UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA INDUSTRIAL

" DISEÑO DE UNA METODOLOGIA PARA LA AUDITORIA DE SISTEMAS INFORMATICOS "

TRABAJO DE GRADUACION PRESENTADO POR

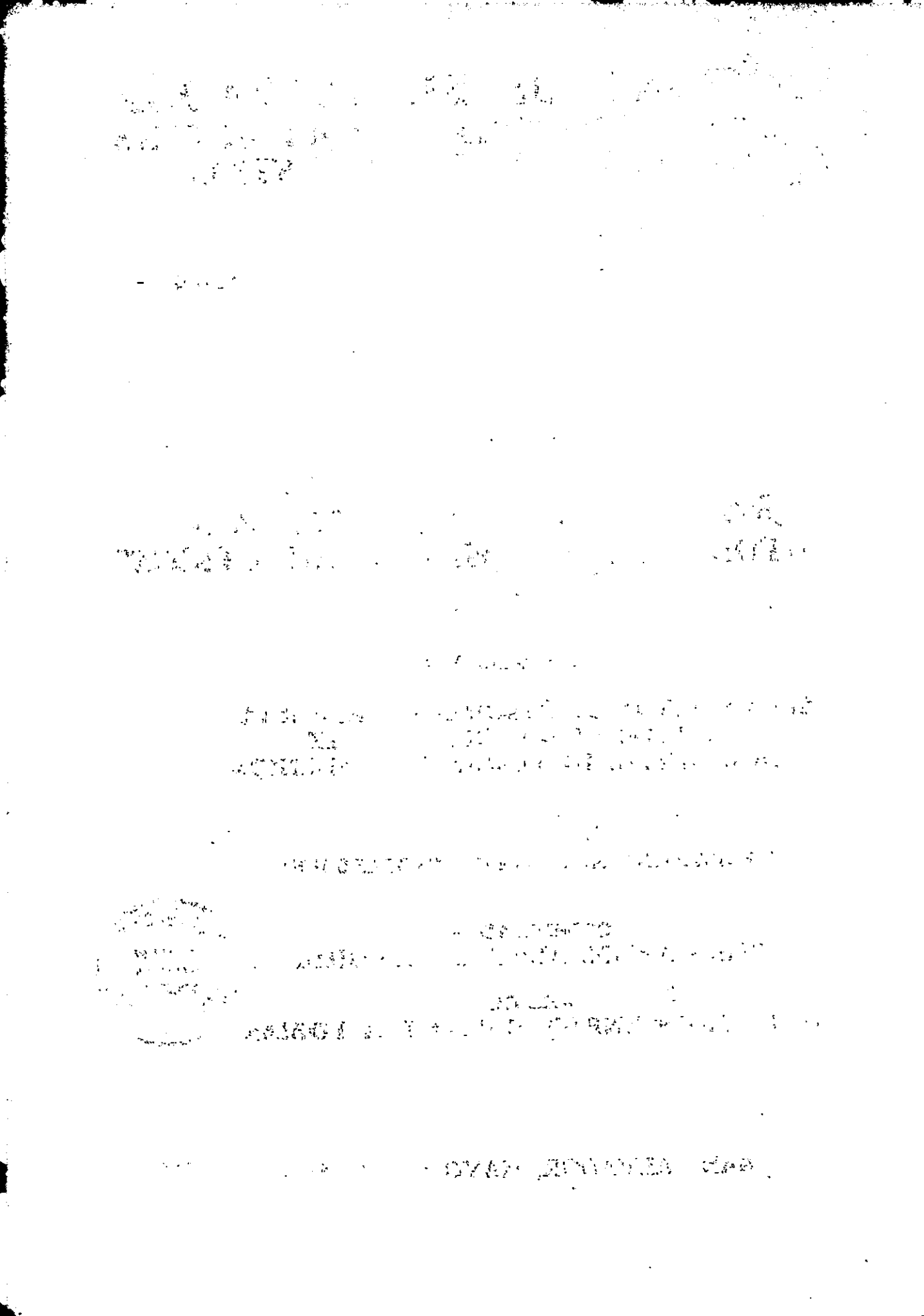
SALVADOR IVAN TESORERO VALENCIA
ROMULO CESAR CHEVEZ PAZ
NELSON ANTONIO TESORERO VALENCIA

PARA OPTAR AL TITULO DE

INGENIERO INDUSTRIAL

MAYO DE 1994

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA



UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA INDUSTRIAL

TRABAJO DE GRADUACION PREVIO A LA OPCION AL GRADO DE

INGENIERO INDUSTRIAL

TITULO

"DISEÑO DE UNA METODOLOGIA PARA LA AUDITORIA DE SISTEMAS INFORMATICOS"

PRESENTADO POR

SALVADOR IVAN TESORERO VALENCIA
ROMULO CESAR CHEVEZ PAZ
NELSON ANTONIO TESORERO VALENCIA

TRABAJO DE GRADUACION APROBADO POR

COORDINADOR
ING. CARLOS ALEGRIA ALEGRIA

ASESOR
ING. JORGE ENRIQUE IRAHETA TOBIAS

SAN SALVADOR, MAYO DE 1994

UNIVERSIDAD DE EL SALVADOR

RECTOR

DR. FABIO CASTILLO FIGUEROA

SECRETARIO GENERAL

LIC. MIRNA ANTONIETA PERLA DE ANAYA

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO

ING. JOAQUIN ALBERTO VANEGAS AGUILAR

SECRETARIO

ING. JOSE RIGOBERTO MURILLO CAMPOS

ESCUELA DE INGENIERIA INDUSTRIAL

DIRECTOR

ING. OSCAR RENE MONGE

ESCUELA DE INGENIERIA INDUSTRIAL

DEDICATORIA

DIOS TODO PODEROSO, A NUESTROS PADRES Y A TODAS AQUELLAS RSONAS DE LAS QUE RECIBIMOS APOYO EN LA REALIZACIÓN DE NUESTRO ABAJO DE GRADUACIÓN.

CESAR, SALVADOR Y NELSON.

INDICE

TERCERA PARTE

DISEÑO DE LA METODOLOGÍA PARA

AUDITAR SISTEMAS INFORMATICOS

INTRODUCCIÓN

El presente documento contiene el " Diseño de una Metodología para Auditar Sistemas Informáticos ", metodología que cuenta con los procedimientos necesarios para que cualquier organización que posea sistemas informáticos y desee auditarlos, pueda efectuar esta labor de manera satisfactoria.

Este informe se divide en cuatro partes: 1) Antecedentes y Planteamiento del problema, 2) Conceptualización de los elementos de los sistemas informáticos, 3) Diseño de la Metodología para Auditar Sistemas Informáticos, y 4) La evaluación.

La primera parte consiste de algunas generalidades interesantes acerca de la Auditoría de Sistemas Informáticos y plantea la problemática existente en nuestro país en este sentido.

La segunda parte plantea los lineamientos fundamentales del diseño de la metodología, y se apoya de muchos esquemas para clarificar las conceptualizaciones.

La tercera parte es el diseño en sí de la metodología, contiene todos los procedimientos, metodologías e instrumentos que son necesarios para ejecutar una auditoría de sistemas de manera profesional. En este apartado se lleva de la mano al auditor, proporcionándole la metodología que necesitará incluso

al momento de planificar sus actividades y organizar un departamento de Auditoria de sistemas, además se encuentra documentación acerca de los papeles de trabajo que el auditor necesitará.

La cuarta y última parte es referente a la evaluación económica y social de esta metodologia.

Al final del documento se encuentran conclusiones, recomendaciones, la bibliografía, los anexos y el glosario de términos técnicos.

OBJETIVOS

OBJETIVO GENERAL

Diseñar la metodología para realizar Auditoría sobre Sistemas Informáticos, que permita evaluar las funciones de salvaguardar los activos de información, de mantener la integridad de la información y de lograr la efectividad y de lograr la efectividad y eficiencia de los Sistemas de Información.

OBJETIVOS ESPECÍFICOS

- Identificar y plantear la problemática existente en nuestro medio, en torno a la situación de la Auditoría de Sistemas.
- Conceptualizar la Metodología para Auditar Sistemas Informáticos, que involucre todos y cada uno de los elementos que forman dichos sistemas, incluyendo el entorno de su administración.
- Establecer la forma en que el Auditor de sistemas habrá de planificar el desarrollo de sus actividades.
- Definir el modelo de organización a través del cual el equipo encargado de la Auditoría se habrá de interrelacionar.
- Establecer el contenido, importancia y uso de los papeles de trabajo en la Auditoría de Sistemas Informáticos .

- Diseñar detalladamente, todos los procedimientos necesarios para Auditar el entorno de la administración de los Sistemas Informáticos.
- Realizar el diseño detallado de todos los procedimientos necesarios para Auditar al sistema Informático, es decir los instrumentos que servirán para auditar los subsistemas de entradas, procesos, salidas, bases de datos y comunicaciones del sistema.
- Presentar una guía para la elaboración de los resultados de la aplicación de la metodología.
- Determinar los beneficios económicos, producto del diseño de esta metodología.

ALCANCES Y LIMITACIONES

ALCANCES

En este documento de establece la metodología para ejecutar auditoría sobre sistemas informáticos. La aplicación de la metodología comprenderá desde la evaluación de las entradas de un sistema informático hasta los resultados que se tienen de el, examinando los procesos que están involucrados y el entorno de la administración del sistema.

Una vez realizada esta evaluación, se podrán emitir juicios acerca de la veracidad, exactitud, privacidad, eficiencia, efectividad y seguridad de manejo de la información del sistema informático.

La metodología se podrá efectuar sobre Sistemas Informáticos de toda magnitud y cualquier función.

LIMITACIONES

- Esta metodología podrá ser aplicada únicamente para sistemas informáticos.
- Es necesario que la persona que requiera aplicar esta metodología, conozca el sistema informático que desea auditar y el entorno del mencionado sistema.
- Los resultados de la aplicación de la metodología, deben ser entregados a la persona de más alto nivel jerárquico de

la organización, para que tome las acciones correspondientes.

