando se trata de clasificar y conceptuar la auditoria, los contadores públicos han aportado nuevos enfoques y puntos de vista en torno al ejercicio de esta actividad profesional. Sin embargo, si se atiende a los campos de actuación del contador público, la auditoría puede clasificarse de manera sencilla en los siguientes grupos:

I. Auditoria.

I.1. Auditorias específicas

I.1.1. Auditoría administrativa.
I.1.2. Auditoría operacional.

I.2. Auditorias de estados financieros.

I.3. Auditorias detalladas.

Otra clasificación importante se da atendiendo a las personas que la ejercen y son: auditoría interna y auditoría externa.

Auditoría Administrativa

Es el examen efectuado sobre las etapas que integran el proceso administrativo de una entidad económica, a fin de opinar sobre la calidad de su realización y sugerir acciones concretas para mejorarlo.

En consecuencia, el campo de aplicación de la auditoría administrativa lo constituyen las siguientes fases del proceso referido:

- Planeación
- Organización
- Integración
- Dirección
- Control

La auditoría administrativa puede abarcar al proceso administrativo en su conjunto, o bien, sólo algunas de sus etapas. De acuerdo con ello, una auditoría sobre la fase de planeación incluye, entre otros aspectos, el examen de la factibilidad de objetivos para una o varias áreas de la entidad, la evaluación de las medidas de previsión establecidas por la gerencia en relación con los objetivos a mediano o corto plazo y su congruencia respecto a ellos.

En la etapa de organización, la auditoría administrativa se dirige hacia las características de la estructura de la entidad, las áreas funcionales y los departamentos que la integran, la especificación de niveles jerárquicos y los canales de comunicación que existen entre ellos.

Esta misma clase de consideraciones se puede hacer respecto al examen de las etapas de integración, dirección y control; la auditoría en cada una de ellas comprende diferentes aspectos, pero con los mismos objetivos ya mencionados: Opinar sobre la calidad del proceso administrativo y, en caso necesario, emitir sugerencias factibles para mejorar su desarrollo.

Auditoría Operacional

La auditoría operacionales el examen del flujo de transacciones llevadas a cabo en una o varias áreas funcionales que constituyen la estructura de una entidad, con el propósito de incrementar la eficiencia y eficacia operativas, a través de proponer las recomendaciones que se consideren necesarias.

De acuerdo con lo anterior, la auditoría operacional se efectua en cualquiera de los ciclos de transacciones ya comentados y, por consiguiente, sobre uno o varios sistemas implementados para el control y el procesamiento de las operaciones.

La auditoría operacional involucra los siguientes tres elementos fundamentales que deben considerarse al realizarla:

1. El examen del flujo de las transacciones debe encausarse hacia los aspectos administrativos de los métodos y los procedimientos que integran un sistema. Una operación puede contemplarse bajo dos puntos de vista: El evento técnico propiamente dicho y su efecto monetario en las finanzas de la entidad; este ultimo es motivo de captura y procesamiento a través de los sistemas en vigor y constituye el punto de atención de la auditoria operacional.

   En eventos técnicos de gran complejidad reservados a otros profesionales, el auditor operacional tiene poco que aportar y debe reconocer sus limitaciones.

2. La auditoría debe tener un enfoque constructivo. Su finalidad esencial es incrementar la eficiencia y la eficacia en el desarrollo de las operaciones.

   En consecuencia, quien lleva a cabo el examen debe tener presente que sus responsabilidad principal es detectar todo aquello que pueda eliminarse, combinarse, transferirse, corregirse o modificarse en la estructura de un sistema.

3. El auditor o sus colaboradores no deben intervenir en le diseño detallado de los cambios que requiere un sistema o sus procedimientos; tampoco debe intervenir en la implantación de los controles que configuran la estructura de dichos procedimientos.

   No obstante, es necesario señalar que los niveles directivos de empresas en etapa de desarrollo muestran una notable tendencia a esperar de sus auditores internos algo mas que un informe con sugerencias para solucionar problemas localizados en el curso de un examen sobre controles en vigor. La participación del auditor en la solución efectiva de los problemas constituye un tema de reflexión que tal vez ocasionara polémicas en el futuro inmediato.

Por otra parte, la auditoria operacional implica un desarrollo integral y secuencial del examen sobre los procedimientos que configuran un sistema; el desarrollo de la revisión debe comenzar en el punto de origen del sistema auditado y debe concluir donde este termina, generalmente, uno o varios asientos contables.

En un sistema de compras, la auditoria operacional deberia iniciarse en el departamento que emite las requisiciones o los documentos fuente para la realización de las adquisiciones de mercancias o servicios y concluir con el examen de los cargos a las cuentas de inventarios y el crédito a los pasivos con proveedores.

De acuerdo con lo anterior, la auditoría financiera es solo una parte del examen de los flujos de operación, pues carecería de fundamento profesional la revisión de movimientos y saldos

Auditoría de Estados Financieros

Es el examen de los estados financieros preparados por la administración de una entidad económica, con objeto de opinar respecto a si la información que incluye está preparada de acuerdo con los principios de contabilidad aplicables a las características de sus transacciones:

La auditoría de estados financieros sólo puede llevarla a cabo un contador público y la información sujeta a examen está integrada por los siguientes documentos:

- Balance General o Estado de Posición Financiera
- Estado de Resultados
- Estado de Variaciones en las Cuentas de Capital
- Estado de Cambios en la Posición Financiera o, en épocas de intensa inflación, Estado de Flujo de Efectivo
- Notas a los Estados Financieros

Tanto el contador público que tomará la responsabilidad de opinar sobre los estados financieros como sus colaboradores o ayudantes, deben tener un criterio independiente que les permita afectar su trabajo en forma imparcial. Los pronunciamientos de ética profesional establecen claramente los hechos y circunstancias que un equipo de auditores debe satisfacer para salvaguardar su independencia de criterio.

La auditoría de estados financieros se lleva a cabo, por lo general, en tres etapas o visitas a la entidad:

- Etapa Preliminar
- Etapa Intermedia
- Etapa Final o Cierre de la Auditoría

La *etapa preliminar* se inicia en el cuarto o quinto mes del ejercicio social. Sus objetivos son el estudio y la evaluación del control interno a través del examen de los flujos de transacciones que producen los estados financieros y, en su caso, la emisión de recomendaciones para mejorar los procedimientos y sistemas en vigor.

La *etapa intermedia* comienza en el octavo o noveno mes del ejercicio auditado. Con base en la evaluación de los controles hecha en la primera etapa, sus objetivos son juzgar la razonabilidad de las cifras de una balanza de comprobación intermedia, detectar situaciones especiales susceptibles de mejoramiento en los rubros y en los registros contables, a fin de evitar numerosos ajustes al cierre anual de operaciones y estableeer bases para que la etapa final de la auditoría se lleva a cabo en forma rápida y eficaz.

La *etapa final* se inicia en el segundo o tercer mes del ejercicio posterior al auditado; sus objetivos son actualizar el juicio relativo a la razonabilidad de las cifras contables mediante el examen del segmento comprendido entre la etapa intermedia y el cierre del ejercicio.

sugerir los ajustes y reclasificaciones necesarios y emitir el dictamen sobre estados financieros.

Auditorías Detalladas

Las auditoría administrativa y la auditoria de estados financieros se efectúan sobre muestras de las actividades, transacciones y cifras sujetas a examen; sus objetivos son compatibles con las pruebas selectivas. Por otra parte, las revisiones exhaustivas serían imprácticas para ambas.

Sin embargo, existen circunstancias especiales que hacen necesarios los exámenes detallados sobre las operaciones o la información financiera de una entidad económica.

De acuerdo a lo anterior, las auditorías detalladas se llevan a cabo en casos como los siguientes:

- Compra venta de una empresa
- Fusión de sociedades mercantiles
- Verificación del cumplimiento con obligaciones fiscales o laborales

En la operación de compra venta de una compañía: El precio fijado a las acciones es por lo general, un reflejo de la rentabilidad presente y futura de las inversiones y de la solidez en la estructura de las finanzas de la empresa. Es evidente que los compradores estarán interesados en la información financiera, cuyos componentes harán posible conocer y evaluar los datos referidos y tomar una decisión adecuada

Surge, en consecuencia, la necesidad de averiguar si las cifras de los estados financieros muestran correctamente los activos, los activos y el capital contable dela entidad.

A los compradores en prospecto les parecía insuficiente un informe de auditoría basado en pruebas selectivas y en términos de que los estados financieros son razonables correctos; ellos requieren precisión en los juicios referentes a la calidad de dichos estados, pues cualquier concepto mal valuado en ellos tendría un impacto inevitable sobre su patrimonio.

En la clasificación de la auditoría que se ha planteado se pueden incluir todas las nuevas modalidades desarrolladas por la profesión contable lo cierto es que la auditoría gubernamental y cualquiera otra de reciente creación , se basa en la metodología que pertenece a la auditoría administrativa, a la auditoría de estados financieros o a la auditoría operacional.

Auditoría Interna

La auditoría interna es una función independiente de evaluación establecida dentro de una organización, para examinar y evaluar sus actividades como un servicio en la organización. El objetivo de la auditoría interna consiste en apoyar a los miembros de la organización en el desempeño de sus responsabilidades. Para ello la auditoría interna les proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente con las actividades revisadas.

Los miembros de la organización a quien los auditores internos apoyan, incluye a la Gerencia y al Consejo de Administración. Los auditores internos, son responsables ante ambos, proporcionándoles información acerca de la adecuación y efectividad del sistema de control interno de la organización y la calidad de la gestión. La información que se proporciona a cada uno puede diferir en formato y detalle, dependiendo de los requisitos y solicitudes de la Gerencia y el Consejo.

El departamento de auditoría interna es una parte integrante de la organización y funciona de acuerdo a las políticas establecidas por la Gerencia y el Consejo de Administración. El establecimiento del propósito, autoridad, responsabilidad (*Manual de Organización*) del departamento de auditoría interna aprobado por la Gerencia y aceptado por el Consejo de Administración deberá ser congruente con la Normas para la Practica Profesional de la Auditoría Interna.

Las normas comprenden:

- La independencia del departamento de auditoría interna respecto de las actividades auditadas y la objetividad de los auditores internos.
- El conocimiento técnico, la capacidad y el cuidado profesional de los auditores internos con los que deben ejercer su función.
- El alcance del trabajo de auditoría interna.
- El desarrollo de las responsabilidades asignadas a los auditores internos.
- La administración del departamento de auditoría interna.

El manual de organización deberá establecer claramente los propósitos del departamento de auditoría interna, especificar que el alcance del trabajo no debe tener restricciones y señalar que los auditores internos no tendrán autoridad y/o responsabilidad respecto de las actividades que auditan.

En todo el mundo la auditoría interna se realiza en diferentes ambientes y dentro de organizaciones que varían en propósito, tamaño y estructura. Además las leyes y costumbres de los países son diferentes. Estas diferencias pueden afectar la practica de la auditoría en cada ambiente. En consecuencia la adopción de estas normas estará regulada por el ambiente en el cual los departamentos de auditoría interna realizan las responsabilidades asignadas. Sin embargo, es esencial el cumplimiento de los conceptos

enunciados por estas normas, ante el cumplimiento de cualquier otra responsabilidad de los auditores internos.

Auditoría Externa

La auditoría externa, conocida también como auditoría independiente. La efectúan profesionistas que no dependen de la empresa económicamente ni bajo cualquier otro concepto, y a los que se reconoce un juicio imparcial merecedor de la confianza de terceros

La mayor parte de las organizaciones presentan en algún momento informes financieros a usuarios externos, tales como bancos, otros acreedores, propietarios y probables inversionistas. Estos usuarios externos de la información necesitan tener la seguridad de que los informes financieros se preparan sin prejuicios y cumpliendo con los principios correspondientes.

La información proporcionada por el auditor interno es confiable, pues aunque los auditores internos son independientes de los demás empleados dentro de la organización cuyo trabajo revisan, también son parte de la organización.

I.4. OBJETIVOS

La auditoria tiene como objetivo general el emitir una opinión critica y constructiva con respecto a los eventos individuales o colectivos que ocurren en la organización, así como promover la implantación de acciones correctivas que se consideren necesarias para mejorar su ejecución.

A continuación se presenta una breve relación de enunciados que indistintamente se han expresado como el objetivo prioritário de la función de la auditoria, donde algunos pueden considerarse como secundarios o consecuentes de otros:

- Evaluar la razonabilidad de las cifras contable/financieras.
- Salvaguardar los activos.
- Apoyar los interesas de la dirección.
- Constituir un factor de cambio.
- Promover la eficiencia y productividad.
- Fortalecer la penetración de bienes y servicios.
- Reforzar el control interno.
- Proporcionar servicio a la alta gerencia.
- Coadyuvar en la toma de decisiones.
- Promover el desarrollo.
- Evitar fugas financieras.
- Garantizar que toda información operativa y financiera sea razonablemente correcta.
- Corregir deficiencias.
- Prevenir posibles problemas.
- Cumplir la normatividad de la profesión.
- Vigilar la autenticidad de los estados financieros.
- Evaluar el cumplimiento de metas y objetivos.

La misma clase de acciones puede hacerse en relación con el cualquiera de las actividades de la empresa pero siempre se podrán identificar los siguientes aspectos:

- Un plan o un esquema teórico que debe cumplirse.
- Una o varias partes ejecutoras.
- La ejecución prioritariamente dicha de los trabajos.
- La posibilidad de que ocurran desviaciones respecto al plan o al esquema teórico.

I.5. TECNICAS

La Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos, en su boletín F-01, ha propuesto la siguiente clasificación de las técnicas de auditoria

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaraciones o Certificaciones
- Certificación
- Observación, y Cálculo.

Estudio General. Es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones, a través de sus elementos mas significativos para concluir si se ha de profundizar en su estudio y la forma en que ha de hacerse.

Análisis. Es el estudio de los componentes de un todo para concluir con base en aquellos respecto de este. Estas técnica se aplica concretamente al estudio de las cuentas o rubros genéricos de los estados financieros.

Inspección. Es la verificación física de las cosas materiales en que se tradujeron la operaciones. Se aplica al estudio de las cuentas cuyos saldos tienen una representación material.

Confirmación. Es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operación, en la que participó y por la cual esta en condiciones de informar validamente sobre ella.

Investigación. Es la recopilación de información mediante platicas con los funcionarios y empleados de la empresa. Generalmente se aplica al estudio del control interno en su fase inicial y de las operaciones que no aparecen muy claras en los registros.

Declaraciones y certificaciones. Es la formalización de técnica anterior, cuando, por su importancia, resulta conveniente que las afirmaciones recibidas deban quedar escritas y en algunos casos certificadas por una autoridad.

Observación. Es una manera de inspección, menos formal, y se aplica generalmente a operaciones para verificar como se realiza en la practica.

Cálculo. Es la verificación de la corrección aritmética de aquellas cuentas u operaciones que se determinan fundamentalmente por cálculos sobre bases precisas.

II. AUDITORIA EN INFORMATICA

II.1. ORIGEN.

La historia puede a veces dar a sus estudiantes la habilidad de hacer predicciones sobre el futuro que no podrían ser hechas si no se tuviese el conocimiento del pasado. Esta capacidad de predicción nos permite anticiparnos a los eventos en lugar de solo reaccionar ante ellos. También esta capacidad nos puede dar la capacidad de evitar algunos errores del pasado; "Aquel que no tiene conocimiento del pasado esta condenado a repetirlos".

La planeación estructurada, es parte indispensable del trabajo de las gerencias modernas de procesamiento electrónico de datos, lo cual es imposible sin tener el entendimiento del contexto histórico, es importante porque nos provee de ideas en dirección de afirmar que las actividades de procesamiento electrónico de datos están principalmente basadas en la experiencia general de las industrias.

Los 50's.

Las primeras computadoras utilizadas en el sector privado fueron adquiridas, ya que , la tecnología era nueva y costosa, y este suceso fue problemático. El impacto que las computadoras tuvieron en las personas y en las organizaciones fue inesperado. Pero ahora los estándares de los sistemas de computadoras de los 50's y de principios de los 60's son primitivos; la tecnología de bulbos; unidades de registro; las lentas unidades de cintas magnéticas; los rudimentarios sistemas operativos de arranque o carga; y los tediosos lenguajes de maquina para programar que ahora consideramos pertenecen a la edad de piedra.

Las primeras aplicaciones en computadora fueron científicas y militares. Muy pronto la oficina de censos de los Estados Unidos y otras oficinas de gobierno empezaron a utilizar computadoras para procesar grandes cantidades de papeles de trabajo. Grandes corporaciones del sector privado rápidamente siguieron esta tendencia ajustándose a ella.

Por lo repetitivas pero bien definidas las operaciones de contabilidad fueron los primeros candidatos a la automatización. Pero el primer impacto organizacional de la computadora fue dentro del grupo de trabajo. Ya que se extendió la idea de que con el tiempo la computadora causaría un serio problema de desempleo entre los oficinistas, tenedores de libros (contadores) y otros trabajadores de oficina. El desempleo en realidad no ocurrió. Porque la gente desplazada fue absorbida dentro delas funciones de procesamientos de datos, por los operaciones de captura y los controladores de oficinas; Gracias a el gran boom economico de los 50's otras personas encontraron trabajo en compañías que aun no estaban automatizadas.

A pesar de los altos precios del primer hardware, algunos ahorros en costos se dieron compensados por las reducciones de los oficinistas. La evidencia sugiere además, que las preocupaciones gerenciales con justificación en el procesamiento electrónico de datos en base de la eliminación del trabajo empezaron a desaparecer a finales de esta época.

Los 60´s

La década de los 60's fue un periodo de gran crecimiento para la industria de las computadoras, se presento el auge de las aplicaciones batch . Grandes volúmenes de datos fueron procesados, pero el procesamiento se realizaba en las rutinas mas utilizadas en ese entonces .Cada compañía obtenía una computadora y cada gerente de proceso de datos estaba obligado a producir facturas , cheques de nomina , y reportes de todo lo que se vendió el día anterior .

Las aplicaciones continuaron siendo muy concentradas en funciones que cuando se realizaban manualmente estaban muy bien definidas. Como aplicaciones contables, nominas, y sistemas de facturación, el desarrollo del control de inventarios, personal y sistemas de manufactura también ocupó un lugar importante. Las firmas empezaron a explorar la computarización de procesos que aun no estaban bien definidos como las primeras aplicaciones financieras. El teleprocesamiento fue introducido a finales de los 60's sin tener mucho uso dentro de la industria.

Además algunos exóticos sistemas de reservaciones en aerolíneas, procesos de tarjeta de crédito y sistemas de seguimiento de seguridad fueron implantados. Fuera de estos sistemas "La oportunidad de nuevos negocios" en el uso general de tarjetas de crédito, eficiente viajes aéreos , y otros aspectos de la vida moderna no eran posibles.

Como se esperaba la mayor parte de los cambios fueron absorbidos por oficinistas y otros empleados de oficina por que las aplicaciones del proceso electrónico de datos se volvieron mas ambiciosas, la gente fuera de las oficinas cada vez estaba mas involucrada: Los almacenistas llevaban en computadora la información de salida y entrada al inventario, los encargados de tiendas usaban facturas para material explosivo y cédulas de producción generadas por computadora, los gerentes de venta examinaban el impacto de sus campañas de mercado, y los gerentes de producción evaluaban los costos de producción de varias líneas de productos.

Los sesentas fueron años de grandes cambios tecnológicos, los bulbos fueron remplazados por los transistores. El almacenamiento de archivos en tarjetas fue reemplazado por cintas magnéticas y discos. La programación en lenguaje maquina fue eliminada por los compiladores y ensambladores virtuales.

El resultado de la tecnología fue un gran número de nuevas funciones en el trabajo. El mas notable de estos fue el programador de sistemas, la carga individual que generaba la compleja operación de sistemas lo hacían propiamente un trabajo. Entonces toma lugar el

crecimiento del grado de especialización en el trabajo. El "hombre renacentista", quien podía "hacerlo todo", fue cubierto por la tecnología y reemplazado por el especialista. Pero algunas cosas permanecieron igual. A pesar de la proliferación de las aplicaciones no financieras, los gerentes de proceso de datos continuaron reportándole al director.

Organizacionalmente en esta década se comenzó a tener un alto grado de centralización del control sobre las funciones de el procesamiento electrónico de datos. Por que, la demanda de servicios computacionales causo una descentralización sustancial.

Los 70's.

El periodo de finales de los 60's. y principios de los 70's estuvo caracterizada por la introducción y el uso del teleprocesamiento (TP). el continuo descenso en los costos del hardware aunado al aumento de la capacidad de teleprocesamiento resulto en la proliferación de aplicaciones en linea y en tiempo real.

Complejos Sistemas de Información Gerencial (MIS),cuya función principal fue la de proveer información para la toma de decisiones fueron intentos de muchas grandes organizaciones. Estos sistemas fueron desarrollados frecuentemente para proveer datos y realizar funciones que no eran posibles antes de la aparición de la computadora.

La creencia algo optimista, fue que la puntualidad y precisión de la información producida por la computadora pueden ser la gran diferencia en la efectividad de la gerencia. Desafortunadamente se probo que esto no era verdadero. Muchos gerentes rechazaron firmemente el uso de información generada por computadora, reafirmando su creencia cuando esto ocurrió. Esto tuvo como resultado la cancelación de muchos proyectos MIS .

A pesar de los decepcionantes resultados obtenidos de muchos sistemas MIS, una mayor cantidad de información para la toma de decisiones estaba siendo disponible a los gerentes como producto de sistemas de procesos tradicionales de transacciones. Los resultados prácticos no fueron la idea central de las líneas gerenciales, como algunas veces paso con las funciones de oficina en los principios de la década, mas bien, el trabajo gerencial cambio

Los cambios tecnológicos que tuvieron gran impacto durante los 70's fueron los siguientes:

- Gran escala y muy grande escala de integración de sistemas (LSI Y VLSI) y otros componentes de miniaturizaron, la cual incremento la velocidad y confiabilidad del hardware.
- Almacenamiento virtual, el cual reduce la importancia del tamaño del programa en relación a las consideraciones de legibilidad y de mantenibilidad.
- Minicomputadoras, las cuales precipitan la tendencias hacia el procesamiento distribuido.
- Terminales interactivas inteligentes, las cuales cambian el aspecto del desarrollo, de la programación y del acceso y trabajo de los usuarios a los archivos centrales.

- Sistemas manejadores de base de datos (DBMS),los cuales contribuyeron a incrementar la integración de archivos y precipitaron planes ambiciosos para la administración de la constitución de datos.
- Gran capacidad periférica y de almacenamiento en memoria principal, lo cual incremento el rango de aplicaciones que pueden ser desarrolladas por grandes cantidades de datos en línea.
- Proliferación de la disponibilidad comercial de paquetes y aplicaciones, los cuales reducen el tiempo de desarrollo de muchos sistemas.

Organizacionalmente, los 70's estuvieron caracterizados por un severo control gerencial de las funciones de procesamiento electrónico de datos y la revaluación de las capacidades de las computadoras y sus limitaciones. Esto frecuentemente resulto en una reducción que causo la cancelación de proyectos periféricos y en la reducción de planes excesivamente ambiciosos. Los gerentes de procesamiento electrónico de datos, incrementando la precaución y el escepticismo de los altos mandos, empezando a utilizar una severa dirección. Implantando para los proyectos gerenciales controles, estándares, y herramientas eficientes y en algunos casos se introdujeron mejoras. Se puso mas atención en los usuarios finales con el objeto de aumentar el soporte para así desalentarlos a que adquirieran sus propios recursos de cómputo.

A mediados de los 70's la grandeza típica, la dispersión geográfica hicieron que la organización tuviera las siguientes características.

- Una o mas computadoras de gran escala que constituya una central de procesos con todo el volumen de las aplicaciones.
- Un grupo central de programadores, analistas, especialistas de software, y similares.
- Terminales en ubicaciones distantes usadas para facilitar el desplazamiento y acceso a la central de datos.
- Pocos iniciadores de minicomputadoras procesando algunas aplicaciones independientemente de la computadora central y otras en conjunto con el mainframe.

Los 80's

Quizás las principales caracteristicas del ambiente de finales de los 70's y principios de los 80's es la proliferación de mini y micro computadoras que aumentaron el poder de cómputo y el control de disponibilidad de los usuarios comunes, y el dramático progreso que tuvo la tecnologia.

Los patrones de los recursos de distribución y control de procesamiento electrónico de datos fueron alterados drásticamente en los pasados diez años. Lenguajes de alto nivel y sistemas de bajo costo para minicomputadores que facilitan el uso y desarrollo de pequeñas demandas que existen en el ambiente fisico, por primera vez, proporcionan a los usuarios finales en gran medida el control de sus propios sistemas. Desafortunadamente, esto frecuentemente tuvo como resultado la redundancia de datos e inconsistencia entre

usuarios, incompatibilidad de equipo carencia de estandarización, y la innecesaria duplicación de hardware, software, y personal. Estos problemas fueron dirigidos directamente a incrementar la flexibilidad de los sistemas de proceso distribuido la necesidad de bases de datos distribuidas es un ejemplo de flexibilidad.

Otro ejemplo de control sobre sistemas distribuidos es la habilidad de varios componentes en una red de "hablar" con algún otro y con la computadora central. Esto reduce la incompatibilidad de hardware y provee a la central de gran control sobre la red., además, la importancia de controlar la incorporación de datos e implantar estándares de proceso de datos que sean reconocidos. la computadora esta presente en cada nivel de la organización. El flujo de información es cada vez mas bidireccional, esto es, que los datos regresan a el lugar de donde fueron provistos en forma útil. Este cambio habilita que las decisiones logísticas sean mas centralizadas, mientras que descentraliza las decisiones tácticas a "donde esta la acción". Esto da un continuo énfasis en aplicaciones no financieras. Los sistemas están siendo desarrollados por menos funciones estructuradas y por aplicaciones que no tienen que justificar previamente sus costos.

Los errores de los MIS de los 70's son rectificados por la implementación de los sistemas MIS en componentes mas modestos que requieren pequeños ciclos de desarrollo. los aciertos de estos sistemas vinieron a ser mas reales.