- Debido a que la metodología es un instrumento de evaluación de sistemas informáticos, es necesario que la persona interesada en aplicarla posea conocimientos de computación en relación al software y hardware del sistema informático que auditará, y sólidos conocimientos en cuanto a la administración de sistemas.
- La realización de la Auditoría de Sistemas Informáticos podría no ser objetiva, si la persona quien ejecuta la metodología, no es lo suficientemente independiente del sistema informático que esté auditando.

PRIMERA PARTE

ANTECEDENTES Y PLANTEAMIENTO DEL PROBLEMA

1. ANTECEDENTES

Las operaciones de los negocios de nuestro país, se mezclan cada día más con la informática, especialmente porque el alto desarrollo tecnológico de esta ciencia en otros países ofrece una gran gama de posibilidades.

Es evidente que todo Sistema Informático tiene un propósito; pero en El Salvador muy pocas personas y empresas se han cuestionado si dicho propósito se ha alcanzado en forma satisfactoria. A pesar de que la Auditoría de Sistemas Informáticos se encarga de lo anterior, y de que en otros países es una disciplina muy refinada, en nuestro medio solo el sector bancario, empresas grandes (por lo general multinacionales) y los grandes consorcios se han preocupado por aplicarla.

En la actualidad, muy poca orientación se tiene en este sentido por parte de las mismas firmas de auditoría, por los colegios profesionales y por las universidades de nuestro país.

En muchos casos, los errores producidos por sistemas mecanizados, han generado en los usuarios una conducta negativa hacia el uso del computador. El resultado es la subutilización o eliminación de los sistemas informáticos y por ende la pérdida de la inversión que se hizo para lograr la implementación de estos, y el retroceso a procedimientos ineficientes y obsoletos.

Es necesario evaluar los sistemas informáticos a través de una Auditoría, porque muchas veces las causas de sus problemas

son, entre otras, la falta de conocimientos técnicos por parte del personal, la defectuosa aplicación de los recursos técnicos, mantenimiento deficiente o trato indebido a los diversos componentes del equipo, condiciones físicas inapropiadas para el sistema informático, inadecuado acoplamiento de sistemas, conservación inconveniente de la documentación, errores en el proceso (y su ocultamiento), falta de unidad y trabajo en equipo, etc. lo que podría llevar al sistema informático a no cumplir óptimamente sus objetivos.

2. PLANTEAMIENTO DEL PROBLEMA

La mayoría de las empresas de nuestro país, no tienen a su alcance una metodología que les permita realizar una auditoría de sus sistemas informáticos, a partir de la cual puedan identificar aquellos aspectos que no permiten que los sistemas informáticos logren sus objetivos óptimamente, o bien, tener una garantía para confiar en los resultados de estos.

2.1 PERSPECTIVA DE LA AUDITORÍA DE SISTEMAS Y LA AUDITORÍA GENERAL

La Auditoría de Sistemas Informáticos es un proceso especializado que está íntimamente relacionado con el concepto básico de la auditoría.

Este capítulo muestra aspectos esenciales de la auditoría tales como su definición genérica, objetivos, procedimientos, técnicas de auditoría, etc. con el objetivo de aclarar que toda la estructura, principios, instrumentos y técnicas utilizadas en la metodología cumplen con los principios y normas de la auditoría de Sistemas Informáticos. Además cumple con los requisitos que exige la máxima autoridad en esta materia, es decir, **The EDP Auditing System.**

El desarrollo de este acápite se estructura con la definición general de auditoría, estudio de las normas y principios; objetivos de la auditoría siguiendo con la definición de Auditoría de Sistemas Informáticos con sus reglas y normas.

DEFINICIÓN

Auditoría es una revisión crítica y exploratoria que hace el encargado de auditar, a los métodos y registros de una empresa (el objeto de estudio depende del tipo de auditoría, es decir si

es operacional, administrativa, etc.), llevada a cabo de tal manera, que le permita expresar una opinión respecto a si el objeto de audito refleja o no su posición y resultados de operación.

Las normas generales de auditoría son:

1. El examen se llevará a cabo por una persona o personas que posean preparación técnica adecuada, y experiencia o capacidad como auditores.
2. En todas los asuntos relacionados con la revisión, el auditor o auditores deben mantener una actitud de independencia mental.
3. Debe aplicarse el debido cuidado y diligencia profesional al practicar el examen y preparar el informe.

Normas de ejecución.

1. El trabajo debe realizarse en forma adecuada y los ayudantes, si los hay, deben supervisarse apropiadamente.
2. Se practicará un estudio y evaluación apropiada del control interno existente como base para la seguridad en el mismo y para la determinación de la extensión resultante, de la

pruebas a alá cuales se restringirán los procedimientos de auditoría.

3. Debe obtenerse material probatorio competente y suficiente, mediante la inspección, observación, investigación y confirmación con objeto de proporcionar una base razonable para una opinión con relación a los estados financieros bajo estudio.

Normas de dictamen.

1. Aclaración de la relación con los documentos del objeto de áudito y la responsabilidad asumida con respecto a ellos.
2. Aplicación de principios.
3. Consistencia en la aplicación.
4. Salvedades.
5. Abstención de opinión.

TÉCNICAS DE AUDITORÍA

Para obtener la información que necesita y poder cerciorarse de la autenticidad de los sistemas objetos de áudito, el profesional independiente necesita realizar investigaciones que, en último resultado, tiendan a darle la convicción que requiere como base de su opinión. Los métodos prácticas de investigación y prueba que el auditor utiliza para lograr la información y

comprobación necesarias para su opinión se denominan técnicas de auditoría.

Las técnicas de auditoría, debido a la variación de circunstancias en que el auditor realiza su trabajo y a la diversidad de condiciones de las empresas que se someten al examen del auditor son de muy diversas clases, pero puede agruparse bajo los siguientes rubros:

a) Estudio General.

b) Análisis.

c) Inspección.

d) Conformación.

f) Investigación.

g) Declaraciones o certificaciones.

h) Observación.

i) Cálculo

TIPOS DE AUDITORIA MAS FRECUENTES

a) Auditoría financiera.

b) Auditoría gerencial.

c) Auditoría operacional.

d) Auditoría de la función de control interno.

f) Auditoría de especializadas.

DEFINICIÓN DE AUDITORIA DE SISTEMAS INFORMÁTICOS.

"La auditoría de sistemas de información se define como cualquier auditoría que guía a la revisión y evaluación de todos los aspectos (o cualquier parte) de un sistema automatizados que están relacionados, y las interfases entre ellos.

Los auditores de sistemas de información revisan y evalúan el desarrollo, mantenimiento, y operación de los diferentes componentes en los sistemas automatizados(o dichos sistemas como un todo) y sus interfases con las áreas no automatizadas de las operaciones de la organización. Los objetivos de dicha auditoría son generalmente asesorar hasta que punto dichos sistemas o componentes producen información precisa y confiable y determinan si dicha información está de acuerdo con los requerimientos gerenciales y cualquier provisión aplicable."

Interrelación .

Para que un profesional llegue al convencimiento total de la confiabilidad de la metodología debe estudiar las técnicas, instrumentos, procedimientos y todos aquellos elementos que involucran la auditoría; luego debe estudiar la metodología y evaluar cada instrumento. Por ejemplo, al evaluar los objetivos del P.E.D. el auditor debe con anticipación planear la evaluación, es decir, determinar en tiempo y espacio el momento

adecuado para llevar acabo la auditoría, además de precisar los recursos y el alcance de la auditoría. Luego es importante tener la evidencia adecuada y necesaria, por consiguiente se procede a la recopilación de los papeles de trabajo, para que en una etapa posterior se estudie dichos papeles. La forma de evaluar cada subsistema es contestando al instrumento diseñado, analizando la información recolectada, examinando cada respuesta y diagnóstico reflejado por el instrumento para formarse un juicio de la situación actual del sistema informático. En la auditoría general existen instrumentos que recopilan información éstos puede ser cuestionarios, formularios con estándares, documentos de índole financiera, organizacional etc. La metodología hace uso de varios instrumentos de la misma naturaleza. Por lo tanto si los otros tipos de auditorías generan recomendaciones profesionales en base a esto la metodología posee una alta calidad en sus procedimientos e instrumentos utilizados y es homogénea con los principios de la auditoría en general.

La confrontación de la definición general de la auditoría se observa más cercana en los instrumentos al ser éstos una revisión crítica por su grado de objetividad y exploratoria porque cada pregunta o elemento considerado posee un grado de profundidad muy detallado.

Para lograr un grado mayor de objetividad se ha optado por

comparar en paralelo las normas de la auditoria con la metodologia, asi pues:

1. Para la norma general que menciona caracteristicas del auditor en cuanto a su preparación técnica y experiencia, en la metodologia se presenta el perfil del auditor para que la institución que desee hacer uso de la metodologia e implementar un departamento de esta índole se guie al seleccionar la persona idónea para el puesto.
2. El auditor de sistemas debe estar consciente de mantener una actitud de independencia mental. En la metodologia se recomienda dicha actitud.
3. Para aplicar con debido cuidado el examen la metodologia posee un capitulo completo de planificación de la misma para poder hacer la diligencia con profesionalismo.
4. Pasando a las normas de ejecución; la primera norma de ellas, se respalda en la metodologia con la presentación de las funciones de los auditores del entorno administrativo y del sistema informático, y que además contienen la forma de supervisarse apropiadamente.
5. En la segunda norma de la auditoria se presenta la necesidad de un estudio y evaluación apropiada del

control interno existente; en el diseño en la planificación de la auditoria existe un apartado que se titula investigación preliminar, en donde presenta información necesaria a recopilar para el análisis del control interno de la empresa.

6. Todo el material competente y suficiente para probar un estado determinado del sistema se especifica en cada instrumento de evaluación.

7. Para las normas de dictamen; en la metodología existe un apartado para la forma en que debe presentarse la información.

SEGUNDA PARTE

CONCEPTUALIZACION DE LOS ELEMENTOS DE EL SISTEMA INFORMATICO

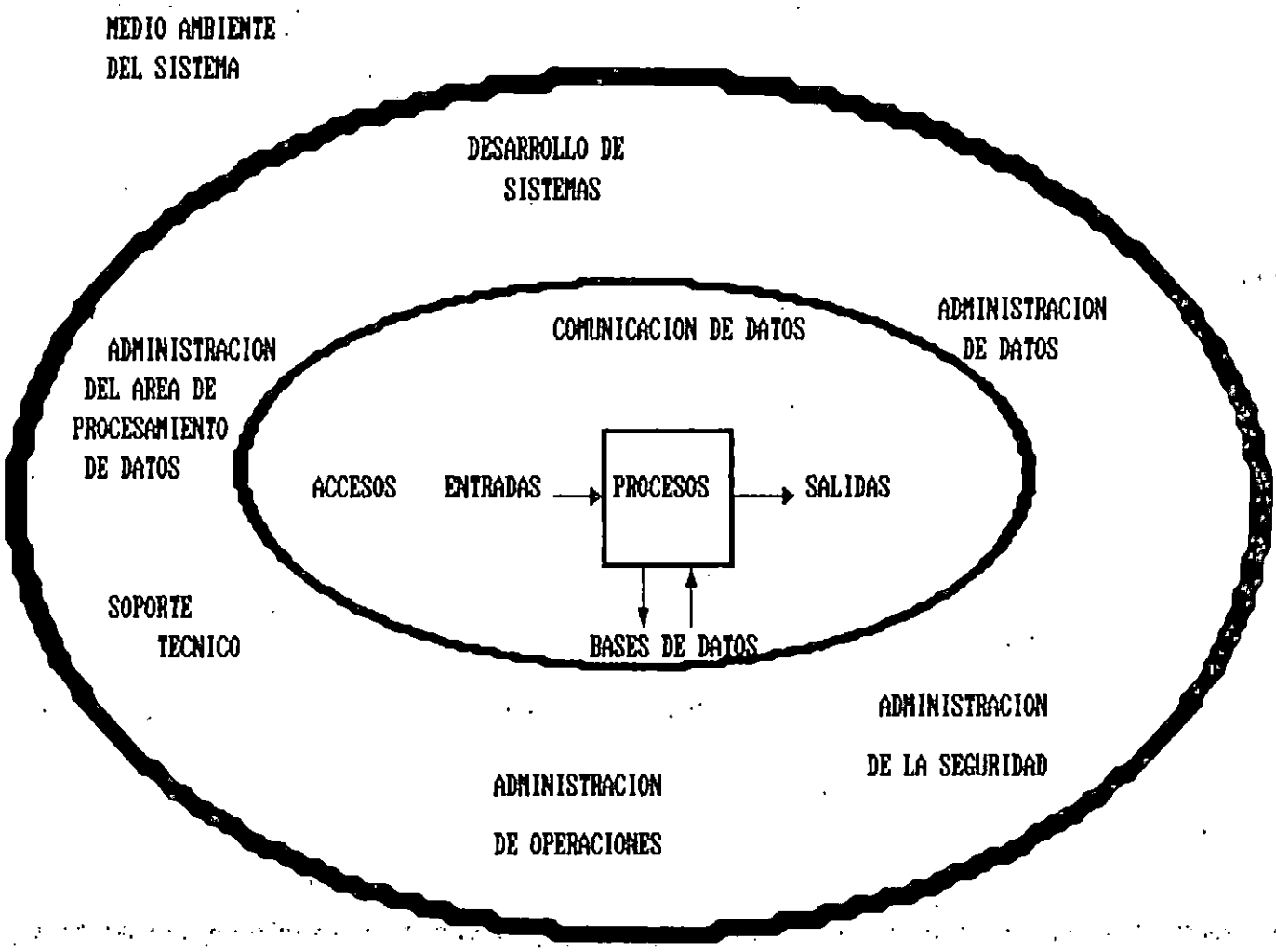
3. CONCEPTUALIZACIÓN DEL ENTORNO ADMINISTRATIVO DEL SISTEMA INFORMÁTICO

3.1 EL ENTORNO ADMINISTRATIVO

El entorno administrativo que está formado por aquellos elementos de carácter operacional en relación a las funciones de administración del centro de procesamiento electrónico de datos se esquematizan en el gráfico que aparece a continuación. Es indispensable aclarar que el método utilizado aquí no es un organigrama ni un flujograma, es mas bien una representación del conjunto de subsistemas que constituyen el entorno administrativo.

Para efectos de la auditoría; cada gráfico se estructura con sistemas que están conformados en varios niveles por subsistemas llegando hasta el punto de colocar el elemento a evaluar y que el detalle de éste es el instrumento utilizado para examinarlo.

En la página siguiente se muestra el modelo gráfico del subsistema para la auditoría (figura. 1).



ELEMENTOS DEL SISTEMA INFORMATICO Y SU ENTORNO

FIGURA 1

3.2 CONCEPTUALIZACIÓN A LA AUDITORIA DE LA ADMINISTRACIÓN DEL ÁREA DE PROCESAMIENTO DE DATOS.

Para la auditoría de la administración, particularmente, se muestra en el modelo gráfico tres grandes funciones, que a su vez serán divididos en caracteristicas que culminan en un instrumento que evalúa un conjunto de elementos que conforman las funciones. Por ello la estructura de la administración se muestra en la figura 2 .

Generalmente la administración del centro de procesamiento de datos posee un comité coordinador de actividades; es posible que no esté definido de esa forma, pero su inexistencia es inevitable. En cualquier caso, este comité es el responsable de la planificación de las funciones del centro de procesamiento de datos (ver detalle en figura 3) .

Un esquema de la evaluación de proyección y la del centro de procesamiento de datos se muestran en las figura 4.

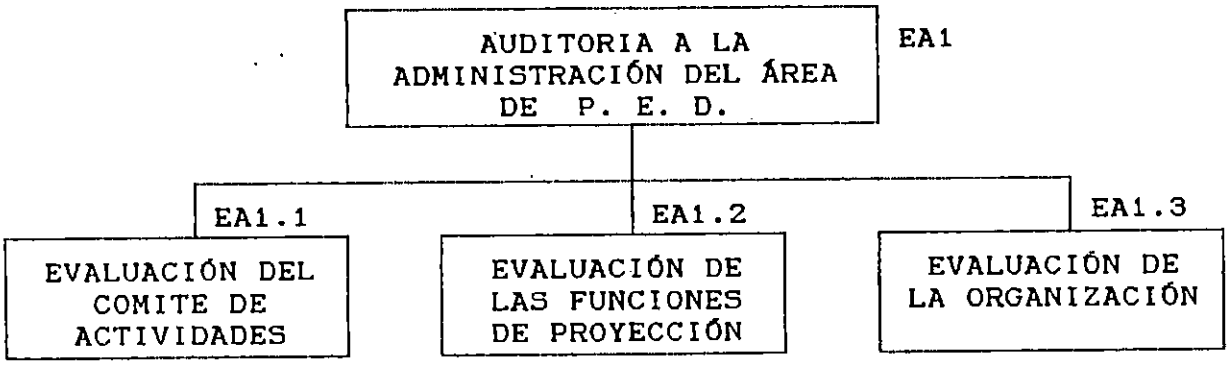


Figura 2. El esquema muestra los aspectos que se han de evaluar con respecto a la Administración del Area de Procesamiento Electrónico de Datos (PED). (EA Significa entorno Administrativo).

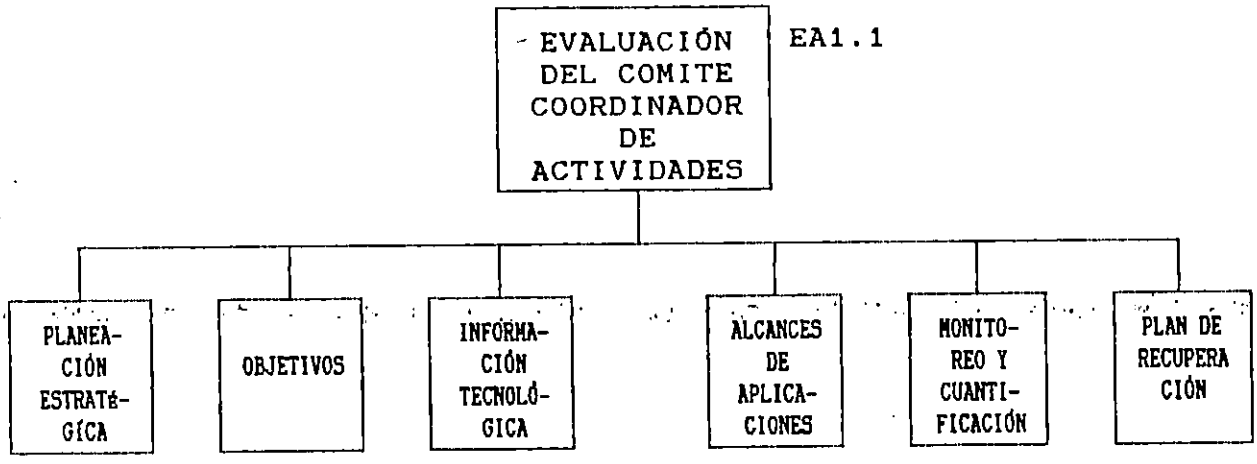


Figura 3. Evaluación al Comité coordinador de las actividades del Procesamiento Electrónico de datos.