Organizacionalmente la función de procesamiento electrónico de datos ahora raramente reporta al director en grandes organizaciones. Pueden reportar al presidente al vicepresidente o a otras áreas como administración, finanzas y servicios de información .

II.2. EVOLUCION.

El Licenciado en Informática puede desempeñar muchas funciones relacionadas con el procesamiento de información tales como: diseñar y desarrollar sistemas, asesorar en el diseño de sistemas, proporcionar servicios de procesamiento de datos, así como realizar, servicios de auditoría que garantizan la optimización de recursos económicos y humanos en el procesamiento electrónico de datos (PED).

La computadora es uno de los descubrimientos tecnológicos mas importantes del siglo XX. Sus usos y posibilidad se han incrementado cada día mas; provocando un fuerte cambio en la forma de realizar operaciones en una organización.

El costo decreciente del equipo de cómputo; además del progreso, de las instalaciones de centros de cómputo, claramente ocasiona el uso de las computadoras, lo cual ha originado cambios importantes en los sistemas de información de los negocios; el desarrollo de sistemas de información para la toma de decisiones en una organización.

La evolución que ha tenido la auditoria en el procesamiento electrónico de datos depende en gran medida del grado de automatización de operaciones de una organización y de la complejidad de los sistemas de información.

Es lógico suponer que las Normas de Auditoria que han sido establecidas son independientes del personal o las maquinas, utilizadas para procesar y mantener los registros contables y financieros. Por ello las Normas de Auditoría deben estar apoyadas en una base amplia a efectos de poderlas aplicar a una variedad de situaciones de auditoria. Sin embargo, se relacionan específicamente con cada examen realizado con la organización a que se refiere a un nivel aceptable de calidad que debe ser conservado por el auditor, al seleccionar aplicar los procedimientos de auditoría apropiados.

En la actualidad, los procedimientos de auditoria se han visto afectados por la presencia de la computadora especialmente cuando el fin es la revisión del procesamiento electrónico de datos pero esto no disminuye la necesidad de evaluar el Control Interno. La evaluación del Control Interno debe ser mas eficiente para cerciorarse que está funcionando adecuadamente.

Además del sistema de procesamiento de datos, de su control el auditor se ha visto en la necesidad de evaluar lo razonable de los registros producidos por un sistema, relativos a la existencia y valuación adecuada del activo, pasivo, capital de las operaciones realizadas en un periodo determinado de tiempo.

Con el objeto de proporcionar elementos de orientación conductal y metodológica para el mejor desempeño en la revisión de distintas especificaciones, tanto de la administración como del control en el procesamiento electrónico de datos. Diversas entidades y profesionales dedicados a la Auditoría en Informática han emitido algunas de las principales guias para definir capacidades conceptuales y practicas que determinan el curso preferente de las acciones previsibles y de las improvisaciones correspondientes cuando se realiza una Auditoria en Informática en la organización.

El siguiente cuadro menciona de acontecimientos de gran relevancia en la evolución de la auditoria en informática desde la década de los 50's hasta los 80's, lo cual no da una visión general de la situación de la misma en nuestra década, así como de los grandes avances que ya hemos hablado.

Evolución de la Auditoria en Informática

1956 Frank, S. Howell. Usó el computador en la reconciliación de las cuentas de inventario.

1961 Felix Kaufman escribió el libro " El computador electrónico y la Auditoría ".

1963 Carol Wiss dio un curso de una semana sobre Auditoría en el Procesamiento Electrónico de Datos.

1968 Gordon Davis escribió el libro " Auditoría y Procesamiento Electrónico de Datos ".

1968 Haskins y Sells desarrollaron un software llamado " Auditape ".

1970 El Instituto Canadiense de Contadores publica las "Guias del Control del Computador".

1971 El Internal Revenue Service (IRS) emite la regla 71-20 que oficializa las regulaciones de procesamiento de datos.

1972 Proliferan los grupos de auditoria de procesamiento de datos.

1973 EDTACS inicia sus publicaciones.

1974 El AICPA emite el " Statements on Audit Standars ".

1974 IBM crea un fondo de $500,000 Dls.

1974 Se crea el Acta sobre Privacia (Privacy Act USA) adaptada por los paises miembros de la organización para el desarrollo y cooperación económica (OECD).

1977 Acta sobre practicas corruptas en el extranjero (Forain Corrupt Practive Act USA).

1977 Se crea el estándar de encriptamiento de datos (DES) por la oficina nacional de estándares de los Estados Unidos de Norteamérica.

1978 El Us General Accounting Office publica "Audit Guide for Assessing Reliability of Computer Output".

1978 Jerry Fitzgerald y asociados publica "Control Interno para Sistemas computarizados".

1979 El instituto de Auditores Externos publica "How to Acquire and Use Generalized Audit Software".

1982 El Instituto de auditores internos publica "Systems Auditability and control".

1982 La Universidad de Queensland Australia/ Ron Weber publica "Electronic Data Process Auditing, Conceptual Foundations and Practice".

1983 La Fundación de Auditores del Proceso Electrónico de Datos, Inc. publica "Control Objectives".

1983 La Fundación de Auditores del Proceso Electrónico de Datos, Inc. publica "Information Systems Audit Process".

1991 El Instituto de auditores internos publica "Systems Auditability and control".

1993 La Fundación de Auditores del Proceso Electrónico de Datos, Inc. publica "Control Objectives".

II.3. OBJETIVO.

En algunas organizaciones la Auditoria en Informática se orienta en forma inicial a la detección de productos defectuosos y a su corrección; posteriormente a la identificación de algunas de las causas de dichos defectos " después a la validación de calidad de los procesos y actualmente se trata de lograr el cumplimiento de los objetivos de el procesamiento electrónico de datos en una empresa. En este sentido resulta determinante la identificación especifica de los objetivos y de los enfoques de intervención que a continuación se enumeran:

1. Normas o estándares del área de auditoria.

En el área de auditoría deben desarrollarse las normas de sistemas que determinen las actividades de análisis, diseño, programación, operación; etc. La auditoria debe asegurarse de su desarrollo y cumplimiento.

2. Contratos de procesamiento de datos.

La auditoría debe llevar un control permanente de los contratos con los fabricantes de equipos, productores de software, empresas de mantenimiento de hardware, instituciones de servicio externo y todas aquellas entidades que tengan alguna relación con el área de informática.

3. Seguros

Se debe verificar que los equipos (hardware). programas y paquetes (software),instalaciones y demás activos estén debidamente cubiertos con contratos de seguros; de la misma manera se deberá controlar la actualización periódica de los mismos.

4. Participación en el ciclo de vida del desarrollo de las diferentes aplicaciones.

El auditor participa activamente en el ciclo del desarrollo de sistemas durante la Auditoria en Informática, asegurando el análisis de la información donde esta se evaluara detalladamente y comparando con los objetivos planeados y los resultados obtenidos de las misma.

5. Auditorias posteriores a la implantación.

Una vez que la aplicación se procese periódicamente se realizaran las evaluaciones del comportamiento de la misma.

6. Mantenimiento del software.

Es necesario que la auditoria verifique estrictamente que las modificaciones en los programas se realicen con la autorización del caso y el cumplimiento de las normas establecidas.

7. Documentación del área de informática.

El auditor buscara que la información deberá estar por escrito o contemplada en los diferentes manuales.

8. Seguridad física.

Verifica que el área disponga de la instalación adecuada en cuanto a pisos falsos, estabilizadores, equipo contra incendio, seguridad contra acceso el físico de personas no autorizadas, paredes y demás aspectos relacionados con la seguridad física.

9. Backup de software y hardware.

El auditor evaluara periódicamente el cumplimiento de las normas o estándares de copias de archivos, software y documentación. Estas reglas detallan la necesidad de disponer de copias de estos elementos en un lugar externo a las oficinas de la instalación, de los equipos y un plan de varias copias que permitan el reproceso por fallas en la instalación física o de la información. El auditor se asegurará de que la organización auditada tenga establecidos convenios con instalaciones similares con el fin de tener un respaldo en caso de la suspensión temporal o la imposibilidad total de realizar el proceso en el sitio habitual.

10. Programa de trabajo.

El auditor evaluara periódicamente el cumplimiento de los planes de trabajo, en cuanto a días y horas de entrega de documentación, transcripción, procesos de devolución de resultados con cada uno de los usuarios.

11. Inventario de equipos y software.

Realizara chequeos de la ubicación física de cada uno de los dispositivos del equipo, su estado y mantenimiento adecuado, de la misma forma se hace el inventario de software disponible contratado o desarrollado internamente.

12. Recuperación de desastres.

Es necesario verificar que el procesamiento de datos desarrolle y mantenga un plan de desastre por suspensión temporal o definitiva de los procesos de información. Este plan debe incluir reposición o reemplazo de software, hardware y personal.

13. Entrada de datos.

Se verificara el cumplimiento de las reglas establecidas en cuanto al acceso de pantallas, documentos, personal autorizado, capacitación en operación de equipos, corrección de errores, ordenes de procesos de datos.

14. Ajustes a inconsistencias de información.

Se debe asegurar que mediante el personal autorizado y a través de los procedimientos adecuados se realicen las correcciones en los archivos o documentos que alimentan la aplicación de la auditoría.

15. Distribución de informes.

Asegurarse de que la tendencia de los informes producidos sean los necesarios, exactos, confiables y se entreguen a las personas indicadas.

16. Comunicaciones.

Se deben de garantizar la recepción de los mensajes y datos de acuerdo con las normas establecidas, en los horarios convenidos, entre las personas autorizadas. Se verificara que los archivos y los datos se hayan recibido en su totalidad.

17. Software del sistema.

Se verificara que el departamento de informática y fabricante de software (compiladores, rutinas de utilidad, manejadores de base de datos, etc.) mantengan en estado optimo este soporte y que su actualización sea la adecuada de acuerdo con los contratos y acuerdos establecidos.

18. Control de librería fuente y en ejecución.

Se verificara la disposición de las librerías, su correcta modificación y el acceso autorizado a las mismas.

19. Auditoría a las oficinas de servicio.

Se trata de controlar los servicios donde se realizan algunos procesos de la empresa. Estos deben estar de acuerdo a los contratos establecidos, con los controles adecuados, a los precios convenidos y con la oportunidad del caso.

20. Capacitación del personal de procesamiento de datos en la auditoria.

En este aspecto se procura incluir las diferentes aplicaciones en el ambiente de controles y de seguridad deseada, facilitando así la comunicación y logrando un mejor resultado final.

II.4. CLASIFICACION.

En la actualidad la Auditoría en Informática varía de acuerdo al nivel de automatización de la organización o del área o áreas de cómputo con que cuenta la misma. Sin embargo, diversos enfoques para la conceptualización y solución de intervenciones en este ámbito por lo que la auditoria de procesamiento electrónico de datos verifica los controles en tres áreas de la organización:

- **Las aplicaciones** incluye todas las funciones de información del negocio, en cuyo procesamiento interviene una computadora. Los sistemas de información que abarcan uno o mas departamentos de la organización así como la operación de la computadora y el desarrollo de sistemas.

- **El desarrollo de sistemas** cubre las actividades de los analistas de sistemas y programadores, quienes desarrollan y modifican los archivos de los sistemas, los programas y otros procedimientos.

- **La instalación de procesamiento de información** abarca todas las actividades relativas al equipo de computación y los archivos de información. Esto comprende la operación de la computadora, la biblioteca de los archivos de la computadora, el equipo de captura de datos y la distribución de la información.

De esa forma es como a través de este trabajo se presenta una propuesta que abarca las tres áreas anteriormente mencionadas pero en forma mas detallada para la intervención del auditor frente a los recursos informáticos y ocasionalmente de telecomunicaciones como sigue:

a) Revisión de administración de áreas de cómputo, es decir, revisar la aplicación del proceso administrativo en áreas de cómputo considerando las siguientes etapas:

   - Previsión
   - Planeación
   - Organización
   - Integración o Coordinación
   - Dirección
   - Control

b) Revisión del ciclo de vida de sistemas. Que consiste en verificar el cumplimiento de cada etapa del desarrollo de sistemas y la documentación existente de cada una de ellas.

   - Planeación
   - Análisis
   - Diseño
   - Codificación
   - Implantación

- Mantenimiento

c) Revisión de controles en redes. Consiste en revisar controles en redes considerando:

- Seguridad lógica
- Seguridad física
- Adquisiciones
- Plan de contingencias

d) Revisión de controles en equipos personales. consiste en la verificación de controles tales como:

- Seguridad lógica
- Seguridad física
- Protección contra virus

f) Revisión de telecomunicaciones. Que consiste en la verificación de existencia de:

- Administración de telecomunicaciones
- Seguridad física de telecomunicaciones
- Seguridad lógica de telecomunicaciones

II.5. TECNICAS.

La comprensión de las técnicas actuales de auditoría

Los auditores ya no pueden emplear las técnicas de auditoría convencionales las cuales eran adecuadas en un ambiente manual para evaluar los controles de cómputo de una organización. Para funcionar de forma efectiva a tratar los rápidos cambios de tecnología de la actualidad los auditores requieren un mayor conocimiento de la tecnología computacional así como una comprensión detallada de los riesgos reales debidos al uso de la computadora. Para mejorar la eficiencia de la auditoría los auditores deben desarrolla técnicas de auditoría que sean apropiadas para su uso con sistemas computarizados avanzados, además se deben involucrar en la creación de sistemas avanzados en las primeras etapas de desarrollo e implantación y deben hacer un mayor uso de los instrumentos automatizados de auditoría que son adecuados para su uso en el ambiente automatizado de su organización.

Técnicas de auditoría sin usar la computadora

El auditor debe entender completamente los procedimientos de auditoría que no requieren el uso de la computadora y deben saber como obtener los registros necesarios para poner en practica estos procedimientos.

Técnicas de auditoría utilizando la computadora

El auditor debe estar en posibilidad de conocer las situaciones en las cuales la computadora puede ser utilizado efectivamente para conducir la auditoría. También debe estar en posibilidad de planear y vigilar el desarrollo y el uso de técnicas tales como datos de prueba, procesamiento controlado y programas de auditoría con computadora.

A continuación se señalan los métodos para obtener evidencia de auditoría para probar los controles internos en los sistemas en la computadora "Pruebas de Computadora" Así como para verificar el contenido de los archivos "Pruebas sustantivas" mantenidos en medios inteligibles solo para las computadoras.

También se describen otras técnicas de como la computadora puede ayudar al auditor para el manejo de su auditoría.

A) Lote de datos de prueba:

Esta técnica equivale a las pruebas de cumplimiento de los controles que lleva a cabo el auditor al efectuar el seguimiento de las operaciones a través de los sistemas.

La utilización de esta técnica consiste en la preparación por el auditor de juegos de datos de entrada a la computadora que le presenten un repertorio de transacciones reales y ficticias,

pero que sean procesados mediante el programa usado en el desarrollo normal de los procesos, con el propósito de identificar resultados predeterminados.

Las pruebas son normalmente registradas en archivos temporales o falsos para evitar interferencias en los archivos reales de la computadora.

Estas pruebas están orientadas a probar operaciones automáticas que realiza la computadora, tales como cálculos, asientos, registros, sumarizaciones, resúmenes, limites, rechazos, etc.

En general, esta técnica esta designada a probar el cumplimiento de los controles en los sistemas y confirmar que la información esta siendo debidamente procesada, registrada e incluida en informes finales a los usuarios.

Los principales controles internos en los programas que el auditor prueba con esta técnica son:

- Validación de los datos de entrada y la efectividad para rechazar información errónea y no autorizada.
- Controles de acceso para modificar archivos maestros y manejo en general de los archivos de transacciones (registros).
- Procedimientos para realizar cómputos correctos (sumas, balanceo o cuadre de cifras, etc.)
- Controles sobre los accesos a terminales.

Los datos que preparará e introducirá el auditor para probar los controles internos en un sistema, por ejemplo de nominas, incluirán la siguiente información:

- Empleados dados de baja
- Empleados con sueldos exagerados
- Códigos de identificación erróneos e incompletos
- Horas extras arriba de los normal
- Deducciones mayores a los ingresos

Asimismo, a través de la preparación de ciertas pruebas, el auditor podrá probar la corrección del sistema de valuacion de los inventarios físicos. Esta técnica es de gran utilidad para probar inventarios voluminosos; asimismo, en sistemas en línea, a través de tratar de introducir información ficticia, se podrá determinar si los controles internos para rechazar, controlar e informar de estos excesos inaceptables funcionan adecuadamente.

La ventaja de esta técnica es que puede ser utilizada por personal con limitada capacidad en procesamiento electrónico de datos, además de que requiere poca asistencia técnica. Es excelente para verificar programas con variedad de procesos limitados y para aplicaciones en línea, donde los archivos se actualizan al momento en que se realizan las transacciones.

El auditor debe planear la aplicación de esta técnica en cuanto a la oportunidad del uso de la computadora y de los programas, pues de preferencia debe utilizarse inmediatamente después que los programas normales han sido utilizados en los procesos rutinarios y utilizar también de preferencia, la técnica de bitácora. El auditor deberá ejercer sumo cuidado en sistemas en líneas, por la ramificaciones que pueden existir al introducir información ficticia a los sistemas. En sistemas complejos y con gran variedad de procesos, el auditor deberá determinar en forma anticipada todas las condiciones variables y alternativas en los programas y afectaciones en los bancos de datos, estadísticas, etc.

B) Datos de prueba integrados

En este caso, se establece una sección ficticia dentro del proceso, en donde se procesaran las pruebas del auditor, pero con la peculiaridad de que serán procesadas al mismo tiempo en que las transacciones reales se llevan a cabo.

También puede desarrollarse esta aplicación, si las circunstancias lo permiten, eliminando la sección ficticia e introduciendo las pruebas del auditor al mismo tiempo que las transacciones reales.

Con esta técnica se obtiene una razonable certeza de que las transacciones reales y las pruebas del auditor son procesadas al mismo tiempo y con el mismo programa y sujetas ambas a los mismos controles internos.

Esta técnica es muy útil en sistemas complejos con gran diversidad de transformación de la información sin dejar huellas visibles, así como en sistemas en línea y con varias terminales de acceso de información.

Al aplicar esta técnica deberá existir plena autorización de la gerencia, pues se introducirá información al flujo normal de la información, así como de una correcta y oportuna coordinación con los diversos departamentos de la empresa involucrados y tener la certeza de que posteriormente podrán eliminarse totalmente las pruebas de los archivos reales y sobretodo, de los bancos de datos, estadísticas, etc.

C) Simulación paralela:

Esta técnica consiste en la formulación por el auditor de su propio programa (a través de programas especiales o de paquetes de auditoría) para realizar el mismo proceso que efectúa el programa del cliente, utilizando la misma información fuente, para luego cotejar resultados. El propósito de esta técnica es verificar la lógica del programa de computadora, así como lo adecuado de los controles asistentes en el mismo.

D) Verificación de los programas a través del estudio de los diagramas:

Solicitar un diagrama de lógica del programa, el cual podrá ser estudiado por el auditor para determinar la confiabilidad de los sistemas. El uso de esta técnica es útil para probarlos

programas en sistemas sencillos. En caso de sistemas complejos se puede requerir asistencia técnica para comprender y evaluar la lógica del proceso; desde luego, con la capacitación adecuada, el auditor podrá estudiar y evaluar directamente los programas fuente de la computadora y cerciorarse de que dicho diagrama coincide con lo que hace el sistema.

Técnicas para comprobar el contenido de los archivos usados en procesamiento electrónico de datos utilizando la computadora (Pruebas Sustantivas)

Normalmente la comprobación manual de estos archivos es impráctica por lo tardado y difícil que resultaría, por la falta de huellas visibles y por los alcances limitados que se obtendrían; por los tanto, el auditor puede utilizar las técnicas que a continuación se describen para probar la validez de la información contenida en los archivos, aprovechando la velocidad y exactitud de la computadora.

Las técnicas para probar el contenido de los archivos usados en procesamiento electrónico de datos son la preparación de programas especiales y el uso de paquetes de auditoría, y son los que se describen a continuación:

E) Programas especiales

En este caso, el auditor elabora sus propios programas para procesar cierta información contenida en archivos de computadora y así poder obtener evidencias suficientes para su posterior evaluación.

Para la elaboración de estos programas especiales, el auditor puede seguir las siguientes alternativas:

1. Prepararlos el mismo si tiene la capacidad técnica para ello.
2. Que personal del cliente en el área de procesamiento electrónico de datos los prepare.
3. Contratar a un especialista para que los formule.

El uso de esta técnica puede ser costoso ya que implica la inversión de tiempo para la elaboración y prueba de los programas. Sin embargo, este inconveniente puede evitarse utilizando los paquetes de auditoría que, en términos generales, cumplen con los mismos objetivos existentes en el empleo de los programas especiales, pero siendo su empleo mucho mas flexible, sencillo y menos costoso y al alcance del auditor en lo que se refiere a su manejo.

F) Paquetes de auditoría.

Es un conjunto de programas que permite al auditor aplicar una serie de técnicas para verificar controles internos en los sistemas pero sobre todo, para extraer y procesar información de los archivos con mayor facilidad.

Estos paquetes han sido desarrollados por fabricantes de computadoras, por las firmas de contadores y de consultaría, con el propósito de que, de una manera rápida, flexible y sencilla el auditor, después de un breve entrenamiento, pueda utilizar la computadora y sus archivos para fines de su auditoría, sin requerir de mayor asistencia técnica para obtener ahorros importantes de tiempos de auditoría.

Se piensa que el uso de estos paquetes es una de las mejores formas en que el auditor puede, eficiente e independientemente, intervenir en los ambientes de computación, ya que obtiene flexibilidad en la utilización de la computadora y sus archivos.

Las aplicaciones de los paquetes de auditoría son muy amplias y a manera de ejemplo de los beneficios que el auditor puede obtener de esta técnica, son obtener amplios alcances en la verificación de las operaciones con el consecuente ahorro de tiempo de auditoría.

A continuación se anuncian algunas de las formas en que esta técnica puede ser utilizada:

1o. Para examinar la corrección de los registros:
2o. Para verificar cálculos y hacer cómputos:
3o. Para comparar información en diferentes archivos:
4o. Para seleccionar e imprimir pruebas de auditoría:
5o. Para sumarizar, reclasificar y analizar información:
6o. Para comprobar información obtenida a través de la auditoría con los archivos en la computadora.

OTRAS TÉCNICAS

Existen otras técnicas para comprobar controles internos, todas con la característica de usar la computadora en mayor o menor grado, sin embargo, son derivaciones de las técnicas antes mencionadas.

G) Prueba especifica:

Prueba para verificar cálculos o procesos específicos simultáneamente al proceso real (cálculos de depreciación, interés, añejamiento de cuentas por cobrar, etc.).

H) Pruebas de sistemas en línea:

Pruebas para verificar sistemas donde las transformaciones, conforme ocurren, se procesan inmediatamente en los archivos de la computadora a través de terminales. En estos sistemas existe una serie de controles internos en los programas para evitar que se introduzcan operaciones no autorizadas a través de claves, o bien, aquellas que no están completas o con datos erróneos. En estos casos, los sistemas normalmente prevén informes de las transacciones procesadas por cada terminal y por cada operario para conocer intentos de acceso no autorizados, transacciones incompletas no procesadas y las transacciones procesadas que sirvan de base para compararlas con los datos fuente que dieron origen a la operación.

En este contexto, el auditor podrá introducir una serie de pruebas para comprobar que ciertos controles internos claves estén cumpliendo con su objetivo.

En sistemas complejos (muchas transacciones de procesos múltiples de cálculos, con varias terminales y utilizando base de datos), no será posible suspender los procesos de la computadora y copiar archivos para que el auditor procese su lote de datos de prueba y, en este caso, deberá emplearse la técnica de datos de prueba integrados conjuntamente con esta técnica.

I) Imagen del contenido de la memoria:

Esta técnica consiste en solicitar una impresión de cierta parte del programa registrada en la unidad central de la computadora.

Si el auditor quisiera ver la lógica y probar la razonabilidad de ciertas instrucciones (valores que en memoria tienen algunas variables), deberá solicitar una copia de la parte correspondiente para evaluarla. En estos casos, generalmente, el auditor deberá solicitar asistencia técnica para poder leer la sección extraída.

J) Seguimiento o rastreo:

Consiste en listar los pasos de los procesos de la computadora para proporcionar una evidencia de auditoría de la lógica de los programas. Una vez determinado esto, el auditor podrá hacer seguimiento de ciertas operaciones antes de su proceso hasta su registro final conforme a los indicado en el programa, o sea, prueba la entrada, el proceso y la salida.

K) Modulo de auditoría integrados:

Esta técnica consiste en incluir en un sistema un conjunto de programas que ejecuten funciones propias de auditoría al momento de procesar una aplicación.

L) Evaluación de casos base:

Consiste en probar, con base en lotes de datos de prueba, los programas antes de que estos sean implantados definitivamente en los sistemas.

M) Bitácora:

Los sistemas producen información relativa al uso de la computadora, archivos utilizados, programas ejecutados, tiempo de maquina empleado, interrupciones, registros procesados, cambios de programas, etc.; la lectura de estas bitácoras por el auditor podrá darle seguridad de que no ha habido cambios no autorizados. El uso de las bitácoras es importante para el auditor cuando lleva a cabo sus pruebas con la computadora, pues podrá cerciorarse de que se están empleando los programas correctos y no otros y que no haya habido paros, interrupciones, introducción o eliminación de información, etc.

N) Mapeo:

Es una técnica que permite conocer el orden en que fueron ejecutadas diferentes rutinas de un programa por ejemplo, cuantas veces fueron llamados, quienes los llamaron, así como el cruce entre variables y rutinas.

II.6. METODOLOGÍA.

El auditor en Informática debe contar con conocimientos y experiencia especializada para efectuar o supervisar con efectividad la auditoria ya sea que la desarrolle directamente o en coordinación con especialistas en informática. Siendo el procesamiento electrónico de datos un área que requiere de especialización la metodología planteada en el boletín 7 en la comisión de auditoria operacional del Instituto Mexicano de Contadores Públicos (IMCP) es general y no se enfoca a ningún tipo de equipo de procesamiento electrónico de datos o empresa en particular.

I)El método para auditar la operación de los centros de procesamiento electrónico de datos que a continuación se describen esta organizado de conformidad a la estructura señalada en el boletín número 2 de la Comisión de Auditoria Operacional.

I.1.) Familiarización.

El auditor debe familiarizare con el centro de procesamiento electrónico de datos mediante el estudio de:

a) La estructura de organización del centro de procesamiento electrónico de datos y su ubicación dentro de la organización general de la empresa.
b) Los planes a corto y largo plazo relacionados con el procesamiento electrónico de datos y su coordinación con los planes y objetivos de la empresa.
c) Los manuales de políticas y procedimientos de las diferentes actividades desarrolladas en el centro de procesamiento electrónico de datos, incluyendo su administración.
d) Los informes resultantes de revisiones efectuadas anteriormente por auditores internos y externos y consultores.
e) Los antecedentes del centro de procesamiento electrónico de datos en relación a su origen, desarrollo, equipo de proceso de datos original y sus modificaciones, relaciones con usuarios, prioridades en el desarrollo de sistemas, etc. y
f) Los estados financieros de la empresa y el impacto que tienen los costos y gastos del centro de procesamiento electrónico de datos en los resultados de operación

Así mismo, el auditor deberá conocer:

a) Cuales son las principales áreas que reciben servicio del centro de procesamiento electrónico de datos y que importancia tienen estas en relación a la empresa, tanto financiera como operativamente.
b) Cuales sistemas están automatizados y en que grado y cuales sistemas importantes susceptibles de automatizarse no lo están.
c) Una descripción detallada de la configuración de equipo de procesamiento electrónico de datos y del sistema operativo, la cual deberá incluir: marca, modelo, cantidad, capacidad y velocidad de la unidad central de proceso, de las unidades periféricas y otro equipo

I.2)Visita a las instalaciones.

Deberán visitarse las instalaciones correspondientes al centro de procesamiento electrónico de datos, incluyendo los lugares en donde se guardan los archivos de respaldo y hacer observaciones sobre:

a) Lo adecuado de su ubicación y de la distribución de las áreas de trabajo y las medidas para restringir el acceso a personal no autorizado.
b) Los controles y aparatos para conservar la temperatura y el grado de humedad dentro de los límites especificados por el proveedor del equipo de cómputo, dentro del área en que se encuentra este instalado.
c) Las medidas establecidas para la detección y contención de incendios detectores de humo prohibición de fumar, sistema de extinción de fuego, etc.
d) El orden y limpieza del equipo y accesorios (Discos, cintas, tarjetas, disquetes, etc.) y de la documentación.
e) Las condiciones ambientales (luz, ventilación, etc.), y
f) Las relaciones de trabajo entre jefes y subordinados y de estos entre sí.

I.3). Investigación y análisis. Análisis de la información financiera y operativa

Por la naturaleza de las actividades de los centros de procesamiento electrónico de datos, es principalmente operativa el auditor deberá obtener y analizar objetivamente la información que se menciona a continuación:

a) Presupuesto de gastos del centro de procesamiento electrónico de datos comparado contra los gastos reales.
b) Estadísticas de tiempo extra trabajado y las razones que lo motivaron.
c) Reportes de recepción de documentos fuente que incluyan información sobre la documentación recibida después de las fechas y horas programadas.
d) Estadísticas sobre la captura de datos fuente (número de golpes por hora y errores por operador).
e) estadísticas de uso de la unidad central de proceso y del equipo periférico (incluyendo terminales remotas) que muestren:

- Producción normal
- Reprocesos
- Corridas especiales
- Pruebas y compilaciones de nuevos programas
- Mantenimiento de equipo y sistema operativo
- Fallas del equipo
- Tiempo ocioso

Cuando sea aplicable deberá obtenerse el detalle a nivel de participación

f) Reportes de actividad por terminal (frecuencia de uso, duración, errores de operación)

g) Estadísticas de mantenimiento por cada unidad de equipo preventivo y por fallas
h) Estadísticas de entregas de reportes a usuarios con datos sobre calidad oportunidad y necesidades de proceso por errores
i) reportes de tiempo incurrido y grado de avance comparados contra presupuestos, por los diferentes proyectos de desarrollo de nuevas aplicaciones y mantenimiento de las existentes.
j) Estadísticas de ocupación de personal, mostrando tiempo productivo, de entrenamiento, vacaciones, rotación, etc.

En caso que la información solicitada no se prepare como parte de las actividades normales del centro de procesamiento electrónico de datos, el auditor deberá evaluar el esfuerzo requerido y la disponibilidad de datos para que se proporcione y solicitar su preparación

I.4)Entrevistas.

Debido a que esta técnica proporciona al auditor información valiosa para el desarrollo de su trabajo, se deberá:

a) Planear las entrevistas necesarias para obtener información sobre la ejecucion practica de las politicas y procedimientos estudiados en la fase de familiarización.
b) Utilizar cuestionarios que sirvan como guía para obtener información sobre el centro de procesamiento electrónico de datos y las actividades que en el se realizan.
c) Efectuar entrevistas con el personal que el auditor considere conveniente y que deberá abarcar los siguiente grupos

- Personal que trabaja en el centro de procesamiento electronico de datos incluyendo las siguientes áreas: gerencia, análisis y diseño de sistemas, programación, operación del equipo, mesa de control, biblioteca de cintas y discos.

- Directivos de la empresa, con objeto de conocer el grado en que participan en el desarrollo de los planes relativos al procesamiento electrónico de datos y la coordinación con los planes generales de la empresa, el grado de supervisión que ejercen sobre el centro procesamiento electrónico de datos y las expectativas en relación al servicio que debe proporcionar el centro de procesamiento electrónico de datos a la empresa en general.

- Usuarios de los servicios procesamiento electrónico de datos, para conocer el grado en que participan en el desarrollo de nuevos sistemas, la forma en que se atienden sus soluciones de servicio, la calidad y oportunidad de la información que reciben, el uso que les dan a los reportes recibidos y la utilidad de la información que contienen y la naturaleza de las relaciones con el personal del centro de procesamiento electrónico de datos.
- Auditores internos y externos para conocer el grado en que participan en el desarrollo de nuevos sistemas, la naturaleza de las revisiones que han efectuado al centro de

procesamiento electrónico de datos y la forma en que utilizan el equipo procesamiento electrónico de datos como herramienta de auditoría.

- Personal de organización y métodos manuales, para conocer su relación con el centro de procesamiento electrónico de datos y su grado de participación en el desarrollo de sistemas automatizados.

I.5)Examen de la documentación.

Además de los documentos estudiados en las etapas de familiarización y análisis de la información financiera y operativa, el auditor deberá examinar otra documentación que puede ser:

1. Descripciones de puestos
2. Evaluaciones periódicas de la actuación del personal del centro de procesamiento electrónico de datos
3. Programas de entrenamiento para el personal del centro de procesamiento electrónico de datos y los usuarios.
4. Estudios de factibilidad para adquisición y ampliación del equipo, compra de programas paquetes y desarrollo de nuevos sistemas.
5. Manuales de estándares de análisis, diseño y documentación de sistemas, de programación y de operación.
6. Documentación de algunos sistemas importantes.
7. Registros de flujo de documentos y datos dentro del centro de procesamiento electrónico de datos.
8. Registros de datos erróneos con datos sobre su conexión y reincorporación al proceso.
9. Programa de uso de equipo.
10. Bitácoras de uso del equipo
11. Procedimientos de custodia, retención y reconstrucción de archivos y programas.
12. Planes de acción en caso de siniestros o fallas prolongadas del equipo.

Durante la ejecución de su revisión el auditor deberá tener presente aquellos aspectos que deben existir en un centro de procesamiento electrónico de datos y cuya ausencia puede afectar la eficiencia de sus operaciones, con el objeto de evaluar la información obtenida en el desarrollo de los pasos anteriores y determinar la existencia de posibles problemas a continuación se mencionan algunos de los principales aspectos a considerar.

a) Estructura de organización balanceada y con una adecuada segregación de funciones

b) Entrenamiento y supervisión adecuados, debidamente documentados para asegurar competencia e integridad personal.

c) Existencia de estándares de actuación y vigilancia de su cumplimiento.

d) La dirección de la empresa interviene en un grado satisfactorio en los planes y administración del centro procesamiento electrónico de datos y el desarrollo de aplicaciones y vigila su coordinación con las políticas, objetivos y planes generales de la empresa.

e) Existencia de procedimientos relacionados con el desarrollo de nuevos sistemas y el mantenimiento de los existentes que permitan una administración adecuada de los proyectos, así como una orientación de los recursos de procesamiento electrónico de datos hacia las áreas de la empresa en donde se obtendrá el mayor beneficio, incluyendo un grado satisfactorio de participación del usuario.

f) La capacidad del equipo instalado es adecuada para las necesidades de la empresa a corto plazo y tiene la flexibilidad para incrementarse de acuerdo a futuros requerimientos además, los conocimientos del personal de procesamiento electrónico de datos y el apoyo que proporciona el proveedor del equipo, permiten utilizar el equipo actual en una forma eficiente, tomando en consideración el uso del sistema operativo y otros programas de soporte (software) mas adecuados al tipo de aplicaciones existentes.

g) Existencia de procedimientos para programar y controlar adecuadamente el uso del equipo de procesamiento electrónico de datos incluyendo terminales remotas y para detectar oportunamente las fallas habidas (del equipo y de personal).

h) Existencia de procedimientos que razonablemente, aseguren que los datos recibidos son controlados y capturados adecuadamente que la información es procesada en su totalidad, sin duplicaciones y alteraciones los reportes son completos, correctos y su distribución es controlada adecuadamente, y el proceso de los datos se lleva a cabo de acuerdo a lo requerido por la aplicación respectiva.

i) Existencia de procedimientos de seguridad y protección que aseguren razonablemente: acceso restringido a personas no autorizadas a los datos, programas y actividades de operación, medidas preventivas y correctivas en caso de siniestros y fallas prolongadas del equipo, reconstrucción de archivos y programas destruidos accidentalmente o por otras causas continuidad en las acciones de procesamiento electrónico de datos en caso de incapacidad del centro de procesamiento electrónico de datos de la empresa para operar normalmente.

II) La Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos (IMCP) en el boletín F-06 señala la siguiente metodología de conformidad con las Normas de Auditoría relativas a la ejecución del trabajo para efecto del procesamiento electrónico de datos en sus pruebas de auditoría.

En términos generales, se señalan tres fases, las cuales se observaran considerando:

1. Características de procesamiento electrónico de datos.
2. La importancia de las aplicaciones.

3. El grado de transformación (desde compilaciones sencillas de datos hasta transformaciones sofisticadas de las huellas o pistas dejadas en estos procesos, ya sean estas visibles o incorporadas en los mismos sistemas y estas ultimas solamente pueden ser localizadas y verificadas a través de pruebas usando la misma computadora).

4. El grado de confianza que el auditor deba depositar en los sistemas de control interno integrado al procesamiento electrónico de datos.

Las fases son las siguientes:

Primera Fase. Estudio preliminar. Obligatorio y necesario efectuar en todas las empresas que usen en alguna forma el procesamiento electrónico de datos para la obtención de su información financiera.

Segunda Fase. Ampliación del estudio del control interno. De aplicación obligatoria cuando en el estudio preliminar se ha determinado que se tienen aplicaciones de importancia para la obtención de la información financiera, que existen transformaciones importantes en la información y de que el auditor tiene que confiar en una medida importante en el control interno que existe sobre dichas aplicaciones.

Tercera Fase. Pruebas a los controles de procesamiento electrónico de datos. De aplicación obligatoria cuando la importancia de los sistemas sujetos a procesos sea tal en cuanto a las transformaciones de información y al grado de confianza que el auditor depositara en el control interno, que el no efectuar pruebas de cumplimiento a los controles de procesamiento electrónico de datos limita el alcance del trabajo del auditor al no obtener la necesaria evidencia suficiente y competente.

Habrá casos en que el auditor deba necesariamente que confiar en el control interno del procesamiento electrónico de datos y, por lo tanto, tenga que evaluarlo después probarlo en forma completa e integral a través de pruebas de cumplimiento. Sin embargo, también habrá casos que por el resultado esperado de sus pruebas sustantivas, de importancia relativa y de riesgo probable, el auditor obtendrá la necesaria evidencia suficiente y competente que le permita solamente evaluar ciertos controles internos importantes y reducir substancialmente sus pruebas de cumplimiento, limitándolas estas a probar controles internos importantes de entrada, proceso y salida y, por lo tanto, solamente cumplir con la primera fase y, según las circunstancias, cubrir parcialmente la segunda y omitir la tercera.

Es importante señalar que desde la primera fase se requiere de experiencia en auditoria en procesamiento electrónico de datos por parte del auditor y conforme se vaya pasando a las siguientes fases, se requerirá de mayor capacitación.

III) La metodología para realizar un estudio y evaluación de controles internos dentro de un sistema de procesamiento electrónico de datos será conceptualmente el mismo que dentro de un sistema manual. la metodología para un sistema de procesamiento electrónico de datos es la siguiente:

PASOS	TRAYECTORIA DE DESICION
• Realizar un estudio preliminar del sistema de contabilidad, así como de los controles generales y de aplicación para determinar si se justifica un estudio mas profundo.	• realizar un estudio mas amplio del control interno o proceder a realizar pruebas mas amplias de auditoría.
• Terminar los estudios de controles generales y de aplicación y realizar una evaluación preliminar de controles establecidos.	• Identificar controles sobre los que se descansaran, suponiendo un cumplimiento satisfactorio, y proceder a las pruebas de cumplimiento; o proceder a ampliar las pruebas de auditoría.
• Realizar pruebas de cumplimiento sobre controles en los cuales se descansara	• Para los controles en que el cumplimiento es satisfactorio, proceder con pruebas de auditoría limitadas, cuando el cumplimiento no es apropiado, ampliar las pruebas de auditoría.
• Realizar una evaluación final de los procedimientos de control.	

III. ESTUDIO GENERAL

III.1. OBJETIVO.

Planear el examen y, como parte de la estrategia general de auditoría, decidir la naturaleza, oportunidad y alcance de la pruebas de auditoría que aplicará (qué procedimientos seguirá, cuando los seguirá y cuantas pruebas aplicará), el auditor dispone de varias estrategias alternativas. En esas decisiones influirán las respuestas a preguntas como estas: ¿Que método ofrece el nivel mas alto de seguridad? ¿Que método es mas eficiente? ¿Cuales son los riesgos principales del negocio del cliente?. No se pretende que estos factores sean exhaustivos, pero si indican los tipos de consideraciones y juicios que debe hacer el auditor.

1. Determinar las principales aplicaciones y su efecto en la información financiera.

2. Conocer las características del equipo de procesamiento electrónico de datos.

3. Concluir sobre el efecto del procesamiento electrónico de datos en la información financiera y en su caso, pasar a la Fase de Pruebas a los controles de procesamiento electrónico de datos.

4. Evaluar la organización del centro de cómputo y los controles generales establecidos.

5. Conocer las características de las aplicaciones y de sus impacto en la información financiera y evaluar los controles de aplicación específicos inherentes a las mismas, considerando el grado de transformación de la información y el volumen de operaciones que dependen del procesamiento electrónico de datos, a efecto de poder juzgar si se deben efectuar pruebas de cumplimiento de los controles del procesamiento electrónico de datos.

6. Formarse un juicio sobre la eficacia del control interno existente en procesamiento electrónico de datos que permita determinar la naturaleza, el alcance y oportunidad de los procedimientos de auditoría, tanto de cumplimiento como sustantivos.

7. Concluir sobre los resultados obtenidos y, en su caso, pasar a la Fase de Pruebas referentes a los controles de procesamiento electrónico de datos, considerando que el no probar los controles de procesamiento electrónico de datos resultaría una limitación importante en el alcance de la auditoría, pues el auditor no obtendrá la necesaria evidencia suficiente y competente.

III.2. RECOPILACION.

El auditor debe obtener información detallada respecto a las características del flujo de operaciones en el área de cómputo de la organización.

Esto implica conocer previamente la estructura de la empresa, con el fin de identificar los ciclos de operaciones en que se localizan los sistemas, los procedimientos y los métodos a que el auditor se enfrentara, por ello es necesario que durante la fase de recopilación de información el auditor conozca profundamente estos aspectos.

La primera etapa de recopilación de información se basa en las siguientes técnicas:

I) Entrevistas
II) Observaciones de campo
III) Cuestionarios

I) Entrevistas.

Las entrevistas son conversaciones que tiene el auditor para obtener información detallada sobre las características de un sistema, procedimiento o método.

Las entrevistas deben celebrarse, en primera instancia, con el ejecutivo de mas alta jerarquía a cuyo cargo este el área de cómputo. Las entrevistas con funcionarios y empleados de menor jerarquía serán necesarias a medida que la investigación involucre mas detalles de los procedimientos y métodos en vigor.

Durante las entrevistas, un recurso de trabajo indispensable para el auditor son las siguientes interrogantes:

- ¿ Qué ?
- ¿ Para qué ?
- ¿ Cuándo ?
- ¿ Quién ?
- ¿ Cómo ?
- ¿ Cuánto ?

Aplicadas con perspicacia e inteligencia, cada una de estas interrogantes permite al auditor obtener datos muy valiosos en esta etapa de recopilación.

La interrogante ¿QUE? es muy útil para conocer las actividades en el área de cómputo de la organización un enfoque general, es el que permite al auditor conocer las características generales y particulares de los métodos y procedimientos vigentes en la entidad.

La pregunta ¿PARA QUE? permite conocer el propósito y como se realizan las actividades del área de cómputo o la toma de una decisión.

A su vez, las interrogante ¿CUANDO? Y ¿QUIEN? permiten al auditor conocer el orden o tiempo en que se llevan a cabo las actividades inherentes a un sistema, así como la persona que las realiza. Por ultimo las preguntas ¿COMO? Y ¿CUANTO? se relacionan con los medios y la cantidad de recursos involuerados en el desarrollo de los trabajos propios del área.

Las anteriores interrogantes son de gran utilidad, sin embargo, la verdadera comprensión del área, el origen autentico de los problemas, la justificación o no justificación de las fallas, los riesgos, las funciones incompatibles, los retrasos en la ejecución de trabajos y actividades y el éxito mismo de la auditoria se logran solo cuando se hace la pregunta ¿POR QUE.?

En esta etapa el auditor debe abstenerse de comentarios o criticas sobre la calidad y confiabilidad de los controles, no solo para evitar inquietudes en el personal del área, sino porque desconoce circunstancias en torno a los sistemas que pueden influir, ser causa o explicar cualquier situación especial respecto a ellos.

Durante el desarrollo de las entrevistas, se deben obtener ejemplares de toda la documentación interna que se utiliza para dar dinámica a los métodos y los procedimientos.

II) Observaciones de campo

Las entrevistas son fundamentales para conocer y estudiar los sistemas: sin embargo, la recopilación de información no será completa y profesional si se carece de las observaciones en el campo donde se desarrollan los métodos y procedimientos.

Observación Directa: Consiste en tomar nota de un hecho que sucede ante el auditor, midiendo el comportamiento externo del individuo esto tiene como objeto el medir el comportamiento de los miembros del área de cómputo ante estimulos internos y externos del área.

La investigación de campo es aquella en la que el mismo objeto del estudio sirve de fuente de información al auditor, el cual recoge directamente los datos del área. Ese método es muy utilizado y se subdivide, en cuatro ramas (FIG 1).

III) Cuestionarios

Al cuestionario se le define como una hoja de cuestiones o de preguntas que se hacen o se proponen para averiguar la verdad. El cuestionario se utiliza para entrevistar al personal o una parte de este.

Antes de elaborar el cuestionario, se necesita identificar el objetivo de la encuesta y relacionar el problema.

Para tener validez, las preguntas del cuestionario deberán recoger los datos necesarios para enjuiciar los métodos o procedimientos que vayan a ser auditados. Para tener verificabilidad, las preguntas deberán poder ser verificables y verificadas por cualquier otro auditor

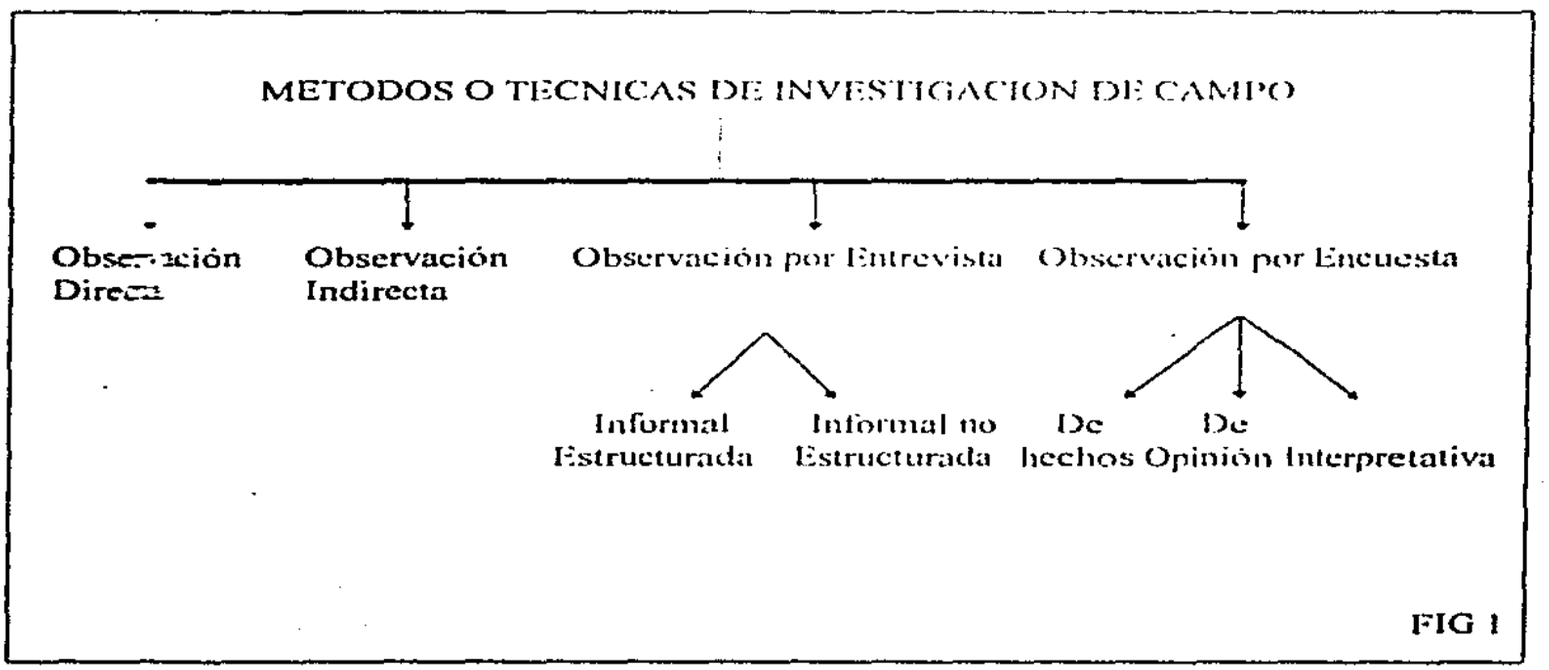

FIG 1

III.3. ANALISIS Y EVALUACION

El análisis del estudio general consta de dos partes la primera es el análisis de la organización del centro de cómputo dentro de esta parte es auditor deberá de asegurase de que:

- No exista incompatibilidad de funciones (por ejemplo que el programador no sea el auditor).
- Se tenga un buen soporte técnico.
- Existan líneas de autoridad bien definidas.
- Haya una planeación a corto y largo plazo.
- Se cuente con políticas bien definidas y acordes a la importancia del departamento y el equipo
- Existan procedimientos para determinar prioridades, asignar proyectos, evaluar resultados, autorizar cambios a los sistemas y fijar los estándares para el desarrollo de sistemas. .

En sistemas pequeños donde no es posible la existencia de todos los controles, deberá determinarse la existencia de controles compensatorios que cubran dicha deficiencia.

La segunda parte es el análisis de los sistemas (Programas), aquí el auditor deberá verificar que el diseño, programación, prueba de datos y mantenimiento de los sistemas esté documentado y de acuerdo a los estándares establecidos, juzgando a su vez lo apropiado de dichos estándares y del flujo de la información.

La evaluación de los controles sobre el proceso de las aplicaciones en esta el auditor deberá verificar los siguientes aspectos:

- Que la información procesada esté sujeta a controles que aseguren que dicha información es valida y completa y que no se procesa información errónea y duplicada.

- Determinar el grado de transformación de la información y asegurarse de que no existan huellas o pistas (visibles o no) que permitan la reconstrucción o seguimiento de la información procesada y de su transformación.

- En caso de información rechazada, que esta sea analizada, corregida y evitada para el futuro y, en su caso, vuelva a ser oportunamente procesada.

Competencia y suficiencia de los elementos de prueba

Competencia

Una norma del trabajo con el cliente exige que el auditor obtenga evidencia que sea suficiente y competente a la vez. Dicho de otro modo, tiene que decidir, con base en la experiencia y el buen juicio, si los elementos de prueba examinados son "buenos" y "útiles" (evidencia competente) y si se han examinado elementos "suficientes" (evidencia suficiente).

Para ser competente, la evidencia debe ser pertinente y confiable. Su pertinencia se refiere a la medida en que contribuye a lograr los objetivos de auditoría fijados. Para ser pertinente, la evidencia debe influir en la posibilidad de que el auditor acepte o rechace una afirmación especifica contenida en un informe. El auditor llega a una conclusión respecto a la presentación imparcial de la información, mediante una serie de evaluaciones hechas a lo largo de la auditoría. Cada elemento de evidencia obtenido es evaluado en términos de su utilidad para el auditor, sea para corroborar o para refutar una afirmación de la gerencia o la evaluación que hizo el auditor de la evidencia obtenida en otras etapas de la auditoría. La pertinencia de la evidencia se mide por el grado en que resulta útil para ese fin.