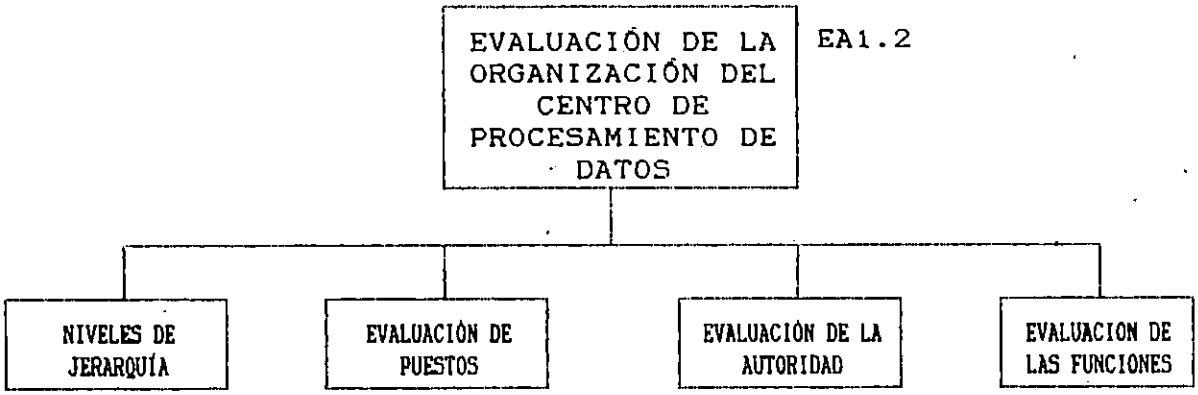


Figura 4. Evaluación de la Organización del Centro de Procesamiento de Datos: Este modelo representa la estructura de evaluación.

3.3 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE DESARROLLO DE SISTEMAS

La conceptualización de la auditoria al subsistema de comunicaciones se realiza a las actividades propias del desarrollo de sistemas, las cuales son Planeación del desarrollo, Especificaciones del usuario, Especificaciones Técnicas, Planeación de la implantación, Programación, Procedimientos, Pruebas del sistema, Revisión y Mantenimiento.

Para mayor claridad, véase en la siguiente página (figura 5) el esquema de la conceptualización de la auditoria al subsistema de Desarrollo de Sistemas.

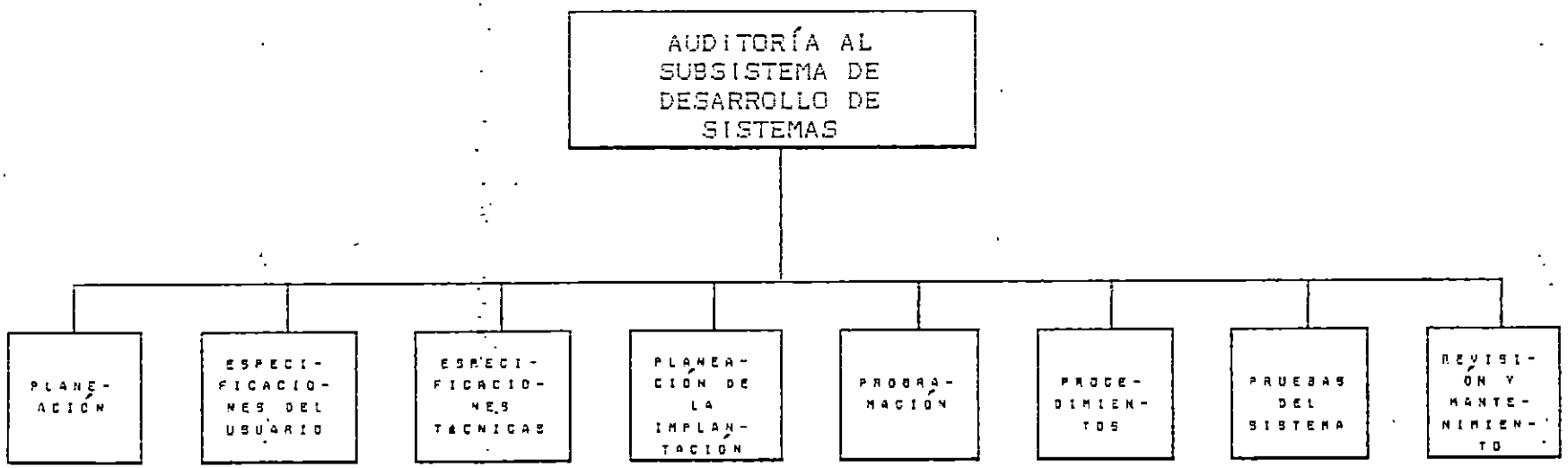


Figura 5. El esquema muestra los aspectos que se auditarán en lo referente al Desarrollo de Sistemas.

3.4 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE ADMINISTRACIÓN DE DATOS

La administración de datos tiene una característica importante que debe ser considerada: La función del administrador de la base de datos (DBA) y el administrador de datos (DA), evaluando la integridad de la base de datos y las funciones del DA y DBA.

Para mayor claridad, véase en la siguiente página (figura 6) el esquema de la conceptualización de la auditoría al subsistema de Administración de Datos.

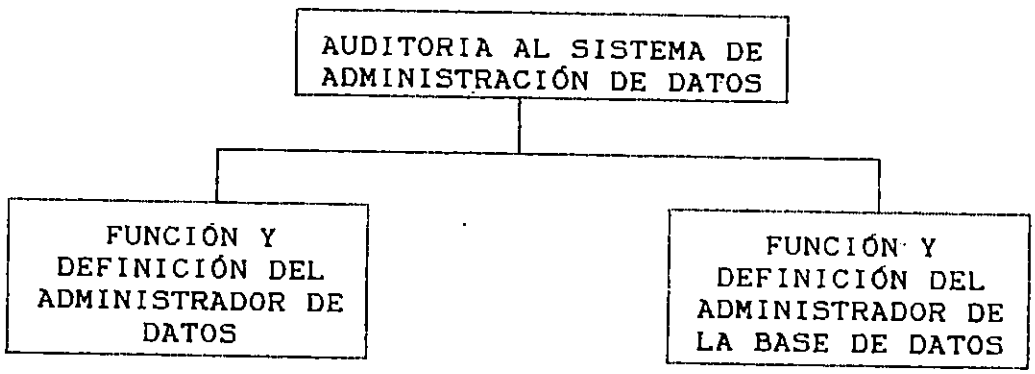


Figura 6. Conceptualización de la Auditoría al Subsistema de Administración de Datos.

3.5 CONCEPTUALIZACIÓN DEL SUBSISTEMA DE ADMINISTRACIÓN DE SEGURIDAD

La seguridad de un centro de procesamiento de datos es de vital importancia debido a la delicadeza de los datos que un departamento maneja.

La seguridad del centro de procesamiento de datos es considerada en este metodología en tres puntos de vista muy importantes, los cuales son : la evaluación de la seguridad física, el estudio de la seguridad del aspecto lógico del departamento y los planes de contingencia.

Es indispensable establecer que las medidas de seguridad se rigen en base a tres estrategias : confinamiento, reglamentación y cifrado de la información.

El confinamiento es el acto de alojar los datos en una ubicación física a la que no se tenga fácil acceso personas no autorizadas. La reglamentación es la determinación de los usuarios que tienen acceso a los datos así puestos a cubierto.

El cifrado consiste en desordenar los datos de acuerdo a reglas predeterminadas de transformación de suerte que carezcan de sentido para quienes no pueden volverlos a ordenar. Ver figura 7 para mayor claridad.

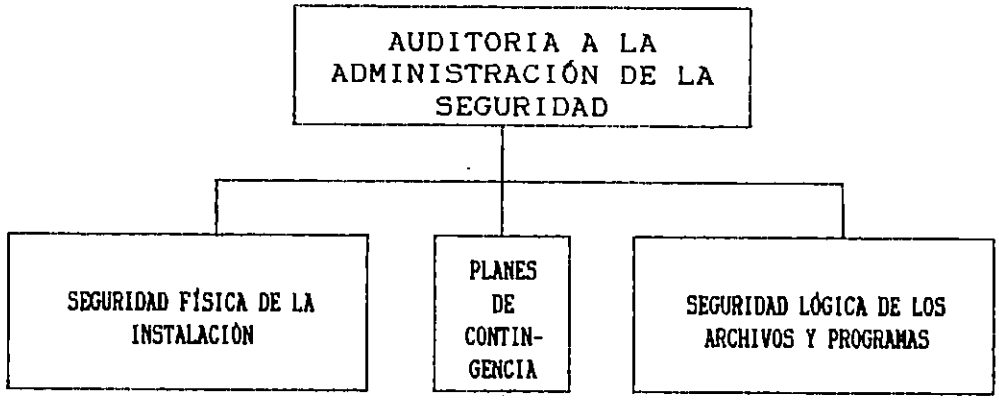


Figura 7. Este esquema muestra los dos subgrupos en que se divide la evaluación de la Administración de la Seguridad.

3.6 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE ADMINISTRACIÓN DE OPERACIONES

La administración de operaciones es responsable por el funcionamiento de las instalaciones de procesamiento de datos, de tal manera que las aplicaciones puedan funcionar correctamente y el personal realice normalmente sus funciones. Existen cuatro áreas a las que se identifican: Funciones de la Administración de Operaciones, flujo de información, medios de almacenamiento, manuales y documentos.

Para mayor claridad, véase en la siguiente página (figura 8) el esquema de la conceptualización de la auditoría al subsistema de Administración de Operaciones.