La evidencia debe ser también confiable para que resulte de utilidad para el auditor. Confiabilidad es "aquella cualidad de la información que garantiza que dicha información es razonablemente libre de error y parcialidad y representa fielmente lo que pretende representar". Como sinónimos de confiabilidad tenemos "formalidad" y "veracidad". Varios factores influyen en la confiabilidad de la evidencia de auditoría

- **Independencia de la fuente**. La evidencia obtenida fuera de la entidad que se examina ofrece por lo general mas garantía de confiabilidad que la que se obtiene exclusivamente dentro de la entidad. En cambio la evidencia proveniente de las preguntas hechas al cliente o de la inspección de documentos proporcionados por el cliente se considera por lo general menos confiable desde el punto de vista del auditor

- **Capacidad de la fuente.** Para que la evidencia de auditoría sea confiable, debe ser obtenida de personas competentes y que tengan la capacidad necesaria para que su información este libre de errores. El auditor no debe suponer necesariamente que mientras mas elevado sea el cargo que desempeña una persona en la empresa mas calificada esta para proporcionar evidencia. Además, los auditores deben poner en duda su propia capacidad cuando evalúan la evidencia que han obtenido.

- **Sistema de control interno.** El auditor no acepta la desempeño del sistema hecha por el cliente si corroborarla. Mas bien, si el auditor tiene la intencion de confiar en controles, observa las actividades del personal de la empresa y pone a prueba los controles para tener la seguridad de que existen realmente y están funcionando en la forma prevista.

- **Objetividad de la evidencia.** La evidencia será objetiva si hay que pensar poco para evaluar su exactitud. La evidencia obtenida directamente por conocimiento personal de auditor, observando, calculando o inspeccionando es por lo general mas objetiva que la basada en la opinión de otras personas. A veces sin embargo, no es posible tener evidencia objetiva.

El objetivo del auditor al practicar una auditoria, consiste en lograr el nivel de seguridad necesario para apoyar su opinión de auditoría y en practicar la auditoría tan eficientemente como sea posible. De manera que, además de considerar la pertinencia y confiabilidad de la evidencia, el auditor debe tener en cuenta también, su disponibilidad, su oportunidad y su costo. A veces, una forma deseada de evidencia simplemente no se encuentra disponible. Los distintos tipos de evidencia van asociados con costos diferentes, y el auditor debe considerar la relación costo-beneficio.

Por fortuna, los auditores disponen normalmente de mas de una fuente de evidencia y de mas de un método para obtenerla. Si una fuente o método no resulta practico, se substituye o bien, una fuente de evidencia mas costosa puede substituir a otra menos costosa pero que no se encuentra disponible. El auditor debe elegir el tipo de evidencia y los métodos para obtenerla (la evidencia corroborativa se busca a menudo aplicando mas de un método) que ofrezcan el nivel de seguridad requerido al costo mas bajo.

El proceso de auditoria.

El nivel de seguridad que el auditor trata de obtener mediante el proceso de obtener y evaluar evidencia de auditoría es el que necesita para respaldar una opinión sin salvedades. No puede quedar satisfecho con menos de ese nivel de seguridad para tal fin. Las fuentes y las maneras de obtener la evidencia necesaria, la cantidad requerida de cada tipo de evidencia y el momento en que se aplicaran los procedimientos para obtenerla se pueden variar de acuerdo con las circunstancias de cada trabajo; así se acrecentara la eficiencia con la que se practicará la auditoria.

Suficiencia

La determinación de la suficiencia de los elementos de prueba implica decir que tanta evidencia es suficiente para lograr el nivel de seguridad requerido. La cantidad de evidencia necesaria depende en parte de la minuciosidad con la que el auditor la busque, en parte de su capacidad para evaluarla objetivamente y en parte del nivel de seguridad necesario para apoyar la opinión en una determinada auditoría. En algunos procedimientos de auditoria, la cantidad de evidencia necesaria corresponde necesariamente a la decisión de aplicar o no un cierto procedimiento: lo aplica o no lo aplica.

Tipos de pruebas y procedimientos de auditoria.

Los tipos de evidencia y la manera de obtenerla descritos anteriormente se pueden clasificar también de acuerdo con la finalidad para la cual se obtiene evidencia. Vistos en términos de finalidad, todos los procedimientos de auditoria, llamados a menudo "pruebas", se pueden clasificar en uno de dos tipos: pruebas de cumplimiento y pruebas de sustancia.

Las pruebas de cumplimiento se llevan a cabo para determinar que tan bien están funcionando ciertos controles internos especificos. Su objetivo es proporcionar al auditor evidencia de que los controles están funcionando como lo prescribe el sistema.. El auditor puede confiar en el funcionamiento de ciertos controles internos, a fin de reducir la cantidad de evidencia que de otro modo tenia que obtener, los controles tendrán que ser sometidos a una prueba de "cumplimiento".

Evidencia y pruebas de auditoria.

Las pruebas de sustancia consisten en exámenes de los detalles de las operaciones, procedimientos de revisión analitica y otros procedimientos de auditoria. La finalidad de las pruebas de sustancia es proporcionar al auditor evidencia directa de la validez de la afirmaciones de la gerencia o bien, en caso contrario descubrir errores o irregularidades.

Decisiones sobre la evidencia de la auditoria.

La cantidad y las clases de evidencia que en opinión del auditor son necesarias para tener una base razonable que permita formarse una opinión de la información, así como la coordinación de los procedimientos seguidos para obtener la evidencia, son cuestiones que requieren un juicio profesional hecho después de estudiar cuidadosamente las circunstancias de un trabajo en particular y considerar los diversos riesgos asociados con la auditoria. La meta de toda auditoria debe ser efectuar el examen en forma efectiva y eficiente.

Por lo general, el auditor encuentra que es necesario confiar en evidencia persuasiva mas bien que convincente. Al decidir que tanta evidencia persuasiva es suficiente, el auditor debe trabajar dentro de limites de tiempo, teniendo en cuenta el costo que implica tener evidencia y evaluar la utilidad de la que se a obtenido. Cuando toma esas decisiones, el auditor no puede pasar por alto el riesgo que representa el expresar una opinión inadecuada o justificar la omisión de una determinada prueba solo porque es de aplicación difícil o costosa.

Una opinión sin salvedades exige que el auditor no tenga dudas importantes a cerca de cualquier partida también importante que aparezca en la información. La seguridad negativa (una declaración en el sentido de que el auditor no encontró nada que de lugar a dudas a cerca de la imparcialidad de la información) no es adecuada. El auditor debe abstenerse de formular una opinión mientras no haya obtenido evidencia competente y suficiente para eliminar cualquier duda de importancia.

III.4. DECISION DE TIPO DE REVISION

La decisión del tipo de revisión de auditoría en informática a realizar es la fase final del estudio. En esta etapa el auditor debe ampliar su conocimiento acerca de los controles obtenidos durante el estudio general mediante investigaciones adicionales, observación, revisión de la documentación y análisis detallado de la misma.

Si se descubren fallas significativas en los controles generales, el auditor podrá dar por terminado el estudio, dado que los controles generales tienen repercusiones serias sobre los controles de aplicación, sin embargo, cuando no existen fallas significativas en los controles generales el auditor procede a concluir su estudio de los controles de aplicación que pertenecen a cada una de las áreas operativas del área de cómputo, significativas, por lo tanto, será necesario obtener respuestas respecto a lo adecuado de los controles.

Por la importancia que han adquirido los sistemas de procesamiento electrónico de datos en la información general de una organización así como el volumen de información procesada en ellos, el objetivo de la evaluación preliminar es identificar procedimientos de control específicos en los cuales se podrá confiar al realizar las pruebas de auditoría suponiendo que se cumple satisfactoriamente con los procedimientos prescritos. Si no hubiera controles que parecieran confiables, el auditor procede directamente al diseño y ejecución de las pruebas de auditoría mas amplias.

Respecto a los controles que parecen ser confiables, el auditor realiza pruebas de cumplimiento para determinar si los controles en efecto están en uso y operando conforme a los planeado. Una vez concluidas las pruebas de cumplimiento, el auditor realiza una evaluación final, esta evaluación identifica los procedimientos de control sobre los cuales se puede confiar al realizar las pruebas de auditoría restringidas. Los cursos de acción y los puntos de decisión para el auditor.

Cuando una organización cuenta con diversas unidades operativas en el área de cómputo resultara eficiente obtener información descriptiva una sola vez para todas las unidades; esto ayudara al auditor a determinar los riesgos significativos para cada unidad operativa (por telecomunicaciones, administración de bases de datos, soporte técnico, mantenimiento, etc.) y la toma de decisiones preliminares con respecto al programa y enfoque de la auditoría a realizar.

Un estudio mas profundo del sistema dependerá totalmente del criterio del auditor respecto a si tal esfuerzo se justificará en términos de costos para la terminación de la auditoría.

IV. REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

IV.1. OBJETIVO DE LA REVISION.

El propósito de la revisión es verificar que los objetivos del área o áreas de informática se cubran satisfactoriamente y estén de acuerdo con los objetivos generales de la organización. En particular en esta revisión se debe garantizar que todos los recursos sean adecuadamente coordinados por la gerencia; con la finalidad de lograr los siguientes objetivos:

1. Establecimiento de un comité u órgano interno de Informática
2. La creación y supervisión de una función de seguridad a equipo de cómputo
3. Asignación de responsabilidades y la supervisión de su cumplimiento
4. Distribución de actividades que debe desempeñar cada persona del área.
5. Establecer lineamientos para el desarrollo y mantenimiento de sistemas
6. Participación activa de los usuarios finales con sugerencias para el desarrollo de Sistemas.
7. Establecer una función que asegure la calidad de Sistemas desarrollados
8. Establecer reportes estándar de actividades realizadas
9. Establecer políticas, procedimientos y programas del área de informática

La administración como un fenómeno universal se da donde quiera que existe un organismo social, porque en el tiene siempre que existir coordinación sistemática de medios.

Aunque se distingan etapas, fases y elementos del fenómeno administrativo, este es único y por lo mismo, en todo momento de la vida de una empresa, se están dando, en mayor o menor grado, todos o la mayor parte de los elementos administrativos. Por ello al hacer planes no se deja de mandar, controlar, organizar, etc.

Todo proceso administrativo por referirse a la actuacion de la vida social, forma algo inseparable en el que cada parte, cada acto, cada etapa tienen que estar indudablemente unida con las demás.

Por ello para facilitar su comprensión se presenta a continuación una síntesis de las etapas, elementos y fases que forman el Proceso Administrativo.

PROCESO ADMINISTRATIVO		
FASE	**ELEMENTO**	**ETAPA**
A. MECÁNICA	PREVISIÓN	Objetivos Investigaciones Cursos alternativos
	PLANEACIÓN	Políticas Procedimientos Programas Pronósticos Presupuestos
	ORGANIZACIÓN	Funciones Jerarquías Obligaciones
B. DINÁMICA	INTEGRACIÓN	Selección Inducción Desarrollo
	DIRECCIÓN	Autoridad Comunicación Supervisión
	CONTROL	Su establecimiento Su operación Su interpretación

IV.2. ASPECTOS QUE ABARCA.

PREVISION

La palabra previsión (de prever: ver anticipadamente) implica la idea de cierta anticipación de acontecimientos y situaciones futuras, que la mente humana es capaz de realizar sin la cual sería imposible hacer planes. Por ello la previsión es base necesaria para la planeación.

Elemento de la Administración en el que, con base en las condiciones futuras en las que una empresa habrá de encontrarse, se determinan los principales cursos de acción que permitirán realizar los objetivos de esa organización.

Para hacer previsiones es indispensable:

- Fijar objetivos o fines que se persiguen
- Investigar los factores, positivos y negativos, que nos ayudan y obstaculizan de alguna manera en el logro de objetivos.

- Coordinar los distintos medios en diversos cursos alternativos de acción, que nos permitan escoger alguno con base en los planes.

ORGANIZACIÓN

La palabra organización viene del griego "organon", que significa: instrumento.

Pero quizás ilustre mejor el significado de este concepto, el uso que en nuestra lengua se da a la palabra "organismo".

Este implica necesariamente:

Partes y funciones diversas: ningún organismo tiene partes idénticas, ni de igual funcionamiento.

Unidad funcional: esas partes diversas, con todo, tienen un fin común e idéntico.

Coordinación: precisamente para lograr ese fin, cada una pone una acción distinta, pero complementaria de las demás; obran en vista del fin común y ayuda a las demás; obra en vista del fin común y ayudan a las demás a construirse y ordenarse conforme a una teleología específica.

La Organización se define como la estructuración técnica de las relaciones que deben existir entre las funciones, niveles y actividades de los elementos materiales y humanos de un organismo social, con el fin de lograr su máxima eficiencia dentro de los planes y objetivos señalados.

Por lo anterior podemos decir que:

La organización se refiere "a estructurar"; es quizás la parte mas típica de los elementos que corresponden a la mecánica administrativa.

Por lo mismo, se refiere a "como deben ser las funciones, jerarquías y actividades".

Por idéntica razón, se refiere siempre a funciones, niveles o actividades que "están por estructurarse".

La organización nos dice en concreto como y quién va a hacer una cosa (esto último, en el sentido de qué puesto; no precisamente de qué persona), y como lo va a hacer. Cuando la organización esta terminada, solo resta "actuar", integrando, dirigiendo y controlando, todo lo cual pertenece a otra a la dinámica.

INTEGRACIÓN

Integrar es obtener y articular los elementos materiales y humanos que la organización y la planeación señalan como necesarios para el adecuado funcionamiento de un organismo social.

La planeación nos ha dicho "que" debe hacerse, y "cuando"; La organización nos ha señalado quienes, donde y como deben realizarlo;

Su importancia:

Es el punto de contacto entre lo estático y lo dinámico, lo teórico y lo practico.

Aunque se da en mayor amplitud al iniciarse la operación de un organismo social (conseguir personal, maquinaria, dinero, etc.) es una función permanente, porque en forma constante hay que estar integrado el organismo, tanto para proveer a su crecimiento normal, ampliaciones, etc., como para sustituir a los hombres que han salido por muerte, renuncia, etc., a las maquinas que se han deteriorado, los sistemas que resultan obsoletos, etc.

DIRECCION

La palabra "dirección", viene del verbo "dirigere"; éste se forma a su vez del prefijo "di", intensivo, y "regere": regir, gobernar. Este ultimo deriva del sanserito "raj", que indica "preeminencia".

La direccion es aquel elemento de la administracion en el que se logra la administración efectiva de todo lo planeado, por medio de la autoridad del administrador, ejercida en base de decisiones, ya sea tomadas directamente, ya, con mas frecuencia, delegando dicha autoridad.

además se vigila simultáneamente que se cumplan en la forma adecuada todas las ordenes emitidas.

Hay dos estratos substancialmente distintos para obtener estos resultados:

1. En el nivel de ejecución (obreros, empleados y aun técnicos) se trata de "hacer", "ejecutar", "llevar a cabo" aquellas acciones que habrán de ser productivas.

2. En el nivel administrativo, o sea, el de todo aquel que es jefe, y precisamente en cuanto lo es, se trata de "dirigir", no de "ejecutar". El jefe, en cuanto tal, no ejecuta, sino hace que otros ejecuten.

CONTROL

Es la medición de los resultados actuales y pasados, en relación con los esperados, ya sea total o parcialmente, con el fin de corregir, mejorar y formular nuevos planes. El control se divide en las siguientes etapas:

- Establecimiento de los medios de control
- Operaciones de recolección y concentración de datos
- Interpretación y valoración de los resultados
- Utilización de los mismos resultados

IV.3 CUESTIONARIO DE CONTROL INTERNO

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

		NOMBRE	FECHA	FIRMA
	PREPARO			
EMPRESA:	REVISO			

		ESTIM	REAL	DIF
TIEMPO				

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
1	COMITE					
11	Se tiene establecido un comité u órgano interno de informática					
	está integrado el comité por todas las áreas de la organización					
111	Se tienen establecidas actividades y funciones del comité u órgano					
112	Se cuenta con una calendarización de reuniones					
113	Se documentan las decisiones a las que llega en las reuniones					
114	Se cuenta con criterios para la elección de miembros del comité					
115	Se tienen documentadas las actividades del comité					
116	Se tienen documentadas las funciones del comité					
117	Se tienen documentadas las obligaciones del comité					
118	Se tienen documentadas las responsabilidades del comité					
2	PREVISION					
21	Previsiones					
211	Se cuenta con un análisis de certeza para determinar los riesgos de la organización para el logro de los objetivos					
212	Se cuenta con un análisis de incertidumbre para determinar los riesgos de la organización para el logro de los objetivos					
213	Se cuenta con un análisis de probabilidad para determinar los riesgos de la organización para el logro de los objetivos					
214	Se consideran hechos anteriores ocurridos en la empresa y/o en otras empresas					
215	Se determinan los posibles factores negativos para el logro de objetivos en bases estadísticas y cálculo de probabilidades					
216	Las previsiones se basan en hechos sin considerar opiniones subjetivas					
217	Se analizan las previsiones en forma cuantitativa o susceptibles de medirse					
218	Se analizan las previsiones en forma cuantitativa o susceptibles de medirse					
22	Objetivos					
221	Se cuenta con una clasificación y jerarquización de objetivos					
222	Se cuenta con objetivos individuales y colectivos					
223	Se cuenta con objetivos generales y particulares					
224	Se cuenta con objetivos básicos secundarios y estratégicos					
225	Se determinan los objetivos a corto y largo plazo					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

		ESTIM.	REAL.	DIF.		- NOMBRE -	FECHA	- FIRMA -
EMPRESA:	TIEMPO				PREPARO			
					REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
226	Los objetivos son estructurados subjetivos o ambiguos					
227	Se cuenta con un área y/o persona responsable de fijar objetivos					
228	Se cuenta con reglas para fijar objetivos					
229	Se procura contar con opiniones de diversas personas para fijar objetivos					
2210	Los objetivos se fijan por escrito en los casos de mayor importancia					
2211	Los objetivos son perfectamente conocidos y aceptados por todos los que hayan ayudado a realizarlos					
2212	Los objetivos son estables					
23	Investigaciones					
231	Se realizan investigaciones para determinar los medios más aptos para lograr el objetivo fijado					
232	Se cuenta con un estudio que analice y contemple los posibles riesgos que pueden afectar el proceso electrónico de datos en la organización					
233	Existe un plan de contingencias elaborado en base al estudio realizado de los posibles riesgos tales como: a) Incendio					
234	b) Inundación					
235	c) Sismo					
236	d) Destrucción de información					
237	e) Robo					
238	f) Vandalismo					
239	El plan de contingencias contiene actividades y funciones de cada persona que forma parte del área especificando responsabilidades y obligaciones de las mismas					
2310	Existe hadica de difusión para el plan de contingencias					
2311	Existe una calendarización de pruebas que aseguren el óptimo funcionamiento de plan establecido					
2312	Se realizan revisiones y actualizaciones periódicas al plan de contingencias					
2313	Se cuenta con un análisis de los factores positivos y negativos que habrán de influir en logro de objetivos					
2314	Se cuenta con una clasificación de los factores positivos y negativos que habrán de influir en el logro de objetivos					
2315	En las investigaciones se identifican los factores internos y externos a la organización					
2316	Se identifican los factores no disponibles determinando en donde y como encontrarlos					
2317	De los factores no disponibles se establecen factores estratégicos					
2318	Se cuenta con técnicas para manejar las investigaciones					
2319	Se tiene establecida la técnica de observación a través de registros contables estadísticos y administrativos para la realización de investigaciones					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

	ESTIM	REAL	DIF
TIEMPO			

EMPRESA:

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
24	Cursos de Acción					
241	Se cuenta con una evaluación de los cursos de acción para lograr la asignación de los medios a fin					
242	Los cursos de acción consideran los factores positivos y negativos considerados en las investigaciones					
243	Se definen los diversos cursos de acción para lograr los objetivos					
244	Se consideran las investigaciones para la definición y la decisión de curso de acción a seguir					
245	Para evaluar los cursos de acción que se presentan se usan criterios tales como: El riesgo externo, minimización de esfuerzos, duración del tiempo y la limitación de recursos con que puede contarse sobre todo los de tipo humano					
246	Se tienen estudios técnicos sobre cursos alternativos de acción					
247	Se utilizan técnicas de carácter administrativo en los cursos de acción					
248	Se utilizan técnicas de carácter matemático en los cursos de acción					
249	Se realiza un análisis de costo-beneficio por cada uno de los posibles cursos de acción					
3	PLANEACION					
31	Pronósticos					
311	Se utiliza información interna y externa para fines de la formulación de pronósticos					
312	Se tiene la información con respecto a la forma en que se formula el pronóstico					
313	Considera el pronóstico información tecnológica, económica y financiera					
314	El pronóstico incorpora cuando menos un juicio de correlación					
315	Se consideran criterios para lograr la mayor exactitud en los pronósticos					
316	Se utilizan métodos para la utilización de pronósticos					
317	Se consideran todas las variables para lograr la mayor exactitud en el logro de los pronósticos					
32	Planes					
321	Se utilizan técnicas para formular planes					
322	Existen planes para cada función de área o áreas de cómputo					
323	Se coordinan e integran las diversas áreas de la organización para elaborar los planes					
324	Contribuyen los planes y los que de ellos se derivan a la consecución de objetivos					
325	Los planes se formulan para un determinado tiempo					
326	Están actualizados los planes con el tiempo suficiente para cumplir con los compromisos					
33	Políticas					
331	Existen políticas generales de área					
332	Existen políticas particulares del área					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

		ESTIM	REAL	DIF
EMPRESA:	TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
333	Son revisadas periódicamente las políticas					
334	Las políticas se difunden					
335	Los medios utilizados para la difusión de las políticas son adecuados					
336	Están concentradas y documentadas las políticas existentes en la organización					
337	Se consideran criterios para el establecimiento de políticas					
338	Se realiza una supervisión para verificar el cumplimiento de las políticas					
339	Las políticas fijadas guían las decisiones administrativas para el logro de los objetivos					
340	Las políticas fueron fijadas en forma sencilla y clara					
341	Las políticas están redactadas por escrito y forman parte del manual de organización					
342	Las políticas se fundamentan en cada nivel					
34	Programas					
341	Existen programas generales de área					
342	Existen programas particulares de área					
343	Los programas se presentan a la autoridad superior de la organización para su aprobación					
344	Se fija el costo y los beneficios que implican de producir					
345	Se estudia el momento más oportuno para iniciar la operación de un programa nuevo					
345	Se determina la cantidad de recursos materiales, humanos y técnicos hacen de conjugarse de acuerdo a lo presupuesto					
347	Se señala como, cuando y donde se van a aplicar los recursos en forma específica					
348	Los programas guardan cierta amplitud de desarrollo de las actividades a realizar					
349	Los programas incluyen una descripción adecuada y precisa de las actividades que habrán de realizarse acompañadas con las fechas de iniciación y terminación, lugar y tiempo					
340	Los programas a largo plazo comprenden programas menores e asociados con mayor detalle					
341	Los programas ejecutivos permiten la elaboración de programa o plan financiero					
35	Procedimientos					
351	Existen procedimientos generales de área					
352	Existen procedimientos particulares de área					
353	Los procedimientos se fijan por escrito y forman parte de manual de procedimientos					
354	Están representados gráficamente					
355	Los procedimientos son revisados periódicamente					
356	Las fases contenidas en los procedimientos prescriben su ejecución dentro de una secuencia lógica					
357	Proporcionan los medios para una coordinación eficaz entre las diversas áreas de la organización					
358	Los procedimientos señalan de manera clara y precisa todas las funciones necesarias para la operación					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

		NOMBRE	FECHA	FIRMA
		ESTIM.	REAL	DIF.	PREPARO			
EMPRESA:	TIEMPO				REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
4	ORGANIZACION					
41	Funciones					
411	Se cuenta con un manual de organización					
412	Se cuenta con un manual de procedimientos					
413	Se consideran los objetivos y planes para fijar las funciones de cada puesto					
414	Están definidas las funciones que cada persona debe de realizar					
415	Se tienen fijadas funciones primarias y secundarias considerando que se favorezca la eficiencia					
416	Se tiene un control sobre el cumplimiento de las funciones					
417	Se consideran los posibles factores negativos que pudieran intervenir en el cumplimiento de las funciones					
418	El análisis de las funciones está basado en consideraciones específicas para su elaboración					
419	Se toma en cuenta información sobre funciones ya definidas en empresas similares, revistas y manuales de organización					
42	Jerarquías					
421	Existe un organigrama completo y actualizado que señale la jerarquía de cada puesto					
422	Existe un organigrama actualizado que señale la jerarquía de cada puesto					
423	Se determina el grado de autoridad que existe en cada línea del organigrama					
424	Se determina que personas serán las que ocupen un cierto nivel jerárquico					
425	Existen criterios para la delegación de funciones que tiene cada nivel jerárquico					
426	Existe un control de que cada nivel jerárquico tenga una delegación de funciones suficiente					
427	Se tiene determinado el tramo de control de cada nivel de organigrama					
428	Se considera el número de personas que dependerán a cada nivel					
429	Se evalúa el número de personas que reportarán a cada nivel					
43	Obligaciones					
431	Cada puesto tiene asignadas obligaciones específicas					
432	Se determinan las obligaciones de cada puesto					
433	Se cuenta con una descripción específica de puesto dentro de los manuales de organización que permita considerar las obligaciones					
434	El puesto cuenta con un perfil que permita cumplir con las obligaciones asignadas a él					
435	Se consideran todas las labores para determinar las obligaciones					
436	Se supervisan las obligaciones de cada individuo					
437	Se revisa que se cumplan las obligaciones					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