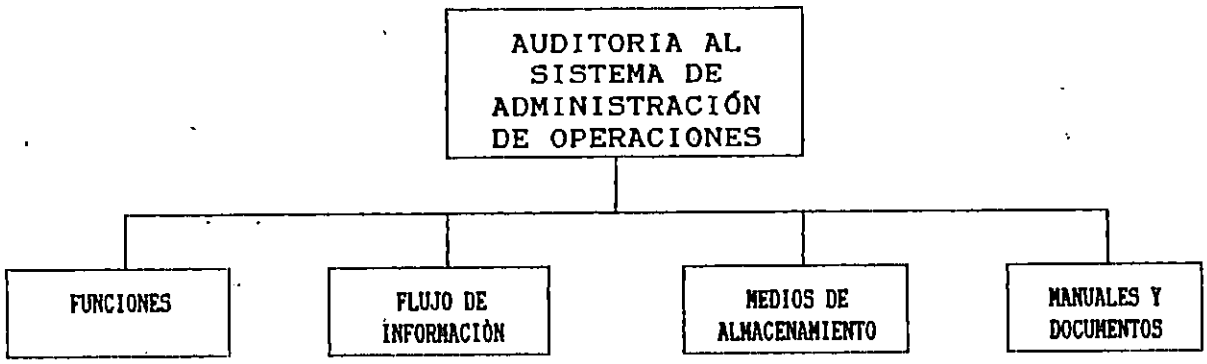


Figura 8. El esquema muestra los grupos de elementos que han de auditarse dentro del subsistema de Administración de Operaciones.

3.7 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE SOPORTE TÉCNICO

La conceptualización de la auditoría al subsistema de Soporte Técnico evaluará el desarrollo y mantenimiento de programas y procesos que interactuan con los programas de soporte al sistema. Todo relacionado al sistema operativo, funcionamiento de la red de comunicaciones, herramientas de desarrollo y el paquete administrador e la base de datos.

Para mayor claridad, véase en la figura 9 el esquema de la conceptualización de la auditoría al subsistema de Soporte Técnico.

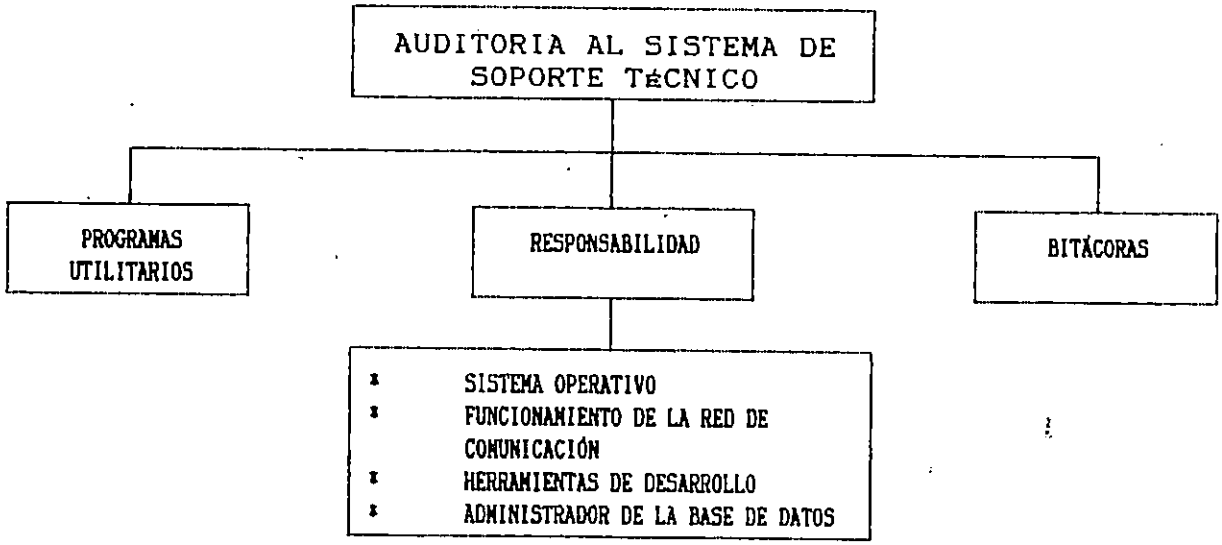


Figura 9. Muestra los tópicos que se han de evaluar en relación al Soporte Técnico.

4. CONCEPTUALIZACIÓN DE LOS ELEMENTOS DEL SISTEMA INFORMÁTICO

4.1 ELEMENTOS DEL SISTEMA INFORMÁTICO

Los elementos que componen un sistema informático son tantos, que se deben por agrupar por subsistemas, identificando así las relaciones entre todos esos elementos. Fue por ello que a través de la Teoria General de Sistemas se establece que un sistema informático agrupa a todos sus elementos dentro de los siguientes subsistemas:

1- Subsistema de acceso al sistema informático.

2- Subsistema de entrada al sistema informático.

3- Subsistema de proceso del sistema informático.

4- Subsistema de salida del sistema informático.

5- Subsistema de bases de datos del sistema informático.

6- Subsistema de comunicaciones del sistema informático.

Estos subsistemas deben ser evaluados por el auditor de sistemas; pero cada uno de ellos habrá de disgregarse (para mayor objetividad) en subcontenidos. Puede ser muy significativo que analice la ilustración de la figura 10 donde se esquematiza el sistema informático y sus elementos. En las siguientes páginas, se detallan cada uno de los subsistemas.

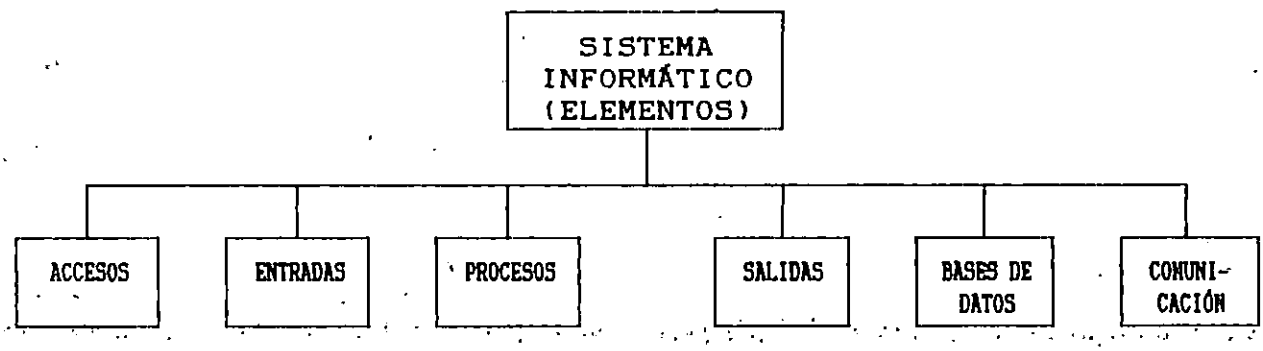


Figura 10. Muestra los aspectos que se auditarán en el Sistema Informático.

4.2 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE ACCESOS

A pesar de que el acceso de personas no autorizadas al centro de procesamiento de datos se realice, ello no garantiza plenamente la confidencialidad de la información. Los sistemas, por ende, deben estar provistos de ciertos mecanismos que controlen el acceso de los usuarios y si se trabaja con alguna red, que controle el acceso de las terminales.

Todo administrador de un sistema, debe haber conceptualizado y elaborado formalmente un esquema o tabla de autorizaciones. Si el esquema ha sido elaborado, el auditor tendrá que evaluarlo, para verificar que sólo las personas que por la naturaleza de sus actividades requieran ciertos datos, tengan la autorización de accesarlos. Accesar implicará por supuesto, leer, copiar, renombrar, borrar, usar archivos, etc.

La identificación de los usuarios y sus terminales, debe ser obligatorio en los sistemas informáticos, si esto no se realiza, jamás se podrán deducir responsabilidades. Muchos métodos existen al dia de hoy para identificación de usuarios, el método elegido dependerá de lo valioso de la información.

Por lo anterior, se concluye que un sistema de accesos debe partir de un esquema de autorizaciones de terminales y usuarios.

En principio los accesos físicos a las instalaciones, proporcionan ciertas garantías; sin embargo el control de los accesos lógicos proporcionará mayor confiabilidad a la privacidad de los archivos, datos, directorios, programas de aplicación o cualesquiera de las formas en que se encuentre almacenada la información.

Los documentos y registros con los que se cuenten, proporcionarán ayuda valiosa: informes de auditoría interna, por ejemplo, acerca de la confiabilidad del sistema de accesos, podrá ser un aporte muy significativo. Un diagnóstico de una compañía aseguradora, memorias de auditorías de Sistemas, bitácoras, etc, es obvio que serán parte de los papeles de trabajo al realizarse una Auditoría de Sistemas Informáticos.

Para mayor claridad, véase en la siguiente página (figura 11) el esquema de la conceptualización de la auditoría al subsistema de Accesos de el sistema informático.

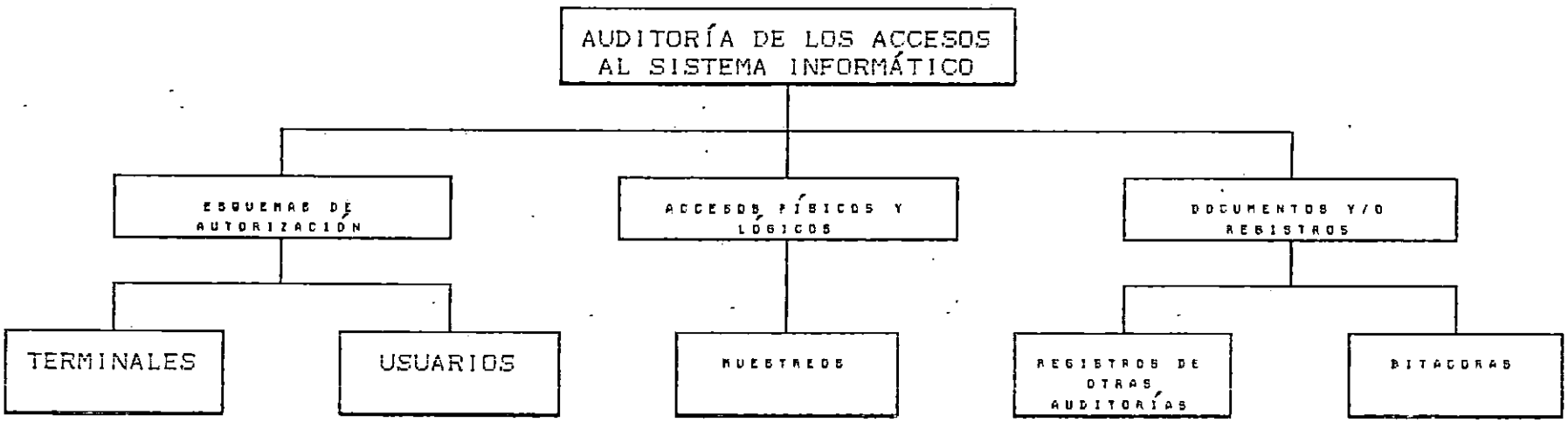


Figura 11. El subsistema de Accesos y los elementos que se han de evaluar.

4.3 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE ENTRADA

La conceptualización de la auditoria al subsistema de Entrada se dirigirá a la evaluación de las funciones de la gerencia, los datos de entrada directa, control a la codificación, documentos fuente, ingreso y validación, recuperación de datos, pistas de auditoria, control de datos y cifras de control.

Para mayor claridad, véase en la siguiente página (figura 12) el esquema de la conceptualización de la auditoria al subsistema de Entrada.

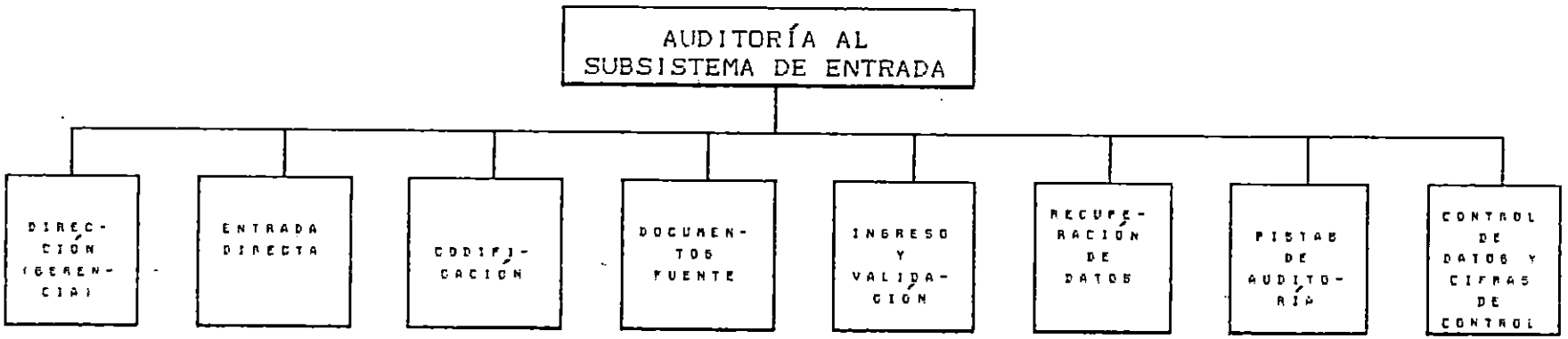


Figura 12. Conceptualización de la forma en que se debe auditar el subsistema de Entradas al sistema informático.

4.4 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE PROCESO

La conceptualización de la auditoría al subsistema de Proceso evaluará el control de las operaciones, la asignación de trabajo, los medios de almacenamiento masivo y control de mantenimiento.

Para mayor claridad, véase en la siguiente página (figura 13) el esquema de la conceptualización de la auditoría al subsistema de Proceso.

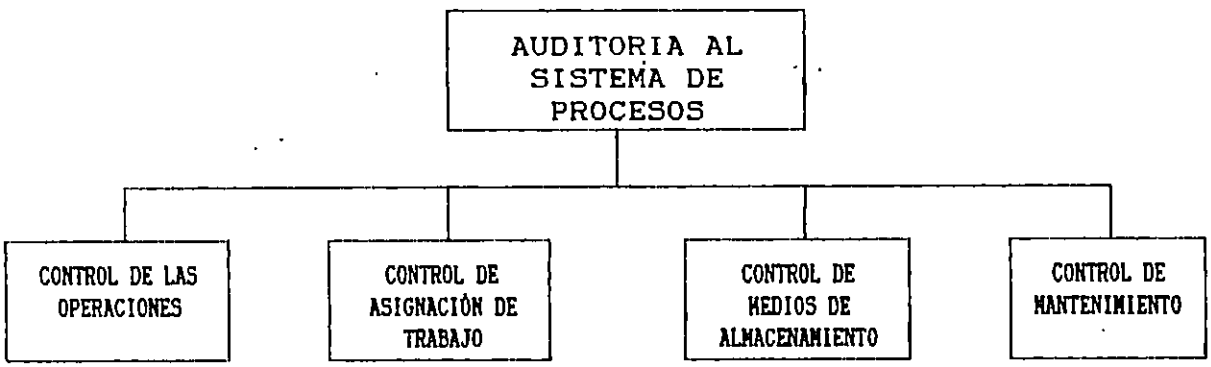


Figura 13. Elementos de evaluación del Subsistema de Procesos.

4.5 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SUBSISTEMA DE SALIDA

La conceptualización de la auditoria al subsistema de Salida se dirigirá a la evaluación de los informes generados por los programas, es decir la presentación que tienen; control a los informes (responsable, seguridad, etc.); control a la inferencia; control a la producción, distribución y control de recuperación.

Para mayor claridad, véase en la siguiente página (figura 14) el esquema de la conceptualización de la auditoría al subsistema de Salida.

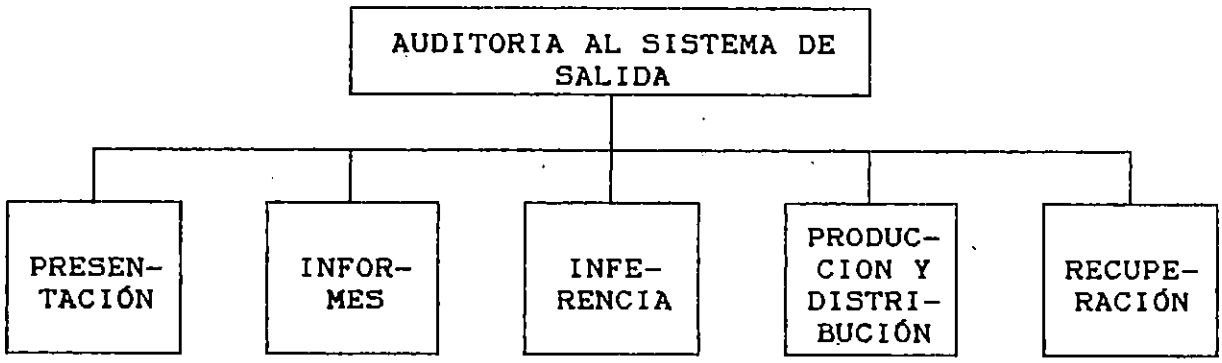


Figura 14. En el esquema pueden visualizarse los aspectos que serán evaluados en lo referente a las Salidas del sistema Informático.

4.6 CONCEPTUALIZACIÓN DE LA AUDITORIA A LOS SISTEMAS MANEJADORES DE BASES DE DATOS

No se trata de ir a cuestionar si un DBMS[1] (por ejemplo FoxProLan) está bien diseñado o no. El usar un XBase, no significa que no habrán redundancias, que no se perderá la integridad de la base de datos, que se haga una **adecuada administración del sistema**, etc. Sin embargo un DBMS deberá ser cuestionado por el auditor en cuanto a criterios de funcionamiento tales como los tiempos de acceso, que involucran velocidad del disco duro, velocidad del procesador central, los métodos de acceso (directo, secuencial o indexado), el modelo del sistema manejador, a saber, jerárquico, relacional o de red.

La velocidad del procesamiento, es otro de los factores que el auditor puede cuestionar, a través de pruebas clásicas para este propósito como lo son la clasificación y la indexación.

La capacidad de almacenamiento de los datos, la compatibilidad de un DBMS con las expectativas que se tenían al momento de ponerlo en marcha, pueden haber generado restricciones al cumplimiento de los objetivos del centro de procesamiento electrónico de datos.

El diccionario de datos, los medios de consulta, la

---

[1] DBMS en adelante significará Sistema Manejador de Bases de datos, por sus siglas en Inglés: Data Base Management System

generación adecuada de los informes, la compatibilidad de archivos con otros programas, la capacidad de reestructuración de la base de datos, y la manipulación efectiva de los errores y la buena documentación y apoyo del software, son características necesarias de los sistemas manejadores de bases de datos.

El manejo de archivos múltiples, la edición de pantalla completa, la generación de formatos de presentación visual en pantalla, la seguridad con palabras de paso, la capacidad para operar en ambientes multiusuarios, son características deseables en los DBMS.

Todo lo anterior podrá ser visualizado claramente en los siguientes esquemas. La figura. 15 muestra el esquema general del sistema de base de datos y sus elementos. En esta figura se encuentran 4 grupos de elementos que el auditor debe considerar. Luego, cada uno de los grupos se esquematizan en las figuras de la 16 a la 19.