						NOMBRE	FECHA	FIRMA
		ESTIM	REAL	DIF	PREPARO			
EMPRESA:	TIEMPO				REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
5	INTEGRACION					
51	Selección					
511	Se cuenta con perfiles establecidos para seleccionar a personal de área					
512	Se seleccona a las personas que cumplan con los requisitos mínimos para desempeñar una función					
513	Se tienen límites superiores e inferiores en las condiciones que se solicitan para un puesto					
514	Existen criterios que determinan las condiciones para seleccionar al personal					
515	Se utilizan medios de selección de personal					
516	Se utilizan fuentes de abastecimiento de personal					
517	Se realizan evaluaciones psicológicas y técnicas a las personas seleccionadas					
518	Se cuenta con un programa de inducción					
52	Inducción					
521	Se supervisa la inducción de los individuos					
522	La inducción se realiza a todos los niveles					
523	Se actualiza el programa de inducción					
524	Se difunde el programa de inducción					
525	Se evalua el programa de inducción					
526	Se considera el momento oportuno para realizar la inducción					
527	Se tienen parámetros de tiempo para realizar la inducción					
53	Desarrollo					
531	Se considera a todos los individuos y niveles de la organización para el programa de desarrollo					
532	Se toman en cuenta las condiciones del individuo					
533	Se efectua desarrollo técnico y práctico					
534	Se practica el desarrollo personal de los individuos de la organización					
535	Se cuenta con políticas de crecimiento expansión y mejoramiento del personal dentro de la organización					
6	DIRECCION					
61	Autoridad					
611	Se tienen identificados los tipos de autoridad existentes en la organización					
612	Se tienen clasificados los tipos de autoridad existentes en la organización					
613	Se delega autoridad de acuerdo a niveles jerárquicos					
614	Se ejerce la autoridad en base a puestos y niveles jerárquicos					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

EMPRESA:

	EST/M	REAL	DIF		NOMBRE	FECHA	FIRMA
TIEMPO				PREPARO			
				REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
615	Se cuenta con políticas para ejercer la autoridad					
616	Existen canales de comunicación a través de los cuales se ejerce la autoridad					
617	Se supervisa el ejercicio de la autoridad					
618	Existe periodicidad para dicha supervisión					
619	Se tienen medios establecidos para transmitir una orden					
6110	Se consideran situaciones extraordinarias para ejercer la autoridad					
6111	Existe un equilibrio entre la autoridad y la responsabilidad					
62	Comunicación					
621	Se tiene un procedimiento definido de comunicación					
622	Se toman en cuenta criterios para desarrollar el procedimiento de comunicación					
623	El procedimiento de comunicación es difundido a todo el personal					
624	Se tiene un control del cumplimiento del proceso de comunicación					
625	Se definen las fuentes de comunicación existentes					
626	Se cuenta con medios y/o canales de comunicación					
627	Se tienen políticas que regulen el tamaño del canal de comunicación					
628	Existen políticas que regulen el contenido de la comunicación					
629	Existe un control del cumplimiento de las políticas de comunicación					
6210	La comunicación es bilateral					
63	Supervisión					
631	Se asignan personas que vayan a hacer la supervisión					
632	Existen políticas para incentivar a los supervisores					
633	Existen programas para capacitar a los supervisores					
634	Se toman en cuenta criterios específicos para capacitar a los supervisores					
635	Se cuenta con políticas para evaluar el trabajo de los supervisores					
636	Existen políticas para la ejecución del trabajo de los supervisores					
637	Se revisan controles del trabajo realizado por los supervisores					
638	Los supervisores realizan informes o reportes periodicamente					
7	CONTROL					
71	Establecimiento					
711	Se distinguen las operaciones del control de la función de control					
712	Existen estándares básicos para medir el control					
713	Se aplica el control en los casos en que no se sigue lo previsto					
714	Se tienen establecidos medios de control					
715	Al establecer los controles se considera la función que va a controlar para ejecutarse mas ob					
716	Se cuenta con una clasificación de las principales áreas de control					

CUESTIONARIO DE CONTROL INTERNO
REVISION ADMINISTRATIVA DEL CENTRO DE PROCESAMIENTO DE DATOS

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
7.2	Operación					
7.2.1	Se realizan operaciones de recolección y concentración de datos para el área de control					
7.2.2	Se analizan interpretan y verifican los resultados de la recolección de datos					
7.2.3	Los resultados obtenidos del análisis del control se utilizan para el futuro					
7.2.4	Se cuenta con medios de control estratégicos					
7.2.5	Los controles reportan oportunamente las desviaciones					
7.2.6	Los controles son claros y sencillos de entender					
7.2.7	Cuando por alguna razón los controles de alguna manera las acciones correctivas					
7.2.8	En la utilización de los datos de control debe seguirse una pauta					
7.2.9	Se cuenta con una planificación de control es sobre cada unidad operativa del área					
7.3	Interpretación					
7.3.1	Los sistemas de control rinden en todo lo posible a la estructura de la organización					
	Se concentran los controles lo más que sea posible para las áreas clave administrativas interpretando					
7.3.2	Los resultados en forma sencilla y clara					

IV.4. DEFINICION DE PROCEDIMIENTOS DE AUDITORIA ADMINISTRATIVA

1. COMITE

PROC.1.1 Conocer la fecha de creación del comité; así como el nombre y puesto de los integrantes del mismo.

PROC.1.2 Conocer y analizar los criterios o bases utilizados para la elección de miembros del comité u órgano interno de informática.

PROC.1.3 Solicitar y verificar los documentos existentes para la difusión de actividades, funciones, obligaciones y responsabilidades del comité.

PROC.1.4 Entrevistar a algunos miembros del comité. Verificando las fechas establecidas para reuniones; y determinando el grado de conocimiento de las actividades, funciones y responsabilidades que tiene como miembros del comité y órgano.

2. PREVISION

PROC.2.1 Determinar si existe un estudio global que evalúe los riesgos y vulnerabilidades del procesamiento de datos ante cualquier contingencia, que permita formular un plan de recuperación en contra de desastres.

PROC.2.2 Verificar que ante posibles desastres este plan determina las actividades a realizar.

PROC.2.3 Conocer la planeación y calendarización de pruebas al plan, verificando los resultados.

PROC.2.4 Entrevistar al responsable del área de informática con la finalidad de conocer si existen otros planes de recuperación dentro de la organización. Y determinar que el plan del área de informática sea homogéneo con los demás existentes.

PROC.2.5 Conocer y evaluar el método y los medios utilizados para determinar, actualizar y difundir los objetivos dentro de la organización.

PROC.2.6 Verificar que exista coordinación y supervisión en el proceso de elaboración y distribución de dichos objetivos.

PROC.2.7 Analizar los medios utilizados para realizar investigaciones que ayudan a identificar factores positivos y negativos dentro de la organización, verificando que cuenten con la posibilidad de ser interpretados en forma cualitativa y cuantitativa de cada uno de ellos.

PROC.2.8 Verificar que los cursos de acción se hayan establecido de acuerdo a las investigaciones realizadas; y que en cada uno de los cursos definidos, presente las ventajas y desventajas que se pueden obtener en caso de que sean utilizados.

3. PLANEACION

PROC.3.1 Conocer y analizar las fuentes de información utilizadas para elaborar los pronósticos técnicos, económicos y financieros, determinando su utilidad, actualización y exactitud.

PROC.3.2 Evaluar las técnicas utilizadas para formular planes, verificando que exista interacción, coordinación, supervisión y control en su elaboración y cumplimiento.

PROC.3.3 Identificar las políticas implantadas, analizando su actualización, difusión, claridad, jerarquización y cumplimiento, de acuerdo a la documentación general y/o particular de cada una de las políticas existentes en cada departamento, área y sección.

PROC.3.4 Conocer los elementos utilizados para la realización de programas verificando que sean autorizados, que contengan los recursos a utilizar, el tiempo de realización y el costo-beneficio al que se pretende llegar con cada uno de ellos.

PROC.3.5 Realizar un análisis de los procedimientos existentes, respecto a su forma de elaboración, los medios utilizados para su difusión, claridad y sencillez en su control para su cumplimiento.

4. ORGANIZACION

PROC.4.1 Verificar que los manuales de Organización y Procedimientos incluyan a el área de Informática.

PROC.4.2 Revisar que la definición de funciones actividades y jerarquías cumpla con los objetivos para los que fueron establecidos.

PROC.4.3 Verificar que existan especificaciones de funciones y actividades, asegurándose de que se tomaron en cuenta alternativas de solución de acuerdo a las contingencias que se pudieran presentar.

PROC.4.4 Verificar que exista una apropiada separación de actividades para determinar que no haya duplicidad.

PROC.4.5 Determinar los medios que se utilizan para difundir las jerarquías y autoridad de cada puesto señalado en el organigrama.

PROC.4.6 Entrevistar a algunas personas del área de Informática para asegurarse que sus actividades concuerdan con las establecidas y publicadas en los manuales.

5. INTEGRACION

PROC.5.1 Revisar que existan perfiles actualizados. Establecidos para garantizar que el individuo cumpla con los requisitos mínimos establecidos para desempeñar un puesto.

PROC.5.2 Estudiar las posibilidades de desarrollo que se ofrecen en la organización, así como, los niveles en que esta se da. Y conocer las personas que están informadas de estas posibilidades.

6. DIRECCION

PROC.6.1 Determinar la existencia de Autoridad en la Organización, identificando su clasificación y distribución, verificando su cumplimento en todos los puestos y niveles jerárquicos, de acuerdo a las políticas fijadas para este fin.

PROC.6.2 Identificar los canales de comunicación verificando que exista coordinación, integración y control para ejercer la autoridad en situaciones normales y extraordinarias; así como la definición de responsabilidades y obligaciones de cada una de las personas responsables de su ejecución.

PROC.6.3 Conocer los criterios utilizados para la elaboración del proceso de comunicación, determinando si estos ayudan a fijar medios de difusión, políticas, controles. Además, proporcionar confiabilidad en la información y/o aspectos que se comunican en la organización.

PROC.6.4 Entrevistar a las personas asignadas para realizar la supervisión con el objeto de conocer las políticas y controles existentes para su ejecución. Así como, la capacitación recibida por cada una de las personas.

PROC.6.5 Investigar y verificar los medios utilizados para registrar, reportar o informar las actividades realizadas, los resultados obtenidos y la periodicidad con que se realiza.

7. CONTROL

PROC.7.1 Conocer los criterios y bases para el establecimiento de controles, verificando que existan estándares para su implantación, actualización, difusión y supervisión.

PROC.7.2 Determinar si las actividades y funciones establecidas para la ejecución del control consideran una identificación, análisis y valoración de los resultados obtenidos.

PROC.7.3 Identificar los controles implantados verificando que se realice supervisión periódica de las actividades y funciones establecidas.

PROC.7.4 Verificar que la definición de políticas y procedimientos para la realización del control, estén documentadas y difundidas dentro de la organización.

PROC.7.5 Conocer los medios utilizados para llevar a cabo la interpretación de los resultados, verificando que su contenido y distribución se realicen a todos los niveles de la organización.

V. REVISION DE CONTROLES EN REDES

V.1. OBJETIVO DE LA REVISION.

Esta revisión abarca todos aquellos aspectos involucrados directamente con la instalación de redes en la organización; así como la de sus controles para el acceso a equipo, aplicaciones y sistemas en red. Principalmente tiene como puntos importantes los siguientes:

1. Equilibrio entre economía y factibilidad de proyectos de inversión para la solución a la problemática de automatización de operaciones en la organización.

2. Supervisión del cumplimiento de políticas y procedimientos de adquisición de bienes informáticos establecidos por la organización.

3. Implantar programas de Seguridad Física, que comprenda recursos humanos, materiales y económicos.

4. Existencia de controles sobre: ubicación de mobiliario y equipo, control de accesos, prevención contra fuego, humedad y otras condiciones adversas que pudieran presentarse.

5. Establecer sistemas de Respaldos para proyectos de desarrollo de software en red.

6. Establecer lineamientos para proteger la confiabilidad de información en redes.

7. Establecer técnicas de identificación y autenticidad; otorgando a los usuarios identificación y password.

8. Establecer los principios de la asignación de derechos necesarios a cada usuario de la red.

9. Establecer principios de asignación de atributos a cada usuario, de acuerdo a actividades y funciones que realiza.

10. Establecimiento de un plan de recuperación en caso de desastres; con el cual la organización pueda continuar sus operaciones por medio de una serie de acciones coordinadas y planeadas.

V.2 ASPECTOS QUE ABARCA

ADQUISICIONES

En este aspecto a partir del análisis, la definición de requerimientos generales y particulares tanto de hardware y software dentro de la organización, se deberán explotar las diferentes alternativas de solución realizando un estudio de factibilidad que comprende los siguientes elementos:

Factibilidad Económica. Involucra todos los costos asociados a la adquisición considerando no solo el desembolso inicial, sino, los costos por entrenamiento del personal y mantenimiento de hardware y software.

Factibilidad Operativa. Orientado a evaluar si el equipo tendrá la capacidad de procesar la información con posibilidades de crecimiento, además de los recursos humanos con los que se cuenta.

Factibilidad Tecnológica. Se realiza sobre las posibles restricciones que impidan aprovechar íntegramente la inversión y el equipo inicialmente contratado.

SEGURIDAD FISICA

La información y los recursos informáticos son activos que deben ser protegidos del acceso no autorizado, la manipulación y destrucción. Por ello la seguridad física debe establecerse para prevenir accesos innecesarios y/o no autorizados a las áreas de informática, detectando intentos de acceso no autorizados.

La auditoría a la seguridad física se refiere a la revisión de las medidas de control , orientadas a la continuidad del servicio, en gran parte considerando los siguientes casos:

Fenómenos naturales. Como incendio, terremoto, huracanes, tormentas, inundaciones, fallas de corriente, picos de voltaje, fallas de aire acondicionado y cortos circuitos.

Fenómenos intencionales. Que pueden ser por parte de ex-empleados, empleados notificados de desempleo, huelguistas, empleados con problemas económicos o descontentos.

SEGURIDAD LOGICA

Día a día los recursos informáticos: equipo, programas y datos, son compartidos por un gran número de personas, físicamente dispersas, lo cual, hace necesario implantar controles que garanticen que el acceso a ellos se realiza de acuerdo a nivel jerárquico y funciones del personal protegiendo a la organización de:

- Destrucción accidental o intencional del equipo
- Destrucción, copiado o eliminación accidental o intencional de información
- Mal uso del equipo
- Mal uso de la información

PLAN DE CONTINGENCIAS

Los desastres pueden ser naturales, humanos y materiales, normalmente se piensa en los fenómenos naturales, pero no en las contingencias que se pueden presentar todos los días, como: fugas de agua, o fugas de gas.

Un plan de contingencias es la habilidad que tiene una organización para continuar sus operaciones diarias a pesar de que ocurra un desastre. El gerente de informática debe ser el líder del plan, pero debe involucrarse seriamente el director de finanzas.

El plan de contingencias y recuperación debe detallar los procedimientos para emigrar a una situación de emergencia en el menor tiempo posible y con el menor grado de riesgo, así como poder regresar a la operación normal de la misma forma, considerando los siguientes puntos:

a) Inventario de sistemas y equipo

b) Realizar un estudio y análisis de todos los conflictos legales y laborales considerándolos como riesgos potenciales.

c) Establecer procedimientos de acciones a realizar

d) Lista de personas que deben ejecutar el plan

e) Clasificar los recursos informáticos de acuerdo a prioridades

f) Procedimientos de seguridad que deberán tenerse en cuenta al trasladar los recursos informáticos a otro sitio

g) Procedimientos de respaldo y recuperación de información

V.3 CUESTIONARIO DE CONTROL INTERNO

CUESTIONARIO DE CONTROL INTERNO
REVISION DE CONTROLES EN REDES

EMPRESA:

	ESTIM.	REAL	DIF.
TIEMPO			

	NOMBRE:	FECHA	FIRMA:
PREPARO			
REVISO:			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
1	ADQUISICIONES					
1.1	Adquisicion de Hardware					
1.1.1	Existe normatividad para regular la adquisición de hardware					
1.1.2	La normatividad para el hardware es homogénea en toda la organización					
1.1.3	Existen políticas generales y particulares para la adquisición de hardware					
1.1.4	Existe una área responsable de la adquisición de hardware					
1.1.5	Existe un responsable de las adquisiciones de hardware.					
1.1.6	Para la adquisición de hardware se realiza un estudio de factibilidad					
1.1.7	Para la adquisición de hardware se lleva a un estudio técnico					
1.1.8	Para la adquisición de hardware se lleva a un estudio contable					
1.1.9	Para la adquisición de hardware se realiza un estudio económico					
1.1.10	Existe documentación de la realización del estudio de factibilidad de la compra de hardware					
1.1.11	Se aplica una evaluación para estudios de factibilidad técnica					
1.1.12	Se aplica una evaluación para estudios de factibilidad operativa					
1.1.13	Se consideran los criterios y/o políticas de adquisición establecidos por el comité de informática					
1.1.14	Existe una especificación para la adquisición e instalación de hardware					
1.1.15	Se difunde la especificación de adquisición e instalación de hardware					
1.1.16	Se cuenta con políticas y procedimientos para la elaboración de contratos en la adquisición de					
1.1.17	El abogado de la organización analiza y evalua los contratos de adquisición de bienes informáticos para dar su opinión al respecto					
1.1.18	Las cláusulas del contrato serán en el siguientes de proveedor					
1.1.19	Se toman en cuenta las condiciones del proveedor para dar mantenimiento a hardware					
1.1.20	Se realizan cotizaciones para elegir la mejor alternativa en la compra de hardware					
1.1.21	Las cotizaciones incluyen especificaciones técnicas y cláusulas					
1.1.22	Se realiza una evaluación de hardware y se realizan pruebas de aceptación					
1.1.23	Los resultados de las pruebas son registrados para elegir la mejor opción					
1.1.24	Se establece para el uso de hardware la capacitación requerida y ofrecida por el proveedor					
1.1.25	Se tienen claramente especificados los requisitos de autorización para la adquisición de hardware					
1.1.26	Se realiza un seguimiento de los resultados que se obtienen al utilizar nuevas adquisiciones de					
1.1.27	Se documentan los resultados obtenidos en uso de nuevas adquisiciones de hardware					
1.1.28	Se analizan los resultados obtenidos en uso de nuevas adquisiciones de hardware					
1.1.29	Se definen prioridades de adquisición de hardware					
1.2	Adquisición de Software					
1.2.1	Existe normatividad para regular la adquisición de software					
1.2.2	La normatividad para el software es homogénea en toda la organización					
1.2.3	Existen políticas generales y particulares para la adquisición de software					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE CONTROLES EN REDES

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
124	Existe un área responsable de la adquisición de software					
125	Existe un responsable de las adquisiciones de software					
126	Para la adquisición de software se realiza un estudio de factibilidad					
127	Para la adquisición de software se realiza un estudio técnico					
128	Para la adquisición de software se realiza un estudio operativo					
129	Para la adquisición de software se realiza un estudio económico					
1210	Existe documentación de la realización del estudio de factibilidad de la compra de software					
1211	Se aplica una evaluación para estudios de factibilidad técnica					
1212	Se aplica una evaluación para estudios de factibilidad operativa					
1213	Se consideran los criterios y/o normas de adquisición establecidos por el comité de informática					
1214	Existe una estandarización para la adquisición e instalación de software					
1215	Se difunde la estandarización de adquisición e instalación de software					
1216	Se cuenta con políticas y procedimientos para la elaboración de contratos en la adquisición de software					
1217	El abogado de la organización analiza y revisa los contratos de adquisición de bienes informáticos para dar su opinión al respecto					
1218	Las cláusulas del contrato señalan obligaciones del proveedor					
1219	Se toman en cuenta las condiciones del proveedor para dar mantenimiento a software					
1220	Se realizan cotizaciones para elegir la mejor alternativa en la compra de software					
1221	Las cotizaciones incluyen especificaciones técnicas y operativas					
1222	Se realiza una evaluación de software y se realizan pruebas de aceptación					
1223	Los resultados de las pruebas son registrados señalando la mejor opción					
1224	Se establece para el uso de software la capacitación requerida y ofrecida por el proveedor					
1225	Se tienen claramente especificados los requisitos de autorización para la adquisición de software					
1226	Se realiza un seguimiento de los resultados que se obtienen al utilizar nuevas adquisiciones de software					
1227	Se documentan los resultados obtenidos del uso de nuevas adquisiciones de software					
1228	Se analizan los resultados obtenidos del uso de nuevas adquisiciones de software					
1229	Se definen prioridades de adquisición de software					
3	SEGURIDAD LOGICA					
31	Acceso a información					
311	Existe un responsable de control de acceso a la información					
312	Se cuenta con criterios para la elección del responsable del control de acceso a la información					
313	Se cuenta con procedimientos para la instalación de información					
314	El responsable del control de acceso cuenta con autoridad para autorizar a los usuarios de la					
315	Se cuenta con políticas para la seguridad de la información					
316	Las políticas están redactadas de manera clara y fácil de entender					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE CONTROLES EN REDES

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
217	Se conocen dentro de las políticas sanciones por violación de la seguridad de la información					
218	Se difunden las políticas a todos y cada uno de los usuarios de la información					
219	Se conocen accesos legales a seguir en caso de violación en la manipulación de la información					
210	Existe software instalado que asegure que no haya modificaciones de información no autorizados					
211	Se cuenta con una detección de accesos no autorizados a la información					
212	Se cuenta con controles de los accesos a información no autorizados					
213	Se actualizan los controles de accesos no autorizados					
214	Se analizan los controles de accesos no autorizados					
215	La seguridad de la información cubre todas las áreas de proceso, bases de datos y sistemas					
216	Se cuenta con políticas específicas para las áreas de información de alto riesgo					
217	Se cuenta con procedimientos para destrucción de información contenida en papel, cintas, pape					
218	Se identifican todas las áreas de alto riesgo					
22	Acceso a Programas					
221	Existe una separación de las librerías de los programas					
222	Se tienen contempladas las restricciones de acceso a programas y librerías					
223	Existen políticas para realizar cambios en las librerías y programas					
224	Se tiene un control de las modificaciones que se realizan en librerías y programas					
225	Se analiza el control de las modificaciones que se realizan en librerías y programas					
226	Se actualiza el control de las modificaciones que se realizan en librerías y programas					
227	Existe protección para prevenir copias no autorizadas de librerías y programas					
228	Se realiza una depuración de las librerías y programas					
229	Se cuenta con un procedimiento para el rescate de librerías y programas					
2210	Se tiene asignado un responsable de el rescate de librerías y programas					
23	Procesamiento de Datos					
231	Existen políticas y procedimientos para el procesamiento de datos					
232	Se tiene contemplado dentro de las políticas procedimientos de emergencia para cuando ocurren					
233	Existen procedimientos para realizar procesamiento de emergencia cuando se presentan condiciones de error					
234	Se cuenta con registros de monitoreo de todos los procedimientos					
235	Se investigan procesamientos inusuales					
236	Existen controles que aseguren que todas las personas autorizadas realizan procesamientos					
237	Existen controles para asegurar que todos se utilizan los archivos de datos necesarios para el procesamiento					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE CONTROLES EN REDES

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
1	SEGURIDAD FISICA					
1.1	Existen políticas para el acceso a las áreas de cómputo					
1.2	Se cuenta con medidas de seguridad que restrinjan el acceso a las áreas de cómputo					
1.3	Los lugares donde se ubican las computadoras garantizan que solo tengan acceso las personas autorizadas					
1.4	Se cuenta con extinguidores y detectores que protejan el equipo					
1.5	Se tiene un control de la temperatura y humedad del lugar					
1.6	Se evaluaron los riesgos potenciales de área donde se ubica el centro de cómputo					
1.7	a) Aeropuertos					
1.8	b) Plantas químicas					
1.9	c) Almacenes y otras estructuras susceptibles a fuego					
1.10	d) Lugares que pudieran ser causa de inundación					
1.11	Se cuenta con candados llaves y cerraduras que limiten el acceso a el área de cómputo					
1.12	Se cambian periódicamente candados llaves y cerraduras					
1.13	Existen registros de las personas autorizadas para acceder a el área de cómputo					
1.14	Se actua con periodicidad en los registros para evitar el acceso de personas no autorizadas					
1.15	Se cuenta con un procedimiento para el acceso y control de visitantes del área de cómputo					
1.16	En las políticas se contemplan que cuando existe un ex-empleado de inmediato se restringa su acceso y se cambien sus llaves y claves					
1.17	Se cuenta con un sistema que detecte la salida no autorizada de equipo					
1.18	Existen procedimientos para proteger el equipo de riesgos potenciales como fuego e inundaciones					
1.19	Existen políticas que regulen la estancia en las áreas de cómputo					
1.20	Los procedimientos y políticas de el área son difundidos entre todos los usuarios					
1.21	Se cuenta con equipo contra incendio					
1.22	Se revisa periodicamente que el equipo contra incendios se encuentre en perfecto estado					
1.23	La habitación en la cual se encuentran las computadoras está construida con materiales que eviten el mayor riesgo de incendios					
1.24	Se cuenta con un seguro que cubra el equipo de cómputo de los riesgos potenciales					
1.25	Existe un plan de recuperación en caso de desastre					
1.26	Se realizan pruebas periodicas del plan de recuperación en caso de desastre					
1.27	Todas las personas conocen el plan de recuperación					
1.28	Se designó un grupo de personas para llevar a cabo el plan de recuperación en caso de desastres					
1.29	Se cuenta con un lugar seguro para el almacenamiento de respaldos y documentación					
1.30	Existe un inventario actualizado de equipo					
1.31	Se tienen procedimientos para el respaldo del equipo en caso de falla					
1.32	Se cuenta con un contrato de mantenimiento preventivo y correctivo que garantice la integridad del					
1.33	Se supervisa que se realicen las reparaciones de manera adecuada					
1.34	Se lleva un control de las reparaciones realizadas					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE CONTROLES EN REDES

EMPRESA:

	ESTIM.	REAL	DIF.
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT.	SI	NO	N/A	OBSERVACIONES
4	PLAN DE CONTINGENCIAS					
4.1	Se cuenta con un plan de contingencias					
4.2	El plan de contingencias está actualizado					
4.3	El plan cuenta con una lista de personal responsable de ejecutar el plan					
4.4	Se tienen establecidas prioridades para el procesamiento electrónico de datos en caso de desastres					
4.5	Se dispone de un sitio para llevar a cabo un proceso de información alternativo					
4.6	Se prueban los procedimientos del procesamiento electrónico de datos en el lugar alternativo					
4.7	Está bien establecido un calendario de pruebas					
4.8	Se analizan los resultados obtenidos en las pruebas					
4.9	Se documentan los resultados obtenidos					
4.10	Se cuenta con un inventario de equipo y software completo y actualizado					
4.11	Se realiza la documentación para las aplicaciones importantes					
4.12	Se guarda la documentación en un sitio adecuado					
4.13	Se realizan respaldos periódicos determinando prioridades de información					
4.14	Se guardan los respaldos en un sitio adecuado					
4.15	El plan de contingencias considera fenómenos naturales					
4.16	Se consideran posibles casos de errores humanos accidentales o voluntarios					
4.17	Se analizan todos los conflictos legales y laborales considerados como potenciales riesgos					
4.18	Falta de elaboración de lista de ayudas de documentación modelo y se prepara un plan preliminar					
4.19	El plan incluye procedimientos detallados que contengan avisos y acciones de los cuales los mas					
	Se asigna un director de contingencias y sus diferentes					
4.20	a) Centro cómputo de procesamiento de datos					
4.21	b) Proveedores					
4.22	c) Clientes					
4.23	d) Servicios de emergencia					
4.24	Se tienen establecidas rutas de transportación primaria y alterna en caso de evacuar a personal					
4.25	Se tienen definidos procedimientos para activar el equipo de cómputo en caso de amenaza de bomba					
4.26	Se establecen mecanismos de notificación y control de actividades					
4.27	Se definen operaciones a procesar en el centro de datos					
4.28	Se cuenta con prioridades de operación de sistemas					
4.29	Se tienen definidos procedimientos para recuperación de líneas telefónicas					
4.30	Se tienen definidos procedimientos para la restauración de los servicios de procesamiento electrónico de					
4.31	Se realiza una actualización y revisión periódica de riesgos existentes					
4.32	Se cuenta con pólizas de contratos de seguros mantenimiento y respaldos					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE CONTROLES EN REDES

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
	Se cuenta con un comité de contingencias que evalúe cualquier cambio a realizarse a:					
4.33	a) Personal					
4.34	b) Instalaciones físicas y de soporte					
4.35	c) Equipo					
4.36	d) Teléfonos					
4.37	e) Usuarios					
4.38	f) Contratos de mantenimiento y respaldo					

V.4. DEFINICION DE PROCEDIMIENTOS DE AUDITORIA EN REDES

1. ADQUISICIONES

1.1 Hardware

PROC.1.1.1 Analizar y evaluar los procedimientos y políticas de adquisición de hardware; verificando su actualización, difusión, supervisión, control, y cumplimiento.

PROC.1.1.2 Verificar el cumplimiento de los criterios establecidos para la adquisición de hardware.

PROC.1.1.3 Verificar la elaboración de estudios de factibilidad que contemple los aspectos técnico, operativo y económico, así como, la evaluación y documentación de los resultados obtenidos, para la adquisición de hardware.

PROC.1.1.4 Identificar la periodicidad de la elaboración de planes de adquisiciones. Verificando que se elaboren en base al análisis realizado de los resultados del uso de las nuevas adquisiciones de hardware.

PROC.1.1.5 Determinar si la elaboración y/o modificación a planes de adquisición e instalación de hardware se hacen tomando como referencia los estudios de factibilidad realizados.

PROC.1.1.6 Verificar que se considere el presupuesto y las condiciones financieras de la organización para la elaboración del plan de adquisiciones de hardware.

PROC.1.1.7 Verificar y analizar las prioridades establecidas identificando los requerimientos y justificación de dichas prioridades para la adquisición de software.

PROC.1.1.8 Conocer y verificar los procedimientos y políticas existentes para la selección de posibles proveedores, encargados de la venta y/o distribución de hardware.

PROC.1.1.9 Investigar si los proveedores seleccionados realizan demostraciones y pruebas a la organización del hardware a adquirir.

PROC.1.1.10 Verificar y analizar los procedimientos establecidos para evaluar, documentar y difundir los resultados obtenidos del uso de las nuevas adquisiciones de hardware.

PROC.1.1.11 Conocer y verificar los contratos celebrados con proveedores de hardware, identificando el visto bueno del área jurídica de la organización.

1.2 Software

PROC.1.2.1 Analizar y evaluar los procedimientos y políticas de adquisición de software; verificando su actualización, difusión, supervisión, control, y cumplimento.

PROC.1.2.2 Verificar el cumplimiento de los criterios establecidos para la adquisición de software.

PROC.1.2.3 Verificar la elaboración de estudios de factibilidad que contemplen los aspectos técnico, operativo y económico, así como, la evaluación y documentación de los resultados obtenidos, para la adquisición de software.

PROC.1.2.4 Identificar la periodicidad de la elaboración de planes de adquisiciones. Verificando que se elaboren en base al análisis realizado de los resultados del uso de las nuevas adquisiciones de hardware.

PROC.1.2.5 Determinar si la elaboración y/o modificación a planes de adquisición e instalación de software se hacen tomando como referencia los estudios de factibilidad realizados.

PROC.1.2.6 Verificar que se considere el presupuesto y las condiciones financieras de la organización para la elaboración del plan de adquisiciones de software.

PROC.1.2.7 Verificar y analizar las prioridades establecidas identificando los requerimientos y justificación de dichas prioridades para la adquisición de software.

PROC.1.2.8 Conocer y verificar los procedimientos y políticas existentes para la selección de posibles proveedores, encargados de la venta y/o distribución de software.

PROC.1.2.9 Investigar si los proveedores seleccionados realizan demostraciones y pruebas a la organización del software a adquirir.

PROC.1.2.10 Verificar y analizar los procedimientos establecidos para evaluar, documentar y difundir los resultados obtenidos del uso de las nuevas adquisiciones de software.

PROC.1.2.11 Conocer y verificar los contratos celebrados con proveedores de software, identificando el visto bueno del área jurídica de la organización.

PROC.1.2.12 Identificar las características de las licencias de uso del software; verificando que hayan sido adquiridas con los mayores beneficios para la organización.

1.3 Mantenimiento

PROC.1.3.1 Identificar y verificar las condiciones de mantenimiento y actualización otorgadas por el proveedor a los productos adquiridos.

PROC.1.3.2 Identificar y analizar el contrato de mantenimiento de hardware, verificando las obligaciones y responsabilidades del proveedor, así como, el hardware que cubre dicho contrato.

1.4 Capacitación

PROC.1.4.1 Conocer y verificar la capacitación otorgada por el proveedor para asegurar la optima utilización y aprovechamiento del hardware y software adquirido.

PROC.1.4.2 Conocer y analizar programas de la capacitación requerida para la operación de el hardware y software adquirido, verificando que cuenten con una estimación de costos personal y tiempo de duración.

2. SEGURIDAD LOGICA

PROC.2.1 Identificar a la persona responsable de la integridad de la información, evaluando los criterios utilizados para su selección, así como, sus funciones, actividades y responsabilidades

PROC.2.2 Conocer y evaluar las políticas para la protección de la información, verificando la difusión y documentación de las políticas.

PROC.2.3 Entrevistar a los usuarios de la información para cerciorarse de el grado de entendimiento de las políticas y la periodicidad con que se actualizan.

PROC.2.4 Evaluar y conocer los medios con los que se cuenta para la protección de la información (software, password, etc.) así como, los controles existentes y el seguimiento que a cada uno de ellos se le da.

PROC.2.5 Identificar que aspectos considera la protección de la información. Determinando si se abarca con estos toda la información que existe en la organización.

3. SEGURIDAD FISICA

PROC.3.1 Identificar a la persona responsable la integridad de el equipo de cómputo, evaluando los criterios utilizados para su seleeción, así como, sus funciones, actividades y responsabilidades

PROC.3.2 Conocer y evaluar las políticas para la protección de equipo de cómputo, verificando la difusión y documentación de las mismas.

PROC.3.3 Entrevistar a los usuarios del equipo de cómputo para cerciorarse de el grado de entendimiento de las políticas y la periodicidad con que se actualizan.

PROC.3.4 Evaluar y conocer los medios con los que se cuenta para la protección de el equipo de cómputo como: instalaciones adecuadas, equipos contra incendios, restricciones del acceso al equipo como candados, llaves, claves de acceso, seguros, etc.; así como, los controles existentes, y el seguimiento que a cada uno de ellos se le da.

PROC.3.5 Identificar que aspectos considera la protección de equipo de cómputo. Determinando si se abarca con estos todo el equipo con que se cuenta en la organización y se consideran todos los posibles riesgos.

PROC.3.6 Entrevistar a algunas de las personas que trabajan en el área para determinar el grado de conocimiento de sus responsabilidades, en cuanto al manejo del equipo de cómputo.

PROC.3.7. Hacer un recorrido por todas las instalaciones para cerciorarse de la existencia de la seguridades que fueron establecidas. Así como de funcionamiento de las mismas.

4. PLAN DE CONTINGENCIAS

PROC.4.1 Conocer y analizar el plan de contingencias elaborado para la organización. Determinando su actualización y difusión.

PROC.4.2 Conocer y evaluar el análisis elaborado para la realización del plan de contingencias de la organización.

PROC.4.3 Identificar a las personas con responsabilidades en el plan de contingencias, verificando que conozcan las actividades y funciones que deben realizar, en caso de contingencia.

PROC.4.4 Entrevistar al personal responsable; verificando que las actividades, funciones y responsabilidades contenidas en el plan, sean claras y sencillas de comprender.

PROC.4.5 Verificar la realización de simulacros de los procedimientos establecidos en el plan, identificando si se realiza una evaluación del personal que los va a ejecutar.

PROC.4.6 Seleccionar varias aplicaciones importantes definidas en el plan. Verificando que cuenten con los requisitos de documentación y archivos de respaldo, señalados en el plan de contingencias.

PROC.4.7 Verificar que los respaldos de aplicaciones importantes para verificar que su almacenamiento sea en un lugar adecuado y seguro.

PROC.4.8 Conocer la calendarización de pruebas del plan de contingencias, en el lugar alterno de procesamiento electrónico de datos. Determinando la periodicidad con que se realizan.

PROC.4.9 Repasar la documentación existente de la ultima prueba del plan. Verificando que incluya un análisis de los resultados, así como, la elaboración de acciones correctivas.

PROC.4.10 En caso de contar con un sitio de proceso alternativo verificar:

- Que el proveedor del sitio proporcione las oportunidades suficientes para probar los procedimientos del procesamiento electrónico de datos de la organización.
- Que el lugar cuente con el equipo necesario y exista compatibilidad con hardware y configuraciones del software de la organización.
- Que se cuente con apoyos alternos de telecomunicaciones, para aplicaciones importantes.
- Que se tengan espacios físicos suficientes y el medio ambiente necesario para la operación del equipo y personal.

PROC.4.11 Conocer los compromisos obtenidos por el proveedor, respecto a entrega de equipo y/o software en caso de presentarse una contingencia en la organización.

PROC.4.12 Conocer los planes de emergencia elaborados por otras secciones y/o unidades operativas. Determinando su consistencia y homogeneidad con las áreas de departamentos de la organización.

VI. REVISION AL DESARROLLO DE SISTEMAS.

VI.1 OBJETIVO.

A través del tiempo la experiencia en las empresas indica que los resultados obtenidos del proceso de Desarrollo de Sistemas de Información. Son deficientes y costosos. La mayoría de las organizaciones destinan enormes recursos al desarrollo de sistemas o a la modificación de los mismos, por ello se debe seguir un enfoque estructurado para nuevos sistemas y mantenimiento de estos. Llevando a cabo, la combinación de técnicas efectivas para administración de proyectos, la participación activa del usuario y especialistas así como la utilización de una metodología estructurada, buscando que todo sistema de información tenga sus fases: Planeación, Análisis, Diseño, Codificación, Implantación y Mantenimiento sujetas a control durante el proceso del desarrollo de sistemas. Asegurando el cumplimiento de los siguientes objetivos:

1.Contar con una proporción adecuada entre costos y beneficios a obtener con el desarrollo de un sistema.

2.Sistemas integrales y económicos.

3.Comunicación eficiente entre usuarios y personal de procesamiento electrónico de datos.

4.Contratación de personal profesional en el área de informática.

5.Satisfacer y cumplir las necesidades de los usuarios.

6.Contar con pistas de auditoria en cada uno de los sistemas.

7.Establecer revisiones técnicas a detalle.

8.Contar con un programa de capacitación eficiente.

9.Crear y/o modificar documentación de los sistemas.

10.Estandarizar una metodología dentro de la organización para el desarrollo de sistemas.

11.Realizar pruebas a los sistemas desarrollados.

VI.2. ASPECTOS QUE ABARCA.

PLANEACION.

La planeación incluye todas las actividades que se requieren para la selección del equipo de análisis de sistemas, la asignación de proyectos adecuados, la estimación del tiempo que cada tarea requiere para su ejecución, y la programación del proyecto, de tal forma que las tareas se concluyan oportunamente. El control denota el uso de la retroalimentación para el seguimiento del proyecto e incluye comparar el plan del proyecto con lo realizado hasta el momento, así como tomar las acciones adecuadas para crear, modificar o eliminar actividades para que todas se concluyan a tiempo.

ANALISIS.

Para realizar un adecuado desarrollo de sistemas es necesario tener una especificación completa de los requerimientos del usuario final. El análisis de los requerimientos es plantear la asignación de software a nivel de sistema y el diseño de programas. Esto facilita especificar la función y comportamiento de los programas, indicar la interface con otros elementos del sistema, establecer las condiciones de diseño que debe cumplir el programa, permitir refinar la asignación de software y representar el dominio de la información y las funciones que pueden ser traducidas en datos, arquitectura y diseño.

DISEÑO.

El diseño es un proceso en el que se traducen los requerimientos en una representación gráfica del software. Inicialmente, la representación describe una visión del software que se acerca mucho al código fuente. El diseño del sistema se realiza en dos fases el diseño general que se refiere a la transformación de los requerimientos en datos y estructura del sistema y el diseño particular, que se enfoca hacia una presentación gráfica mas completa y detallada de algoritmos y estructuras de datos en el sistema.

CODIFICACION.

La codificación ayuda a lograr el objetivo de eficiencia, ya que también puede facilitar el ordenamiento apropiado de los datos, además los estos codificados pueden reducir espacio valioso de almacenamiento y memoria. Los tipos específicos de código permiten manejar a los datos de una manera particular y lograr los siguientes propósitos:

1. Clasificación de la información.
2. Ocultar información.
3. Revelar información.

IMPLANTACION.

La implantación es el proceso que asegura la operación del sistema y que permite al usuario obtener beneficios por su uso además de aprovechar la asignación de mayor capacidad del equipo de cómputo, lograr la capacitación de los usuarios, realizar la conversión del sistema anterior y evaluar el nuevo sistema.

Otro enfoque de la implantación es la elección de una estrategia para la las conversiones de los sistemas, así como estar involucrado en la evaluación del sistema, ponderar la situación y proponer un plan de conversión que sea apropiado para la organización.

MANTENIMIENTO.

El mantenimiento se realiza generalmente para mejorar un software existente, mas que para responder a una crisis o falla de sistema. Conforme cambian los requerimientos de los usuarios, el software y la documentación también deberían cambiar, como parte del trabajo de mantenimiento. Además los programas podrían volverse a codificar para mejorar su eficiencia sobre el programa original. El mantenimiento también se realiza para actualizar el software en respuesta a los cambios de la organización.

VI.3 CUESTIONARIO DE CONTROL INTERNO

CUESTIONARIO DE CONTROL INTERNO
REVISION DE DESARROLLO DE SISTEMAS.

		ESTIM	REAL	DIF
TIEMPO				

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

EMPRESA:

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
1	PLANEACION					
1.1	Durante la planeación se determinó el alcance del sistema					
1.2	El alcance del sistema está definido					
1.3	Se cuenta con planes y programas de trabajo para el desarrollo de sistemas					
1.4	Los planes para el desarrollo de sistemas son documentados y difundidos					
1.5	Los programas de trabajo para el desarrollo de sistemas son documentados					
1.6	Se realiza una estimación de recursos a utilizar para el desarrollo de sistemas					
1.7	Se cuenta con técnicas para el desarrollo de sistemas					
1.8	Se estiman los recursos humanos a utilizar para el desarrollo de sistemas					
1.9	Se estiman los recursos de hardware a utilizar para el desarrollo de sistemas					
1.10	Se estiman los recursos de software a utilizar para el desarrollo de sistemas					
1.11	Se cuenta con técnicas para medir la productividad de los sistemas desarrollados					
1.12	Se cuenta con técnicas para medir la calidad de los sistemas desarrollados					
1.13	Se cuenta con técnicas para analizar la función de los sistemas desarrollados					
1.14	Se cuenta con técnicas para evaluar el tamaño de los sistemas desarrollados					
1.15	Se utilizan modelos de estimación para la planeación de sistemas de información					
1.16	Se utilizan herramientas de estimación para la planeación de sistemas de información					
1.17	Se cuenta con una estructura orgánica para el desarrollo de sistemas					
1.18	Se realizan estimaciones Costo - Beneficio para el desarrollo de sistemas					
1.19	La planeación de desarrollo de sistemas se autoriza					
1.20	La planeación de desarrollo de sistemas se difunde					
1.21	La planeación de desarrollo de sistemas se documenta					
1.22	Se realiza control de las actividades y funciones en la fase de planeación					
1.23	Se realiza supervisión de las actividades y funciones de la fase de planeación					
2	ANALISIS					
2.1	Se realiza un análisis de requerimientos para el desarrollo de sistemas					
2.2	Se identifican las áreas del problema					
2.3	Se aplican en la organización principios para el análisis					
2.4	Se construyen prototipos de software a desarrollar					
2.5	Se elaboran especificaciones de sistema a desarrollar					
2.6	Se realizan revisiones de las especificaciones determinadas					
2.7	La organización cuenta con métodos de análisis de requerimientos					
2.8	Con cuales metodologías para el análisis de requerimientos					
2.9	Se cuenta con métodos de análisis orientados al flujo de datos					
2.10	Se cuenta con métodos de análisis orientados a la estructura de datos					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE DESARROLLO DE SISTEMAS.

EMPRESA:

	ESTIM.	REAL	DIF.		NOMBRE	FECHA	FIRMA
TIEMPO				PREPARO			
				REVISO			

No.	PREGUNTA	RPT.	SI	NO	N/A	OBSERVACIONES
2.11	Son utilizadas herramientas para la automatización del análisis de requerimientos					
2.12	Se elaboran requerimientos de base de datos					
2.13	Los requerimientos de base de datos son autorizados					
2.14	Los requerimientos de base de datos son documentados					
2.15	Se realiza supervisión de las actividades y funciones de la fase de análisis					
2.16	Se lleva a cabo control de las actividades y funciones de la fase de análisis					
3	DISEÑO					
3.1	Se cuenta con un proceso de diseño para el desarrollo de sistemas					
3.2	El diseño se elabora en base a la fase de generación					
3.3	El diseño se elabora en base a la fase de análisis					
	Se cuenta con fundamentos de diseño como					
3.4	Arquitectura del sistema					
3.5	Estructura del programa					
3.6	Estructura de datos					
3.7	Modularidad					
3.8	Abstracción					
3.9	Ocultamiento de información					
3.10	Se elabora un diseño arquitectónico para el desarrollo de sistemas					
3.11	Se elabora un diseño de datos para el desarrollo de sistemas					
3.12	Se elabora un diseño procedimental para el desarrollo de sistemas					
3.13	El diseño elaborado para el desarrollo de sistemas se autoriza					
3.14	El diseño elaborado para el desarrollo de sistemas se documenta					
3.15	El diseño elaborado para el desarrollo de sistemas se difunde					
3.16	Se elabora un diseño de flujo de información					
3.17	Se cuenta con procedimientos para la construcción lógica de programas y sistemas					
3.18	Son utilizadas técnicas para la elaboración del diseño de nuevos sistemas a elaborar					
3.19	Se cuenta con lineamientos para la elaboración del diseño de nuevos sistemas					
3.20	Se lleva a supervisión de las actividades y funciones de la fase de diseño					
3.21	Se lleva a cabo control de las actividades y funciones de la fase de diseño					
4	CODIFICACION					
4.1	Se lleva a un proceso de traducción del diseño de sistema a un lenguaje de programación					
4.2	Se analizan las características de lenguaje de programación a utilizar					
4.3	Se toman en cuenta diversos criterios de lenguajes de programación, para emplear uno					
4.4	Se contemplan los tipos de datos que se van a utilizar en el nuevo sistema					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE DESARROLLO DE SISTEMAS.

		ESTIM	REAL	DIF		NOMBRE	FECHA	FIRMA
EMPRESA:	TIEMPO				PREPARO			
					REVISO			

NO.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
4.5	Se tiene definido un estilo de codificación dentro de la organización					
4.6	Se elabora documentación de la codificación realizada					
4.7	Se evalua el grado de eficiencia de la codificación realizada					
4.8	Se cuenta con técnicas para determinar la calidad del código					
4.9	Se cuenta con herramientas para determinar la calidad del código					
4.10	Se realiza supervisión de las actividades y funciones de la fase de codificación					
4.11	Se realiza control de las actividades y funciones de la fase de codificación					
5	PRUEBAS					
5.1	Se determina el objetivo de cada prueba a realizar					
5.2	Se determina el alcance de cada prueba a realizar					
5.3	Se determina el procedimiento de cada prueba a realizar					
5.4	Se documentan los objetivos y alcances de las pruebas					
5.5	Se diseñan diferentes casos para cada prueba					
5.6	Se documentan los resultados obtenidos en las pruebas					
5.7	Se analizan los resultados obtenidos en las pruebas					
5.8	Se obtienen conclusiones con base en las pruebas					
5.9	Se realizan pruebas de unidad a los sistemas desarrollados					
5.10	Se realizan pruebas de integración a los sistemas desarrollados					
5.11	Se realizan pruebas de validación a los sistemas desarrollados					
5.12	Se realiza supervisión de las actividades y funciones de la fase de pruebas					
5.13	Se realiza control de las actividades y funciones de la fase de pruebas					
6	MANTENIMIENTO					
6.1	Se tienen documentadas las características del mantenimiento para los sistemas de la organización					
6.2	Se elabora un análisis Costo - Beneficio del mantenimiento del sistema					
6.3	Se consideran los posibles factores negativos para dar el mantenimiento a los sistemas					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE DESARROLLO DE SISTEMAS.

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
6.4	La organización cuenta con una estructura orgánica para proporcionar mantenimiento a los sistemas					
6.5	Se tienen establecidas tareas para el mantenimiento de sistemas					
6.6	Se tienen documentadas las tareas para el mantenimiento de sistemas					
6.7	Se tienen difundidas las tareas para el mantenimiento de sistemas					
6.8	Se consideran los efectos provocados por el mantenimiento realizado a los sistemas					
6.9	Se realiza control de las actividades y funciones de la fase de mantenimiento					
6.10	Se realiza supervisión de las actividades y funciones de la fase de mantenimiento					

VI.4. DEFINICIÓN DE PROCEDIMIENTOS DE AUDITORIA AL DESARROLLO DE SISTEMAS.

1.- PLANEACION

PROC.1.1. Conocer los medios y/o métodos establecidos para determinar el alcance de un sistema, Verificando que se aplique durante la fase de planeación en todos los sistemas desarrollados.

PROC.1.2. Verificar que durante la fase de planeación, el alcance del sistema este delimitado, documentado y difundido.

PROC.1.3. Revisar los planes y programas de trabajo, indicando si en su contenido.

- Se definen objetivos.
- Tiempos y costos estimados.
- Personal asignado.
- Actividades, funciones, responsabilidades y obligaciones del personal.

PROC.1.4. Solicitar y evaluar las estimaciones cuantitativas realizadas para el desarrollo de nuevos sistemas en la organización.

PROC.1.5 Conocer los medios utilizados para realizar las estimaciones de recursos humanos, hardware y software, necesarios para el desarrollo de sistemas en la organización. Verificando que las estimaciones sean completas, autorizadas, difundidas y documentadas.

PROC.1.6. Conocer las técnicas utilizadas para medir la productividad del sistema, Verificando la revisión de calidad, función y tamaño de cada sistema.

PROC.1.7. Conocer los modelos utilizados para la planeación del desarrollo de sistemas, Verificando que su utilización sea general, este documentada, difundida y actualizada.

PROC.1.8. Conocer las herramientas utilizadas para la planeación del desarrollo de sistemas, Verificando que su uso sea fácil, sencillo y claro permitiendo obtener resultados rápidamente.

PROC.1.9. Evaluar la estructura Orgánica para el desarrollo de sistemas, Verificando que cuente con adecuadas líneas de autoridad, responsabilidad y control.

PROC.1.10. Conocer y evaluar la planeación del desarrollo de sistemas dentro de la organización. Verificando que sea autorizada por la persona y/o instancia adecuada contando con medios actualizados para su documentación y difusión.

PROC.1.11 Conocer los medios y/o métodos utilizados para llevar a cabo la supervisión y control de las actividades y funciones de la fase de planeación del desarrollo de sistemas. Verificando que exista una persona responsable de su ejecución encargada de documentar los resultados obtenidos

2.- ANALISIS.

PROC.2.1. Verificar la elaboración del análisis de requerimientos para el desarrollo de sistemas. Evaluando la forma de su realización, así como los medios utilizados para la definición de los mismos.

PROC.2.2. Conocer las técnicas y/o métodos utilizados para identificar las áreas del problema dentro de la organización. Verificando su confiabilidad y cumplimiento.

PROC.2.3. Conocer las técnicas y/o herramientas utilizadas para construir prototipos de software a desarrollar. Verificando que se haya realizado una petición del sistema, así como una consideración de todas las circunstancias y apreciaciones que se requieren en la construcción de un prototipo.

PROC.2.4. Identificar y evaluar las especificaciones elaboradas para el sistema. Verificando la aprobación y documentación formal de los requerimientos para que estos puedan ser analizados y verificados con oportunidad por cualquier miembro del equipo de trabajo.

PROC.2.5. Verificar que las especificaciones elaboradas sean autorizadas y difundidas oportunamente, con la finalidad de determinar el grado de oportunidad y funcionalidad de las mismas.

PROC.2.6. Conocer los métodos de análisis de requerimientos utilizados. Verificando que faciliten al analista la aplicación de los principios fundamentales del análisis de una manera sistematizada, examinando algunas de las características comunes en todos los métodos.