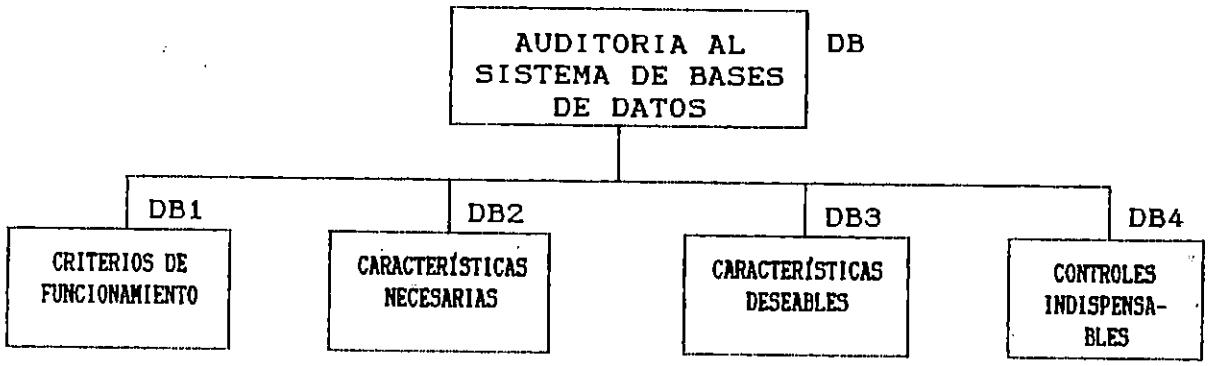


Figura 15. Este esquema muestra los aspectos que serán evaluados en torno a los Sistemas de Manejo de Bases de Datos (sean mecanizados o no).

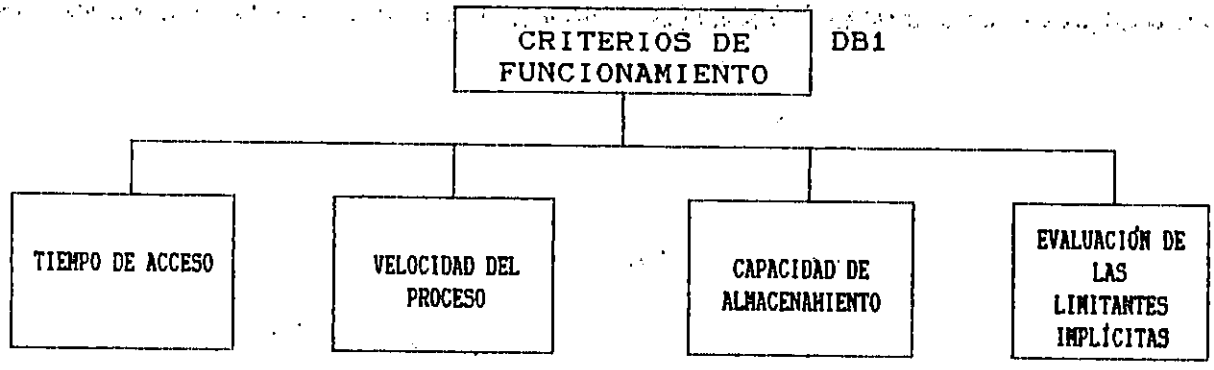


Figura 16. Se ven en el esquema los elementos de criterios de funcionamiento que serán evaluados.

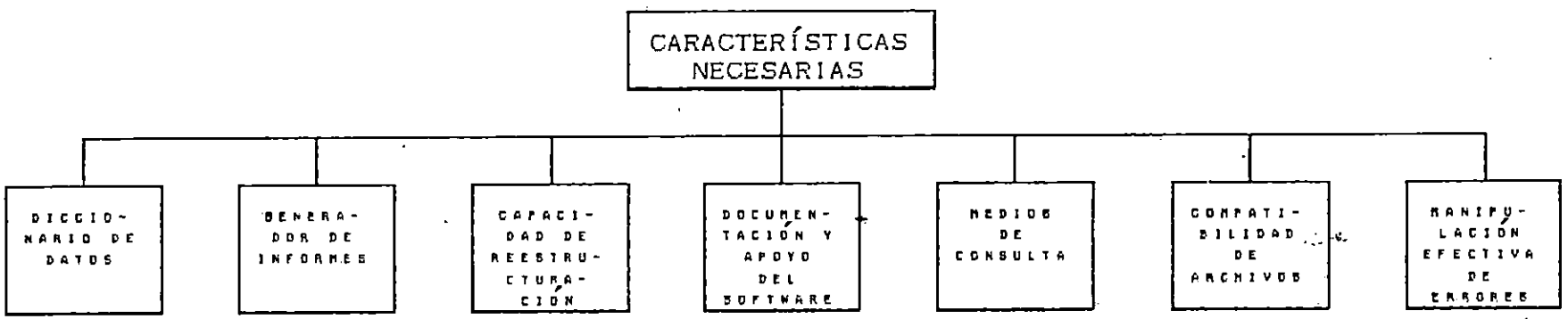


Figura 17. La figura muestra los 7 grupos de aspectos que se han de considerar al evaluar las características necesarias de los sistemas manejadores de bases de datos.

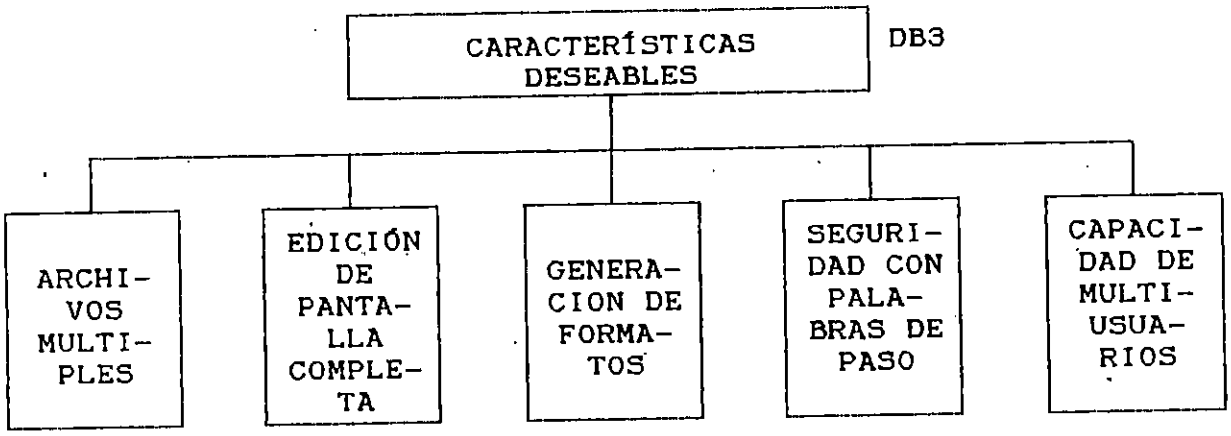


Figura 18. La figura ilustra los grupos de aspectos que se han de considerar cuando se auditen las características deseables de los Sistemas Manejadores de Bases de Datos (DBMS).

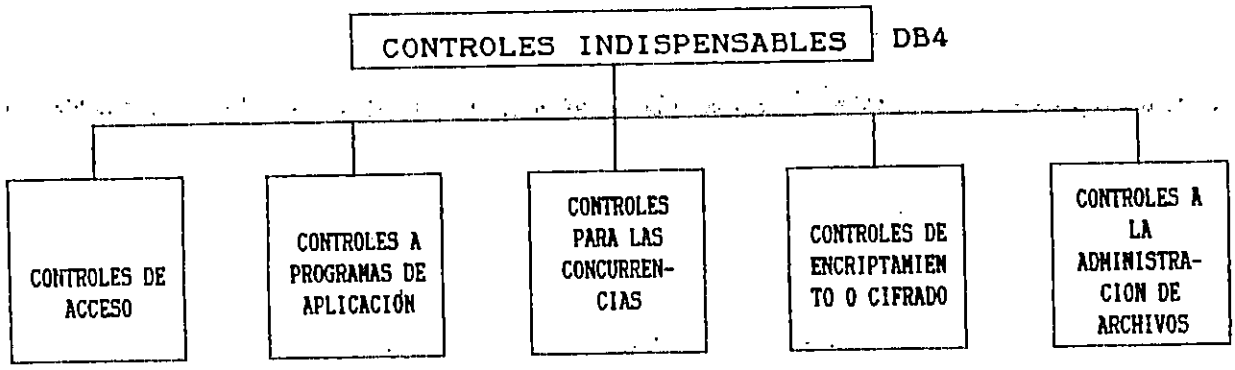


Figura 19. Los controles indispensables acerca de un DBMS, se han de agrupar como se ven en la figura para su evaluación.

4.7 CONCEPTUALIZACIÓN DE LA AUDITORIA AL SISTEMA DE COMUNICACIONES DE LOS SISTEMAS INFORMÁTICOS

Para tener la certeza de que la red de comunicación de datos y las estaciones de trabajo de las microcomputadoras cuentan con todos los controles necesarios y que estos controles ofrecen protección adecuada, se construirá una matriz bidimensional en la que se incorporarán todos los controles que se encuentren presentes en ese momento en la red.

La matriz se construye identificando primero todas las amenazas que enfrenta la red y, después, todos los componentes de la red.

- Una amenaza a la red de comunicación de datos es cualquier evento adverso potencial que pueda dañar la red, interrumpir los sistemas que se encuentran utilizando la red, o provocar pérdidas económicas a la organización. Por ejemplo, la pérdida de mensajes es una amenaza potencial.
- Un componente es una de las partes individuales que, cuando se ensamblan juntas, integran la red de comunicación de datos. Un componente puede considerarse un bien que se encuentra sometido a revisión o un bien sobre el que se está intentando mantener control. Así, los componentes son Hardware, Software, Circuitos, y otras piezas de la red.

La matriz terminada con los controles mostrará la relación que tiene cada control *en el lugar* con respecto a la amenaza que se supone que dicho control mitiga y el componente al que salvaguarda o controla.

El último paso en el diseño de una matriz de controles para una red de comunicación de datos especifica es evaluar la idoneidad de los controles.

Para mayor claridad, véase en la figura 20 el esquema de la conceptualización de la auditoria al subsistema de Comunicaciones de el sistema informático.