PROC.2.7. Conocer las metodologías de análisis de requerimientos. Verificando que se cumpla como mínimo con los siguientes aspectos :

- Para subdividir el problema.
- Representaciones Mecanismos para el análisis.

- Método de presentación.
- Mecanismos lógicas y físicas.

PROC.2.8. Conocer los métodos de análisis de flujo de datos. Verificando el uso de técnicas que representen el flujo de información a través del sistema. Identificando la presentación de una transformación clara y sencilla de la información.

PROC.2.9. Conocer los métodos de análisis de estructuras de datos utilizadas para representar los requerimientos del software. Verificando que los métodos ayuden al analista en la identificación de los objetos de información (acciones o procesos).

PROC.2.10 Conocer los requerimientos de bases de datos. Verificando que incluya documentación formal y autorizada; con las mismas tareas que el análisis de requerimientos del sistema.

PROC.2.11 Conocer los medios y/o métodos utilizados para llevar a cabo la supervisión y control de las actividades y funciones de la fase de análisis del desarrollo de sistemas. Verificando que exista una persona responsable de su ejecución encargada de documentar los resultados obtenidos

3.- DISEÑO.

PROC.3.1. Conocer el proceso para la elaboración de diseño en el desarrollo de sistemas en la organización. Verificando que se realice en base a la planeación y análisis de requerimientos realizados previamente.

PROC.3.2. Conocer las estrategias utilizadas por la organización, para fundamentar el diseño elaborado. Identificando la estrategia utilizada, los elementos que considera, así como las ventajas y desventajas que otorga cada una.

PROC.3.3. Identificar el /los método(s) empleados para elaborar el diseño de datos. Verificando que est actividad se realice durante el desarrollo del sistema; contando con una persona responsable. Independientemente de las técnicas de diseño usadas.

PROC.3.4. Conocer el diseño arquitectónico elaborado, Verificando su claridad, y comprensión con la finalidad de identificar que el diseño desarrolle una estructura de programa modular y represente las relaciones de control entre módulos.

PROC.3.5. Verificar el diseño procedimental del sistema. Identificando y evaluando que se haya elaborado definiendo los detalles algoritmos de forma clara para todos los miembros del equipo de desarrollo de sistemas de la organización.

PROC.3.6. Solicitar la documentación existente del sistema. Verificando que este completa y autorizada. Identificando los medios utilizados para su difusión.

PROC.3.7. Identificar el diseño de flujo de información elaborado. Verificando que el diseño contenga:

- Establezca el tipo de flujo de información.
- Indique los límites del flujo.
- Convierta los DFD (Diagramas de Flujo de Información) en la estructura del programa.

PROC.3.8. Conocer los procedimientos existentes para la construcción lógica de programas y sistemas. Verificando que estén documentados, difundidos y autorizados.

PROC.3.9. Conocer e identificar las técnicas y herramientas utilizadas para elaborar el diseño de sistemas. Verificando que su uso sea general, documentado, estándar, autorizado y difundido en toda la Organización.

PROC.3.10 Conocer los medios y/o métodos utilizados para llevar a cabo la supervisión y control de las actividades y funciones de la fase de diseño del desarrollo de sistemas. Verificando que exista una persona responsable de su ejecución encargada de documentar los resultados obtenidos

4.- CODIFICACION

PROC.4.1. Conocer el proceso de codificación para el desarrollo de sistemas. Verificando que se haya realizado en base la diseño realizado previamente.

PROC.4.2. Solicitar el análisis elaborado, para la elección del lenguaje de programación a utilizar para la fase de codificación del sistema. Identificando que este contenga las ventajas y desventajas proporcionadas, así como el costo-beneficio obtenido por la organización, con su elección.

PROC.4.3. Verificar que se hayan considerado los tipos de datos utilizados en el sistema. Señalando si estos fueron considerados de igual manera en el análisis elaborado para la elección del lenguaje de programación.

PROC.4.4. Entrevistar a la persona responsable del área de desarrollo de sistemas con la finalidad de obtener información respecto a:

- La existencia de una persona responsable de la fase de codificación de los sistemas.
- Conocer el estilo establecido y/o definido por la organización para la codificación de sus programas y/o sistemas.
- Los medios y/o métodos utilizados para la autorización y difusión entre todo el personal del estilo de codificación existente en la organización

PROC.4.5. Solicitar la documentación existente de la fase de codificación, con el objeto de verificar su autorización, actualización y difusión entre todo el equipo de desarrollo de sistemas en la organización.

PROC.4.6. Conocer e Identificar las técnicas y herramientas utilizadas en la organización para medir la calidad de los sistemas desarrollados. Verificando que su uso sea general y adecuado.

PROC.4.7. Conocer los medios y/o métodos utilizados para llevar a cabo la supervisión y control de las actividades y funciones de la fase de codificación del desarrollo de sistemas. Verificando que exista una persona responsable de su ejecución encargada de documentar los resultados obtenidos

5.- PRUEBAS.

PROC.5.1. Solicitar la documentación existente para la realización de pruebas a los sistemas de la organización. Verificando que cada prueba a ejecutar cuente con objetivo, alcance, autorización, actualización y difusión.

PROC.5.2. Conocer el procedimiento a seguir en cada prueba. Identificando que tenga una secuencia lógica, clara y sencilla para el personal encargado de su ejecución.

PROC.5.3. Identificar los aspectos que se consideran para la elaboración de pruebas. Verificando la existencia de varios casos para cada una de ellas.

PROC.5.4. Conocer las herramientas utilizadas para la elaboración de pruebas. Verificando que sean de uso general y adecuado para los sistemas en prueba.

PROC.5.5. Conocer la documentación que se elabora, cuando se realiza la prueba. Identificando los medios utilizados para la documentación y difusión de resultados. Verificando que se realice un análisis completo y profundo cuando los resultados no sean los esperados.

PROC.5.6. Entrevistar al responsable del área de Informática, con la finalidad de conocer los siguientes aspectos

- Tipos de pruebas existentes.
- Como y por que se eligieron esos tipos
- Ventajas y desventajas que ofrecen.
- Métodos y/o medios utilizados para su actualización, difusión y autorización.

PROC.5.7. Conocer los medios y/o métodos utilizados para llevar a cabo la supervisión y control de las actividades y funciones de la fase de pruebas.

Verificando que exista una persona responsable de su ejecución encargada de documentar los resultados obtenidos

6.- MANTENIMIENTO.

PROC.6.1. Conocer la documentación existente que contenga las características del mantenimiento a los sistemas. Verificando que contenga los siguientes puntos:

- Las actividades requeridas para cumplir el mantenimiento.
- Los costos del mantenimiento.
- Determinación de los problemas del mantenimiento.
- Análisis de los problemas del mantenimiento.

PROC.6.2. Identificar en el organigrama del área de Informática al responsable del mantenimiento de sistemas. Verificando que se cuente funciones, actividades, responsabilidades y obligaciones para el puesto.

PROC.6.3. Conocer los medios y/o métodos utilizados para la documentación, autorización y difusión de las características del mantenimiento de sistemas.

PROC.6.4. Conocer las actividades establecidas por el área de informática y la organización en general; para analizar los efectos primarios y secundarios provocados por el mantenimiento.

PROC.6.5. Conocer los medios y/o métodos utilizados para llevar a cabo la supervisión y control de las actividades y funciones de la fase de mantenimiento del desarrollo de sistemas. Verificando que exista una persona responsable de su ejecución encargada de documentar los resultados obtenidos

VII. REVISION DE EQUIPOS PERSONALES

VII.1. OBJETIVO DE LA REVISION.

En este capitulo se llevara a cabo una revisión completa de todos los aspectos relacionados con equipos personales. Dentro de los equipos personales se encuentran considerados todos los que no están conectados a ninguna plataforma de trabajo.

Esta revisión tiene como objetivo asegurarse de que se hayan contemplado tanto la seguridad física como lógica en los equipos personales, ya que los mismos son susceptibles a peligros similares a los que ya hemos mencionado en capitulos anteriores.

Cabe aclarar que aunque los aspectos que se tratan en este capitulo son similares a los que corresponden a la revisión en redes, es muy importante retomarlos ya que existen diferencias muy sobresalientes en la forma de revisar dichos aspectos, y por otro lado la estructuración de la revisión también está contemplada en forma distinta a la de redes.

De entre los puntos mas importantes a considerar, mencionaremos a continuación algunos de ellos:

1. Evaluación de las necesidades de equipo que trabaje de manera aislada , equiparado con el costo que este representa.

2. Establecer que la ubicación de equipos personales, los controles de acceso, los responsables de los mismos se encuentran documentados, son del conocimiento de los usuarios y se actualizan periódicamente.

3. Evaluar la seguridad física que para los componentes de hardware y software se tiene establecida.

4. Revisar las políticas establecidas para el acceso y uso de equipos personales, para establecer los aspectos que abarcan, así como el nivel de seguridad con que se cuenta.

5. La existencia de programas de respaldo que aseguren la integridad de la información en el caso de ocurrir alguna contingencia.

6. Establecimiento de políticas para la instalación de nuevos programas y para la restricción de copias no autorizadas.

7. Creación de programas de protección antivirus

8. Establecimiento de lineamientos para salvaguardar los equipos personales, como el uso de passwords y llaves.

9. Establecimiento de programas de seguridad física que contemplen equipos personales y portátiles.

10. Supervisión de controles de información y programas recibidos de fuentes remotas.

VII.2. ASPECTOS QUE ABARCA.

COSTO-BENEFICIO (Adquisiciones)

Este aspecto considera un estudio profundo de las necesidades que la empresa tiene, las posibles soluciones que se puedan generar y el costo que cada una representa para la organización.

Generalmente se estudian los aspectos económicos, operativos y tecnológicos, para facilitar la toma de decisiones, y con ello garantizar la mejor solución dentro de un contexto equilibrado de el costo-beneficio que resulta para la empresa.

Una vez realizado dicho estudio se debe considerar también, la existencia dentro de los planes y políticas una sección especializada en adquisición de hardware y software para equipos personales.

SEGURIDAD LÓGICA

Con el constante avance de la informática y la cada vez mas generalizada y amplia cultura informática, dentro de las organizaciones se ha difundido el uso de las computadoras personales. Esto hace a la información y programas susceptibles de sufrir daños ya sea de manera intencional, no intencional o por fenómenos naturales. Cualquiera que sea la causa resulta indispensable que en las empresas se implanten controles, planes y políticas muy estrictos para proteger todos y cada uno de los equipos personales.

Esta seguridad por lo tanto debe cubrir los siguientes puntos:

- Destrucción de información
- Mal uso de información y programas
- Copias no autorizadas
- Introducción de informacion y paquetería no autorizada
- Introducción de virus informáticos
- Protección de respaldos de programas, paquetes e información.

SEGURIDAD FÍSICA

En este punto podemos mencionar, que como todos los recursos informáticos los equipos personales y la información contenida en ellas es susceptible de sufrir algún daño ya sea por parte de los usuarios, consciente o inconscientemente, o bien, por fenómenos naturales, deben existir políticas, programas y planes para evitar al máximo cualquier daño.

La seguridad física entonces, es la que se encarga de prever todas las posibles causas por las que pudiera existir un daño al equipo y por su puesto de tratar de evitar estos daños siempre y cuando sea posible; como en el caso de que algún empleado tratara de dañar el equipo, variaciones de voltaje, o daños provocados por la mala ubicación del equipo.

VII.3 CUESTIONARIO DE CONTROL INTERNO

CUESTIONARIO DE CONTROL INTERNO
REVISION DE EQUIPOS PERSONALES

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

EMPRESA:

	ESTIM	REAL	DIF
TIEMPO			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
1	COSTO-BENEFICIO (Adquisiciones)					
1.1	Existe dentro de las políticas de adquisiciones de hardware y software un apartado para equipos personales					
1.2	Se actualizan con periodicidad las políticas de adquisición de equipos personales					
1.3	Existe un área responsable de la adquisición de hardware y software en equipos personales					
1.4	Existe una persona responsable de la adquisición de hardware y software para equipos personales					
1.5	Se tienen establecidos criterios para la selección de los responsables					
1.6	Existen criterios que definan cuando es válida la solicitud de un equipo personal					
1.7	Se encuentran bien fundamentados los criterios de validez de una solicitud de equipo personal					
1.8	Se ha difundido entre los usuarios los criterios de validez de solicitud					
1.9	Para la adquisición de hardware y software de equipos personales se realiza un estudio de factibilidad técnica					
1.10	Para la adquisición de hardware y software de equipos personales se realiza un estudio de factibilidad operativa					
1.11	Para la adquisición de hardware y software de equipos personales se realiza un estudio de factibilidad económica					
1.12	En los estudios de factibilidad realizados se evalúan las mejoras por los cuales es necesario adquirir equipo destinado a trabajo avanzado					
1.13	Se documentan los estudios realizados					
1.14	Se lleva a cabo una evaluación de cada uno de los estudios realizados					
1.15	Se cuenta dentro de las políticas de adquisición con una sección para el apartado de contratos de adquisición de equipos personales					
1.16	Se solicitan varias ofertas técnicas					
1.17	Se realizan evaluaciones de las ofertas para adquirir la mejor opción					
1.18	En las ofertas se incluyen especificaciones técnicas					
1.19	Se comentan las evaluaciones de las ofertas					
1.20	Se tienen establecidos requisitos para la compra de hardware y software avanzado					
1.21	Se revisan periódicamente los requisitos para la compra de equipos personales					
1.22	Se actualizan periódicamente los requisitos de compra de equipos personales					
1.23	Cuando se realiza una actualización de los requisitos de compra de inmediato se hace de conocimiento de todos los usuarios					
1.24	Se documentan los resultados obtenidos con las adquisiciones de equipos personales					
1.25	Se evalúan los resultados obtenidos con las adquisiciones					
1.26	Se publican entre los usuarios los avances y logros obtenidos con las adquisiciones de equipos personales					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE EQUIPOS PERSONALES

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

	ESTIM	REAL	DIF
TIEMPO			

EMPRESA:

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
2	SEGURIDAD LOGICA					
2.1	Existe una terminal de control de acceso a equipos personales					
2.2	Se cuenta con políticas para seguridad de información en equipos personales					
2.3	Se actualizan con periodicidad las políticas de seguridad de información de equipos personales					
2.4	Son de conocimiento de los usuarios de equipos personales estas políticas					
2.5	Las políticas son claras y fáciles de entender					
2.6	Se cuenta con documentación de los controles de acceso					
2.7	Se limita la documentación de los controles de acceso					
2.8	Se realizan actualizaciones periódicas de los controles de acceso					
2.9	Dentro de las políticas se consideran sanciones por violaciones a la integridad de la información					
2.1	Las sanciones por violar la integridad de la información son del conocimiento de todos los usuarios					
2.11	Las sanciones son aplicadas sin importar el usuario de que se trate					
2.12	Existen planes y programas de respaldo de información					
2.13	Existen dispositivos para evitar la contaminación por virus					
2.14	Los dispositivos contra virus cuentan con una actualización constante					
2.15	Se cuenta con copias de seguridad de programas y software					
2.16	Existen políticas para la instalación de programas y software					
2.17	Se cuenta con controles y dispositivos para evitar la instalación de software y programas no autorizados					
2.18	Se tienen controles de información recibida de fuentes remotas					
2.19	Los controles para protección y uso de información recibida por fuentes remotas se documentan					
2.20	Los controles para protección y uso de información recibida por fuentes remotas se analizan					
2.21	Las políticas de seguridad en equipos personales son mismas en todas las áreas de la organización					
2.22	Los equipos portátiles se consideran dentro de la sección de seguridad de información de equipos personales					
2.23	Los programas y software cuentan con password para el acceso a alguna otra clase de dispositivo o clave de protección					
2.24	Se cuenta con políticas y controles específicos para los equipos personales relacionados para recibir o enviar información a lugares remotos					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE EQUIPOS PERSONALES

EMPRESA:

		ESTIM	REAL	DIF
TIEMPO				

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

NO.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
3	SEGURIDAD FISICA					
3.1	Existen planes y políticas para seleccionar los lugares en que se ubican o se deberán ubicar los equipos personales					
3.2	Se cuenta con normas de seguridad física para equipos personales					
3.3	Todos los lugares destinados para un equipo personal cumplen con las normas de seguridad de					
3.4	Se lleva un control de los accesos a equipos personales					
3.5	Se cuenta con controles de uso de equipos personales para evitar el robo de componentes					
3.6	Existen candados, llaves u otro tipo de dispositivos para proteger los equipos personales					
3.7	Existe un responsable de la integridad física de los equipos personales					
3.8	Se cuenta con criterios establecidos para la asignación de los responsables					
3.9	Se cuenta con políticas para el acceso a equipos personales					
3.10	Se divulgan entre los usuarios de los equipos personales las políticas para el acceso					
3.11	Para los equipos portátiles se utilizan los mismos criterios que para los equipos personales					
3.12	Se evalúa en los riesgos potenciales a los que están expuestos los equipos personales dependiendo de su ubicación					
3.13	Se cuenta con mantenimiento correctivo y preventivo para los equipos personales					
3.14	Dentro del mantenimiento se debe considerar el reemplazo del equipo					
3.15	Se cuenta con seguros que cubran el equipo de posibles riesgos naturales como sismos, inundaciones, etc.					
3.16	Se revisan y analizan periódicamente todos los controles para seguridad en equipos personales					

VII.4. DEFINICION DE PROCEDIMIENTOS DE AUDITORIA EN EQUIPOS PERSONALES

1. COSTO-BENEFICIO (Adquisiciones)

PROC.1.1 Evaluar las políticas de adquisiciones de hardware y software, para establecer la existencia de un apartado especializado en equipos personales.

PROC.1.2 Analizar las políticas de adquisiciones de hardware y software para equipos personales, evaluando cuales fueron los criterios tomados en su elaboración.

PROC.1.3 Analizar y evaluar los criterios utilizados para la asignación de un área responsable de las adquisiciones de equipos personales.

PROC.1.4 Entrevistar a algunas personas responsables de las adquisiciones de equipos personales, para determinar el cumplimiento de las políticas establecidas.

PROC.1.5 Establecer la periodicidad con la que se actualizan las políticas de adquisiciones de equipos personales establecidas.

PROC.1.6 Analizar la elaboración de estudios de factibilidad técnica, operativa y económica. Evaluando los criterios utilizados en ellos y la documentación surgida de los mismos

PROC.1.7 Verificar y determinar que se consideren todas y cada una de las condiciones de la empresa (presupuestarias, financieras, etc.).

PROC.1.8 Verificar el cumplimiento de las políticas para elaboración de contratos.

PROC.1.9 Analizar y evaluar los requisitos que fueron especificados, para ser proveedor de la organizacion.

PROC.1.10 Verificar las especificaciones requeridas para las propuestas económicas se cumplan en todos sus puntos.

PROC.1.11 Entrevistar a algunas personas de el área encargada de adquisiciones de equipos personales, para determinar el grado de entendimiento y aplicación de los criterios de evaluación de propuestas y proveedores.

PROC.1.12 Verificar y evaluar, que exista una documentación adecuada y completa de todo el procedimiento de adquisiciones de equipos personales.

PROC.1.13 Verificar y evaluar, que exista una documentación adecuada y completa de los avances y resultados alcanzados con las adquisiciones de equipos personales.

PROC.1.14 Verificar que se realice una supervisión de todo el procedimiento de adquisiciones.

PROC.1.15 Determinar si las actualizaciones de políticas para adquisiciones, se realizan en base a la documentación y estudios realizados en anteriores adquisiciones.

PROC.1.16 Identificar las caracteristicas tanto de la licencias de software como de las garantías de hardware, para determinar si fueron las mejores ofrecidas.

1.1 Capacitación de Software para equipos personales

PROC.1.1.1 Identificar y evaluar los criterios que se utilizan para determinar la capacitación de software requerida por los usuarios de equipos personales.

PROC.1.1.2 Determinar si se verifican planes de estudio y temarios propuestos por varias instituciones, para seleccionar el mas adecuado a las necesidades de software.

PROC.1.1.3 En el caso de que la capacitación sea interna, identificar cuales son los puntos que se tomaron en cuenta para elaborar los temarios. Y determinar quienes fueron las personas que los autorizaron.

2. SEGURIDAD LÓGICA

PROC.2.1 Verificar que existan y se apliquen políticas para la asignación de un responsable de el acceso a la información en equipos personales.

PROC.2.2 Verificar que existan políticas de seguridad de información de equipos personales.

PROC.2.3 Determinar y evaluar los criterios empleados para elaborar las políticas de seguridad de información de equipos personales.

PROC.2.4 Verificar que existan políticas de manejo y uso de información de equipos personales.

PROC.2.5 Entrevistar a algunos usuarios de equipos personales, para verificar la difusión de las políticas tanto de acceso, como de uso y manejo de la información

PROC.2.6 Identificar entre los usuarios de equipos personales el grado de conocimiento y entendimiento de las políticas establecidas, para determinar la claridad con la que fueron realizadas.

PROC.2.7 Verificar la periodicidad con que se actualizan y difunden las políticas de acceso y protección de información en equipos personales.

PROC.2.8 Determinar la existencia de controles de acceso, verificando que se cuente con documentación de los mismos.

PROC.2.9 Identificar la periodicidad con la que se actualizan los controles de acceso a equipos personales.

PROC.2.10 Verificar que se lleve a cabo un análisis de la documentación de los controles de acceso. Y determinar que se apliquen las medidas establecidas en el caso de existir violaciones a las políticas de uso y acceso a la información de equipos personales.

PROC.2.11 Verificar la existencia de programas de respaldo de información en equipos personales; evaluando su cumplimiento, difusión entre los usuarios y documentación.

PROC.2.12 Verificar la existencia de controles para evitar la contaminación por virus, su difusión y la aplicación entre los usuarios de equipos personales; así como la periodicidad con la que se actualizan.

PROC.2.13 Identificar la existencia, aplicación, difusión y actualización de controles, para la instalación de programas y software en equipos personales y evaluar la seguridad existente en contra de programas y software no autorizado.

PROC.2.14 Verificar la existencia de procedimientos, políticas o controles para el manejo de información de fuentes remotas.

PROC.2.15 Entrevistar a algunos usuarios de equipos personales de diferentes áreas, para determinar las diferencias de uso y aplicación de las políticas de protección de software, dependiendo del área que se trate.

PROC.2.16 Determinar cual es la seguridad que se tiene especificada para la información contenida en equipos portátiles.

PROC.2.17 Determinar además de los controles y políticas, con que tipo de seguridad se cuenta para la protección de la información en equipos personales.

3. SEGURIDAD FÍSICA

PROC.3.1 Verificar y evaluar los planes y políticas para seleccionar, los lugares de colocación de los equipos personales. Identificando los criterios utilizados para su elaboración, la periodicidad con que se actualizan, y la difusión que les da entre los usuarios.

PROC.3.2 Revisar físicamente los lugares en los que se ubican los equipos personales para verificar el cumplimiento delas normas de seguridad física de los mismos.

PROC.3.3 Identificar y evaluar los controles de uso de equipos personales, que pudieren servir para prevenir o detectar los faltantes de componentes de equipos personales.

PROC.3.4 Verificar que se cuente con candados o llaves para proteger los equipos personales.

PROC.3.5 Identificar a los responsables de la integridad física de cada uno de los equipos personales, para evaluar los criterios utilizados en su selección, así como sus responsabilidades.

PROC.3.6 Identificar y evaluar las precauciones tomadas para prevenir los riesgos potenciales a los que están expuestos los equipos personales.

PROC.3.7. Verificar que exista un programa de mantenimiento preventivo y correctivo, evaluar las condiciones que ofrece el mismo y determinar si se contrato la mejor opción de mantenimiento.

PROC.3.8 Verificar que existan seguros, identificando cuales son los posibles desastres y contingencias que cubren, para evaluar que criterios se utilizaron en su contratación.

PROC.3.9 Verificar la periodicidad con que se revisan, analizan y actualizan los controles para seguridad de equipos personales. Y determinar si se lleva a cabo un seguimiento de posibles deficiencias y violaciones de la seguridad.

PROC.3.10 Revisar que exista documentación tanto de las actualizaciones como de el seguimiento que se da a las revisiones realizadas.

PROC.3.11 Identificar que criterios se utilizan para la actualización de los controles y normas de seguridad en equipos personales.

VIII. REVISION DE TELECOMUNICACIONES

VII.1. OBJETIVO DE LA REVISION.

El objeto de revisar telecomunicaciones en un centro de cómputo o área(s) de informática es asegurar la protección de hardware, circuitos de red y software a través de la revisión de seguridad física, además, garantizar la integridad de la información con la evaluación que se realiza sobre seguridad lógica.

El software y hardware en Telecomunicaciones juegan un papel vital para los sistemas de aplicación en línea, en donde datos y programas son transmitidos de un punto a otro a través de líneas de teléfono, vía satélite u otros medios. Es por ello que se considera necesaria la revisión de telecomunicaciones.

En la actualidad las organizaciones gastan enormes cantidades de recursos en telecomunicaciones para lograr un crecimiento del negocio a nivel nacional e internacional.

La adquisición e instalación de hardware y software deben ser contemplados como parte de la planeación integral de la organización. Esta alternativa para la solución del problema del negocio, deberá ser idónea para ayudar al crecimiento y logro de los objetivos y metas en toda la organización.

El análisis de telecomunicaciones deberá considerarse en aplicaciones de desarrollo de sistemas y proyectos para asegurar la adecuada definición de hardware y software como parte de un sistema en general.

La seguridad debe ser revisada con atención desde la administración e instalación, dado que numerosas computadoras de la organización tienen acceso a archivos de datos y programas que pueden ser destruidos o modificados en forma intencional o errónea.

Por lo anterior es necesario que en una organización exista una función formal de Telecomunicaciones que tenga como objetivos los siguientes:

- Asegurar la existencia de procedimientos y controles para lograr: la administración, instalación, operación, seguridad y mantenimiento de las telecomunicaciones.
- Detectar el grado de confianza, satisfacción y desempeño que brindan las telecomunicaciones a la organización.
- Verificar que existan parámetros de medición del desempeño de las telecomunicaciones (bitácoras, gráficas, estadísticas).

- Evaluar el grado de soporte que se brinda a los usuarios en el uso de sistemas y software en la red de telecomunicaciones.

- Determinar si existen los suficientes controles y procedimientos de seguridad de las telecomunicaciones de la organización.

- Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes de telecomunicaciones.

- Verificar que se cuente con software que apoye el monitoreo y la auditoria de los diversos elementos que componen las telecomunicaciones.

VII.2. ASPECTOS QUE ABARCA.

Dentro de la revisión de telecomunicaciones se deben considerar 3 aspectos:

I. Administración de Telecomunicaciones.

II. Seguridad Física de Telecomunicaciones.

III.Seguridad Lógica de Telecomunicaciones.

ADMINISTRACION DE TELECOMUNICACIONES

En un principio el controlar y administrar telecomunicaciones no era complicado, pues solo consistía en llamar a una compañía telefónica para instalar equipo y resolver cualquier problema con las líneas o comunicaciones. Con la desregulación y la aparición de nuevos equipos telefónicos y compañías operadoras, el manejo de estas funciones se volvió una tarea complicada.

El procesamiento de datos típico de una organización, utiliza ahora una gran variedad de proveedores para satisfacer sus necesidades de telecomunicaciones y cuando surgen problemas, una persona especializada de los mismos proveedores auxilia a las organizaciones cada vez que es necesario.

Un elemento importante en la Administración de Telecomunicaciones es su fortaleza, basada en un correcto control, por lo cual es necesario considerar cuando se trata de redes muy grandes, una área especializada de telecomunicaciones pero cuando la red es pequeña puede delegar la responsabilidad de el manejo de telecomunicaciones a el departamento encargado Redes.

Las funciones típicas de la administración de telecomunicaciones son las siguientes:

- Administrar y controlar los recursos de telecomunicaciones.
- Reportar sobre el uso de telecomunicaciones.
- Monitorear periódicamente las telecomunicaciones para evitar accesos no autorizados o daños en las mismas.

SEGURIDAD FÍSICA DE TELECOMUNICACIONES

La seguridad depende en última instancia, de la integridad de los individuos que conforman una organización. No existe una seguridad total, por lo tanto cada organización depende de su personal y de las medidas adoptadas para lograr los niveles de seguridad requeridos. Por ello es importante considerar dentro de la revisión física los siguientes aspectos:

- La documentación en la que se describen los sistemas de telecomunicaciones se encuentre en lugar seguro, al cual solo tienen acceso las personas autorizadas.
- Existencia de planes y políticas para prevenir posibles daños o robos del equipo de telecomunicaciones, causados por personas autorizadas o no autorizadas, de manera intencional e involuntaria, además, que estos controles sean publicados y revisados periódicamente.
- Existencia de normatividad y controles para el acceso y uso del equipo de telecomunicaciones
- Las líneas de teléfono cuenten con llaves o candados, además de la elaboración de controles de uso.

SEGURIDAD LÓGICA DE TELECOMUNICACIONES

En una organización, la seguridad lógica permite garantizar la integridad de la información manejada por telecomunicaciones, ya que esta se encuentra expuesta a sufrir daños o a ser mal utilizada, por la complejidad y amplitud que han alcanzado las telecomunicaciones.

La seguridad lógica abarca varios aspectos para poder garantizar la integridad de la información o en su defecto prevenir irregularidades, así como, detectar a los responsables de las mismas, a continuación se mencionan los puntos mas importantes:

- Existencia, difusión y actualización de documentación sobre la normatividad del manejo de información.
- Controles de los usuarios autorizados a accesar la información de telecomunicaciones
- Controles de el uso de la información de telecomunicaciones.
- Existencia, difusión y actualización de planes y políticas para la recuperación de información en caso de contingencias.

VIII.3 CUESTIONARIO DE CONTROL INTERNO

CUESTIONARIO DE CONTROL INTERNO
REVISION DE TELECOMUNICACIONES

EMPRESA:

	ESTIM	REAL	DIF		NOMBRE	FECHA	FIRMA
TIEMPO				PREPARO			
				REVISO			

NO.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
1	ADMINISTRACION DE TELECOMUNICACIONES					
1.1	Se cuenta con procedimientos y políticas establecidas para la administración de telecomunicaciones					
1.2	Existe dentro de los procedimientos y políticas una sección especializada en administración de telecomunicaciones					
1.3	Existe un encargado de la administración de telecomunicaciones					
1.4	Se cuenta con políticas o criterios para elegir al encargado de la administración de telecomunicaciones					
1.5	Se actualizan las políticas para la elección de encargado de administración de telecomunicaciones					
1.6	Se encuentran documentadas las funciones de encargado de telecomunicaciones					
1.7	Se revisan y actualizan periódicamente las funciones del encargado de telecomunicaciones					
1.8	Las funciones de administración de telecomunicaciones están redactadas de forma concisa y clara					
1.9	La documentación de las funciones de administración es de conocimiento de encargado					
1.10	Se realizan visitas sobre el uso de telecomunicaciones					
1.11	Existen criterios y políticas para la elaboración de los informes sobre el uso de telecomunicaciones					
1.12	Se revisan y analizan periódicamente los informes de uso de telecomunicaciones					
1.13	Las políticas y procedimientos para administración de telecomunicaciones son del conocimiento de los usuarios					
1.14	Existen sanciones para la violación de los procedimientos y políticas de telecomunicaciones					
1.15	Las sanciones se encuentran documentadas dentro de las políticas y procedimientos de telecomunicaciones					
1.16	Se realiza un análisis periódico de las violaciones a los sistemas de telecomunicaciones					
1.17	Existen políticas o criterios para la selección del personal de telecomunicaciones					
1.18	Se encuentran documentados los criterios para selección del personal de telecomunicaciones					
1.19	Entre las funciones del personal de telecomunicaciones se considera su participación en la implantación de nuevos sistemas de telecomunicaciones					
1.20	Entre las funciones del personal de telecomunicaciones se considera el diseño y desarrollo de nuevas aplicaciones					
2	SEGURIDAD FISICA DE TELECOMUNICACIONES					
2.1	La documentación sobre sistemas de telecomunicaciones se encuentra en un lugar seguro					
2.2	Solo tiene acceso a la documentación de los sistemas de telecomunicaciones personal autorizado					
2.3	Se cuenta con un control de los accesos a la información de telecomunicaciones					
2.4	Se actualiza periódicamente la documentación sobre los sistemas de telecomunicaciones					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE TELECOMUNICACIONES

EMPRESA:

	ESTIM.	REAL	DIF.
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO:			
REVISO:			

No.	PREGUNTA	RPT	SI	NO	N/A	OBSERVACIONES
21	La documentación se difunde entre los miembros de telecomunicaciones					
22	Existen planes y políticas para prevenir posibles contingencias					
23	Se difunden los planes y políticas similares en caso de contingencias					
24	Se revisan y actualizan con periodicidad los planes y políticas de contingencias					
25	Dentro de los planes y políticas de contingencias se consideran fenómenos naturales					
26	Dentro de los planes y políticas de contingencias se consideran fenómenos humanos internos					
27						
28	Dentro de los planes y políticas de contingencias se consideran fenómenos humanos externos					
29	Se cuenta con los contratos realizados para la adquisición de equipos para telecomunicaciones					
30						
31	En el contrato de adquisición de equipo de telecomunicaciones, se especifica la garantía que sobre el					
32	mismo proporciona el proveedor					
33	Dentro de los contratos están claramente definidos los pasos a seguir para reclamar la garantía del					
34	equipo y las condiciones de la misma					
35	Dentro de los contratos se especifican las erogaciones a las que está sujeta la garantía					
36	Dentro de los planes y políticas de contingencias se considera la recuperación de equipo de					
37	telecomunicaciones					
38	En el apartado para recuperación de equipo se especifican las funciones de personal de					
39	telecomunicaciones					
40	Se cuenta con inventario de equipo de telecomunicaciones					
41	Se realizan periódicamente revisiones físicas de inventario de telecomunicaciones					
42	Se actualiza periódicamente el inventario de telecomunicaciones					
43	Existen medidas y controles para evitar accesos no autorizados al equipo de telecomunicaciones					
44	Existen seguros y llaves para proteger las líneas telefónicas					
45	Se cuenta con seguros para el equipo que ya no está cubierto por garantía					
46	Los seguros cubren fenómenos naturales y humanos					
47	Se lleva un control de vencimiento de los seguros para su renovación					
48						
49	SEGURIDAD LOGICA DE TELECOMUNICACIONES					
50						
51	Existen políticas y procedimientos para el uso y manejo de la información de telecomunicaciones					
52	Se difunden las políticas y procedimientos para el uso y manejo de la información					
53	Se revisan y actualizan periódicamente las políticas para el uso y manejo de la información de					
54	telecomunicaciones					
55	Existen controles de las personas autorizadas para acceder a información de telecomunicaciones					
56						
57	Se revisan y actualizan periódicamente los controles de usuarios autorizados para acceder a					
58	Se tienen controles de los accesos a información de telecomunicaciones					

CUESTIONARIO DE CONTROL INTERNO
REVISION DE TELECOMUNICACIONES

EMPRESA:

	ESTIM.	REAL.	DIF.
TIEMPO			

	NOMBRE	FECHA	FIRMA
PREPARO			
REVISO			

No.	PREGUNTA	RPT.	SI	NO	N/A	OBSERVACIONES
2.1	Se auditan los controles de acceso a información de telecomunicaciones					
2.2	Se actualizan periódicamente los controles de acceso a la información de telecomunicaciones					
3.1	Existen dispositivos de seguridad para evitar accesos no autorizados a la información de telecomunicaciones					
3.1.1	Se revisan periódicamente los dispositivos de seguridad para evitar accesos no autorizados a la					
3.1.1	Se actualizan periódicamente los dispositivos de seguridad					
3.1.2	Los miembros de telecomunicaciones conocen el manejo de los dispositivos de seguridad					
3.1.3	Se imparte capacitación a los miembros de telecomunicaciones para manejo de las actualizaciones en					
3.1.4	Existen planes para la recuperación de información de telecomunicaciones					
3.1.5	Se encuentran documentados los planes para recuperación de información					
3.1.6	Se difunden los planes para la recuperación de información					
3.1.7	Dentro de los planes para recuperación de información se contemplan las funciones de los miembros de					
3.1.8	Se realizan simulacros sobre recuperación de información para verificar el buen funcionamiento de los					
3.1.9	Se revisan y actualizan periódicamente los planes para recuperación de información					

VII.4. DEFINICION DE PROCEDIMIENTOS DE AUDITORIA EN TELECOMUNICACIONES

1. ADMINISTRACION DE TELECOMUNICACIONES

PROC.1.1 Conocer y verificar los procedimientos y políticas para la administración de los recursos de telecomunicaciones, determinando su actualización y difusión.

PROC.1.2 Verificar que exista un encargado de la administración, evaluando los criterios utilizados para su selección.

PROC.1.3 Conocer las funciones del encargado de telecomunicaciones, verificando su documentación y difusión.

PROC.1.4 Entrevistar al encargado de telecomunicaciones, para verificar el grado de entendimiento de sus funciones.

PROC.1.5 Verificar que en los procedimientos de administración de telecomunicaciones, este contemplada la elaboración de reportes sobre el uso de las mismas.

PROC.1.6 Conocer el monitoreo de las telecomunicaciones, verificando la periodicidad y documentación de su realización.

PROC.1.7 Entrevistar a algunos usuarios de telecomunicaciones, verificando el grado de difusión que tienen los procedimientos y políticas de administración de telecomunicaciones entre ellos.

PROC.1.8 Conocer las sanciones definidas para la violación a los procedimientos y políticas establecidas de telecomunicaciones

PROC.1.9 Verificar que se lleve a cabo un análisis periódico sobre las violaciones a sistemas de telecomunicaciones.

PROC.1.10 Conocer y evaluar las políticas y criterios existentes para la selección del personal de telecomunicaciones.

PROC.1.11 Determinar las funciones y responsabilidades del personal de telecomunicaciones, verificando su participación en la implantación de sistemas de telecomunicaciones.

PROC.1.12 Verificar y analizar que dentro de las funciones administrativas de telecomunicaciones, se contemple su participación en el diseño y desarrollo de nuevas aplicaciones.

2. SEGURIDAD FISICA DE TELECOMUNICACIONES

PROC.2.1 Evaluar el lugar donde se encuentra la documentación sobre los sistemas de telecomunicaciones de la organización.

PROC.2.2 Conocer y verificar con que periodicidad se actualiza la documentación de los sistemas de telecomunicaciones.

PROC.2.3 Entrevistar a algunos miembros de telecomunicaciones, para determinar la difusión de la documentación sobre los sistemas de telecomunicaciones entre ellos.

PROC.2.4 Analizar y evaluar la existencia de planes y políticas para prevenir posibles contingencias sobre el equipo de telecomunicaciones.

PROC.2.5 Verificar que dentro de los planes y políticas de contingencias en telecomunicaciones, se contemplen fenómenos naturales.

PROC.2.6 Verificar que dentro de los planes y políticas de contingencias en telecomunicaciones, se contemplen fenómenos humanos intencionales e involuntarios.

PROC.2.7 Conocer los contratos con proveedores de telecomunicaciones, verificando las obligaciones y garantías sobre el equipo se ofrecieron.

PROC.2.8 Entrevistar a algunas personas de telecomunicaciones para determinar el grado de conocimiento sobre las políticas y procedimientos de recuperación de equipo en caso de contingencia.

PROC.2.9 Verificar que existan inventarios del equipo de telecomunicaciones, determinando la periodicidad con que se actualizan.

PROC.2.10 Verificar que periódicamente se realice una revisión física de los inventarios de telecomunicaciones.

PROC.2.11 Conocer y evaluar las medidas existentes para evitar el acceso a personas no autorizadas al equipo de telecomunicaciones.

PROC.2.12 Verificar y evaluar las llaves y seguros con los que se cuenta para proteger las líneas telefónicas.

PROC.2.13 Conocer y analizar los seguros con que se cubren los equipos que ya no cuentan con garantía.

3. SEGURIDAD LOGICA DE TELECOMUNICACIONES

PROC.3.1 Conocer y verificar la existencia de políticas y procedimientos que regulen el manejo y uso de información de telecomunicaciones.

PROC.3.2 Entrevistar a usuarios de telecomunicaciones para verificar la difusión de las políticas y procedimientos para el manejo y uso de información de telecomunicaciones, verificando el grado de conocimiento y claridad de las mismas.

PROC.3.3 Conocer y evaluar la actualización de las políticas y procedimientos del manejo y uso de información de telecomunicaciones.

PROC.3.4 Analizar y evaluar los controles sobre usuarios autorizados para accesar la información de telecomunicaciones.

PROC.3.5 Verificar y evaluar la periodicidad con la que se revisan y actualizan los controles de usuarios de telecomunicaciones.

PROC.3.6 Conocer y evaluar los controles existentes para el uso de información de telecomunicaciones.

PROC.3.7. Verificar que se actualicen periódicamente los controles para el uso de información de telecomunicaciones.

PROC.3.8 Conocer y evaluar los dispositivos de seguridad, para evitar accesos no autorizados a la información de telecomunicaciones.

PROC.3.9 Conocer y verificar la periodicidad con que se actualizan los dispositivos para seguridad de la información de telecomunicaciones.

PROC.3.10 Entrevistar a algunos miembros de telecomunicaciones, verificando su conocimiento sobre la operación y uso de los dispositivos de seguridad para información de telecomunicaciones.

PROC.3.11 Conocer y analizar, planes para respaldo y recuperación de información de telecomunicaciones.

PROC.3.12 Analizar y evaluar la periodicidad con que se actualizan los planes de respaldo y recuperación.

IX. PRESENTACION DE INFORME.

Terminada la auditoría en informática se procede a la elaboración de un documento que refleje todas las observaciones, debilidades, acciones de mejoramiento, plazos sugeridos para su realización, responsables y personas involucradas.

El orden y forma de este documento llamado también "Informe", puede variar de acuerdo con la creatividad y estilo de los auditores o de los estándares establecidos por el responsable de la auditoria.

El auditor en informática elabora formalmente este documento con el apoyo y asesoramiento del equipo de trabajo que participó en la revisión.

Una vez que un informe esta en proceso de elaboración se deben considerar los siguientes aspectos:

I) A QUIEN VA DIRIGIDO.

- Director o gerente general de la organización
- Director o gerente general de las arreas usuarias auditadas.
- Director o gerente general de informática.
- Director o gerente general de auditoria.

El informe deberá ser dirigido a los principales niveles de administración y operación de la organización como el área de informática, con la finalidad de que los resultados obtenidos de la revisión de informática sean conocidos y evaluados por la organización en general.

II) QUIENES REVISAN Y APRUEBAN EL DOCUMENTO.

- Director o gerente de las áreas usuarias auditadas.
- Director o gerente de auditoria.
- Director o gerente de informática.

Antes de presentar el "informe final" (FIG1 Y FIG2) o definitivo, es recomendable elaborar un "informe borrador" (FIG3 Y FIG4), con el cual las áreas auditadas y el responsable de la auditoria comentarán las observaciones, con el objeto de aclarar, modificar o eliminar cualquiera de ellas

III) REQUISITOS DEL INFORME.

A) Ser veraz.
B) Estar documentado formalmente.
C) Mostrar observaciones.
D) Tener recomendaciones y soluciones para observaciones.

A) Toda la información reflejada en el informe de auditoria en informática, debe ser verídica, de manera que se tomen consideraciones y conclusiones con la certeza de que los datos son reales y de buena fuente.

B) Todo el proceso de auditoría, incluso desde su planeación y justificación, debe estar documentado, ya que, el informe final es el resultado, de los datos registrados desde el inicio hasta el final del proyecto:

- Planes.
- Matriz de riesgos.
- Entrevistas aplicadas.
- Visitas.
- Cuestionarios aplicados.
- Observaciones.
- Recomendaciones.
- Revisiones formales e informales.
- Sugerencias y comentarios relevantes.
- Informe preliminar.

C) Cada una de las observaciones detectadas a lo largo del proceso de auditoría en informática deben ser documentadas en el informe; asimismo, se clasificarán por orden de importancia o impacto negativo que pueden tener en la organización si no se atienden oportunamente. Además, han de tener un significado relevante en los aspectos financieros, materiales, políticos, de control, procedimientos y seguridad.

Si se considera conveniente se deben exponer los motivos de estas debilidades u observaciones con el fin de aclarar responsabilidades y percibir los efectos que pueden llegar a tener en la organización.

Aquí es muy importante señalar que todas esas observaciones o debilidades se identificaron a lo largo del proyecto y que, de alguna manera, se comentaron con los responsables de las áreas o funciones que las originaron, excepto situaciones muy delicadas como fraudes o delitos graves contra la organización.

D)Todas las debilidades mencionadas en el informe han de tener una solución clara y contundente que comprenda la siguiente información:

- Observaciones.
- Acciones de mejoramiento.
- Plazos de implantación:
    - Inmediatos.
    - A corto plazo.
    - A mediano plazo.
    - A largo plazo.
- Responsables de cada acción.
- Involucrados:
- Usuarios.
- Alta dirección.
- Informática.
- Auditoria.
- Auditoria en informática.
- Asesores externos.
- Otros.

SEGUIMIENTO DEL INFORME.

La empresa debe decir con cuál de las siguientes alternativas se asegurará, que se dé cumplimiento oportuno a los compromisos y tareas que resulten del informe de Auditoria en Informática:

a) Auditores internos.
b) Auditores externos.
c) Ambas alternativas.

La importancia de que se dé seguimiento formal estriba en que los gastos y tiempos incurridos en el proyecto de auditoria sólo serán reflejados en beneficios tangibles una vez ejecutadas ala pie de la letra, las medidas seguidas por el auditor de informática a través de políticas y procedimientos acordes a las necesidades de la organización.

Es recomendable realizar un informe posterior a la implantación que brinde la garantía de que todo fue satisfactorio, o en caso contrario indique las medidas correctivas pertinentes

FECHA _____

INFORME FINAL
NO _____

AT'N Director General
Gerente General
PRESENTE

Adjunto al presente envio el informe definitivo de Auditoria el cual fue comentado con usted en el que se indican las observaciones y sugerencias derivadas de la revisión efectuada a _____ durante el periodo del _____ al _____, esperando se cumpla con las fechas pactadas para la implantación de las sugerencias señaladas en el mismo

OPINION DE AUDITORIA

FIG 1

INFORME FINAL

EMPRESA: FECHA:

OBSERVACION	CONSECUENCIA	SUGERENCIA	FECHA COMPROMISO

FIG. 2

EMPRESA _____

NOMBRE DEL DIRECTOR O GERENTE GENERAL _____

_____

NOMBRE DEL DIRECTOR O GERENTE DE INFORMATICA _____

_____

CLAVE DE TRABAJO ☐☐☐☐☐

RESPONSABLE DE LA AUDITORIA _____

TIPO DE REVISION

☐ ADMINISTRACION

☐ CONTROLES EN REDES

☐ EQUIPOS PERSONALES

☐ DESARROLLO DE SISTEMAS

☐ TELECOMUNICACIONES

FECHA DE INICIO DE LA REVISION _____

FECHA DE TERMINO DE LA REVISION _____

GRUPO RESPONSABLE

_____

_____

_____

_____

_____

FIG 3

INFORME BORRADOR

EMPRESA: FECHA:

OBSERVACION	CONSECUENCIA	SUGERENCIA	FECHA COMPROMISO

FIG. 4

CONCLUSIONES.

La auditoria informática representa, una transición sobre la trayectoria profesional del Licenciado en Informática. Desde un principio el contacto con esta actividad requiere de cambios significativos en actitud y en la visión de las organizaciones y sus instalaciones de cómputo. Sencillamente, no es lo mismo actuar como el "desarrollador" en plena búsqueda de la perfección algoritmica de sus aplicaciones, que fungir como el "evaluador" objetivo e independiente, capaz de identificar debilidades de control en el uso de los recursos informáticos.

En este sentido, la filosofía de control requerida por el auditor también plantea la necesidad de conocer y asimilar una variedad de conceptos desconocidos y pertenecientes a otras disciplinas como Administración y Contabilidad. Sin embargo, la Informática es verdaderamente sorprendente como una función, que en apariencia pertenece al terreno de la técnica y la "automatización" encontrando su fundamentación a partir de los cánones establecidos por una rama administrativa.

Dentro de una empresa resulta igualmente interesante y problemático el concebir a una organización como un ente socioeconómico expuesto a infinidad de riesgos y amenazas, que bien podrían traducirse en pérdidas de dinero, en la destrucción parcial o total de sus activos, en la interrupción de sus operaciones o en su irrevocable desaparición. Por ello, en la generalidad de los casos, la tarea mas difícil para el auditor consiste precisamente en identificar los riesgos existentes y los controles requeridos para evitarlos y cuyas consecuencias pueden ser aún mas catastróficas.

Es importante mencionar que el principal objetivo de una revisión en Informática, es lograr un centro de cómputo que cuenta con una infraestructura tecnológica de hardware y software acorde con las necesidades operativas de la empresa y con un grupo de profesionales altamente calificados. Sin embargo, estos elementos pueden llegar a convertirse en condiciones irrelevantes, en tanto las organizaciones no procuren el establecimiento de un sistema de control interno tendiente a la salvaguarda de los activos informáticos, a elevar el nivel de integridad de los datos y a promover la efectividad y eficiencia de las aplicaciones desarrolladas.

La tecnología continúa evolucionando a ritmo acelerado, teniendo los auditores como principal reto, mantenerse actualizados con los nuevos avances tecnológicos y en desarrollar metodologías viables para la auditoria y control de sistemas computarizados. Sin embargo, esta evolución también ha provisto al auditor de poderosas herramientas de software que promueven una mayor eficiencia durante todo el proceso de evaluación. Estas técnicas de auditoria apoyadas por computadora, seguirán perfeccionándose predominando en el futuro, así sin lugar a dudas, el continuo refinamiento técnico procurado por esta novedosa disciplina como los programas de certificación establecidos por algunas asociaciones con renombrado prestigio contribuirán de maneras decisiva en la formación de mejores profesionales, preparados para enfrentar y controlar la era de la tecnología de información.

BIBLIOGRAFIA

AUDITORIA
JOHN W. COOK, PH. D., C.P.A. Y
GARY M. WINKLE
3ª EDICION
EDITORIAL MC. GRAW HILL
GEORGIA STATE UNIVERSITY, 1987.

ELEMENTOS DE AUDITORIA
VICTOR MANUEL MENDIVIL ESCALANTE
DUODECIMA REIMPRESION
EDITORIAL ECASA
MEXICO, 1993.

CUESTIONES FUNDAMENTALES DE AUDITORIA
ENRIQUE FOWLER NEWTON
EDITORIAL TESIS
BUENOS AIRES, REPUBLICA DE ARGENTINA, 1989.

AUDITORIA I
C.P. ISRAEL OSORIO SANCHEZ
DECIMA SEPTIMA REIMPRESION
EDITORIAL ECASA
MEXICO, 1994.

CONCEPTOS GENERALES DE AUDITORIA
SANTIAGO LAZZATI
HUGO O. DE LA TORRE
EDICIONES MACCHI
ARGENTINA, 1991.

AUDITORIA MONTGOMERY
PHILIP L. DEFLIESE C.P.S.
SEGUNDA EDICION
EDITORIAL LIMUSA
MEXICO, 1991.

NORMAS Y PROCEDIMIENTOS DE AUDITORIA
TOMO I Y II
DUODECIMA QUINTA EDICION
INSTITUTO MEXICANO DE CONTADORES PUBLICOS
MEXICO, 1995.

AUDIT MANAGEMENT AND SUPERVISION
GIL COURTEMANCHE
EDITORIAL WILEY
1996.

AUDITORIA OPERACIONAL
EL EXAMEN DE FLUJO DE TRANSACCIONES
GABRIEL SANCHEZ CURIEL
EDITORIAL ECASA
MEXICO, 1993.

AUDITORIA EN INFORMATICA
JOSE ANTONIO ECHENIQUE GARCIA
EDITORIAL MC GRAW HILL
MEXICO, 1995.