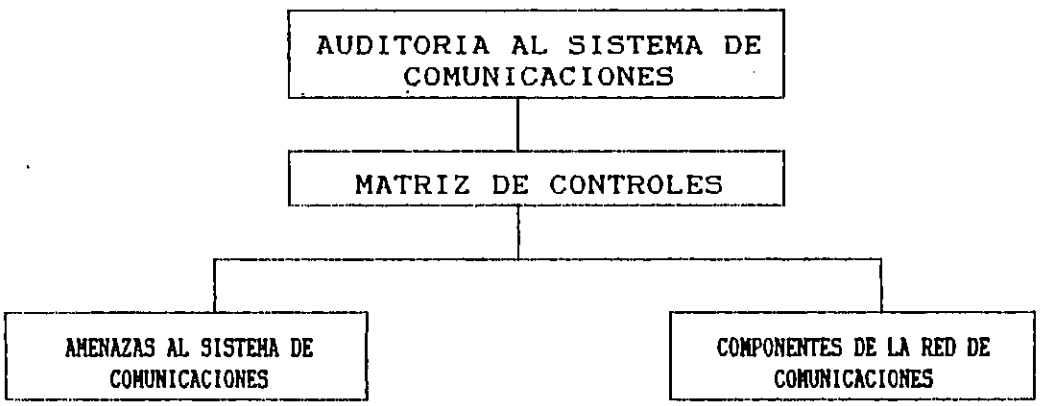


Figura 20. Conceptualización de la metodología para auditar al Subsistema de Comunicaciones de Datos: Amenazas contra Componentes.

Los elementos de la matriz a través de la cual se mezclan las amenazas y componentes se muestran en la figura 21.

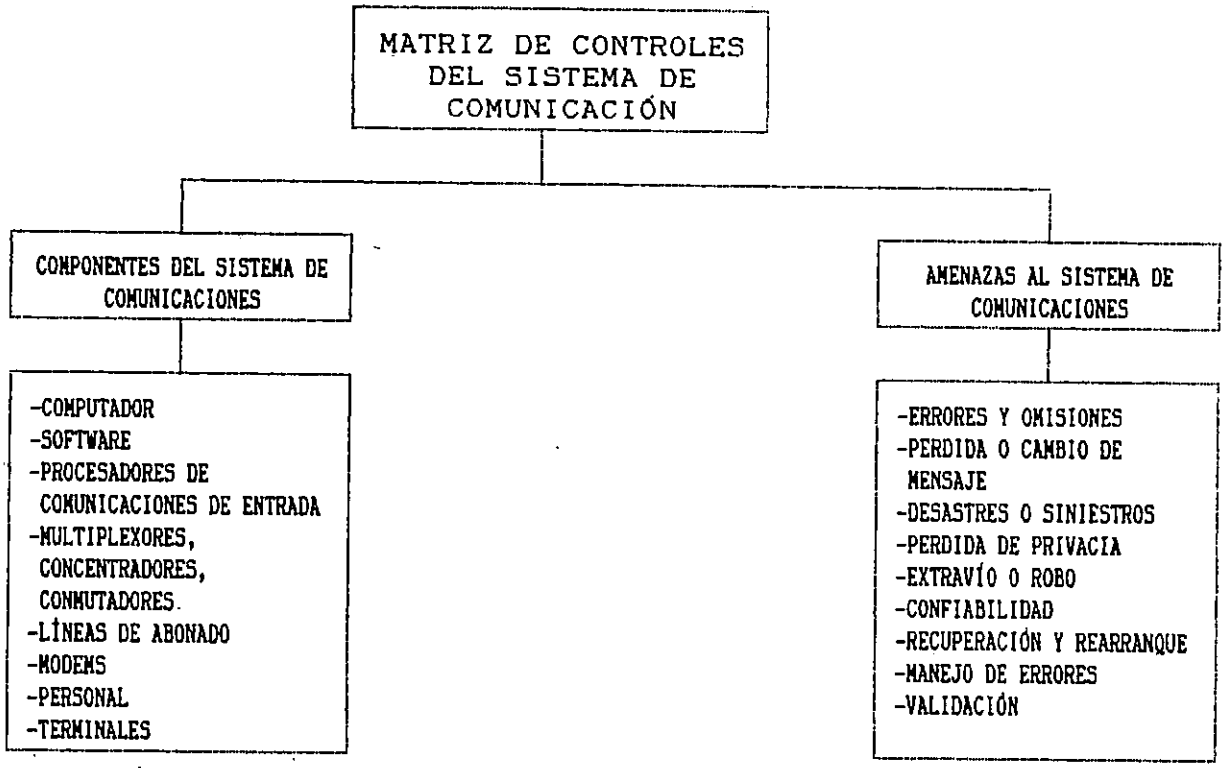


Figura 21. Elementos de la matriz a través de la cual se mezolan: Amenazas, Componentes y controles.

TERCERA PARTE

DISEÑO DE LA METODOLOGIA PARA AUDITAR SISTEMAS INFORMATICOS

5. PLANIFICACIÓN Y ORGANIZACIÓN DE LA AUDITORIA

5.1 PLANIFICACIÓN DE LA AUDITORIA

En esta fase se desarrolla la planificación de todas las actividades, recursos y funciones necesarias; con el objeto de que los encargados de efectuar la auditoría ejecuten sus actividades de forma eficiente.

Los elementos necesarios para llevar a cabo la planificación de la auditoría son :

a) Definición de actividades, Cuyo contenido es el de un listado con una breve explicación de las actividades.

b) Confirmación de la disponibilidad de recursos.

c) Contar con un personal técnico especializado en cada área que sea necesario.

Proceso general para desarrollar la auditoría.

Con el fin de entender, informar y rendir una opinión, el auditor debe :

a) Investigar, que es un paso en donde se recopila información ya sea solicitándola o contestando los formularios y cuestionarios.

b) Analizar, que es una etapa en donde se examina la información y se obtienen las recomendaciones pertinentes del caso.

c) Autenticar, En este paso se obtiene la aprobación total del auditor del sistema en cuestión.

Para lograr una auditoria eficiente se detalla la metodología para la planificación con los documentos respectivos para poder desarrollarla.

Metodología para desarrollar la planificación

La planificación de la auditoria se desarrollará en base a formularios, cuya elaboración quedan en manos del auditor general. Es necesario aclarar que las visitas, actividades y recursos se planificarán con una base no programada, es decir, que durante el año se programarán visitas con diferentes intervalos de tiempo y con desconocimiento de las autoridades.

Por lo tanto el auditor debe ejecutar los siguientes pasos:

a) Listar las actividades a desarrollar, en esta parte de la planificación se anotarán todas aquellas actividades a desarrollar por los auditores y respectivamente se describirá cada una de ellas.

b) Priorización de actividades, en este acápite se ordenan las actividades según sea su importancia o necesidad.

c) Preparar documento de actividades, el auditor debe completar el formulario.

d) Planificación de recursos, para esta parte se desarrolla un formulario que posee la información necesaria para ejecutar la actividad.

e) Investigación Preliminar, en este paso se recopila la información pertinente a evaluar.

f) Definición de funciones, en base a las actividades plasmadas anteriormente se estructurarán las funciones necesarias para ejecutar las actividades.

g) Programación de actividades, la necesidad de definir las actividades en tiempo es indispensable para el control de la ejecución de las mismas.

h) Presupuestación, además de la planificación de los recursos, éstos deben valuarse económicamente y obtener una base estimada de los recursos necesarios para llevar a cabo las actividades; además de conocer el momento en que serán necesarios.

i) Gestión de control, en relación a esta parte se sugiere utilizar un formulario que evalúa la actividad en base a su ejecución en tiempo.

j) Guía para el adecuamiento de la metodología para un sistema en particular.

DESARROLLO DE INSTRUMENTOS DE PLANIFICACIÓN DE LA METODOLOGÍA.

a) **Listar actividades a desarrollar.** Para llevar a cabo esta actividad complete el siguiente formulario. En el debe listar todas aquellas actividades que ejecutará durante la auditoría, en base al proceso general de la auditoria y además en base al subsistema a auditar

EMPRESA AUDITOR:	*FECHA:*
CÓDIGO: PRO1-FMO1	*RESPONSABLE:*

FASE	*ACTIVIDAD*	*DESCRIPCIÓN*

b) **Priorización de actividades.**En base a las actividades

planeadas se estructuran en orden de importancia. Las actividades del comité coordinador o empresa de auditores que evaluarán el centro informático deben considerar el siguiente rubro de actividades en ese orden:

b.1) Funciones administrativas, relativas a las operaciones administrativas de la auditoría, tales como, planificar la auditoría, controlarla, organizarla, ejecutarla y dirigirla, manejando el personal adecuado y emitiendo los reportes pertinentes en relación a las recomendaciones de la evaluación.

b.2) Funciones de auditoría, que se enfocan al desarrollo de las actividades de evaluación que conciernen a la auditoría de sistemas informáticos, por tal motivo es necesario considerar las siguientes macro-actividades:

I. Investigación de las características del sistema informático, en donde se utilizarán los métodos de recolección de datos, tales como: entrevistas, cuestionarios o formularios y observación general; en cada subsistema utilizará cualquiera de las tres formas para lograr el objetivo de la investigación.

II. Análisis de la información, en esta parte el auditor en base a su experiencia y conocimiento evaluará el sistema informático.

III. Autenticación del reporte, en base al análisis del paso anterior el auditor presenta un reporte con recomendaciones pertinentes al caso y con la aprobación del sistema.

En base a lo anterior se pueden estructurar y priorizar las actividades; sin embargo cada subsistema posee elementos y características que hacen seleccionar las actividades de máxima prioridad en una forma mas especifica.

c) **Preparar el documento de actividades.** En esta etapa es necesario recopilar la información en base a actividades con un orden de importancia por lo tanto es necesario desarrollar un pequeño sumario contenido en el siguiente formulario:

EMPRESA AUDITOR:		*FECHA:*	
CÓDIGO: PRO1-FM02		*RESPONSABLE:*	
FASE	*ACTIVIDAD*	*RECURSOS*	*PERSONAL*

d) **Planificación de recursos.** Es indispensable detallar los recursos mínimos necesarios para auditar. Por consiguiente se debe completar el siguiente formulario:

EMPRESA AUDITOR:	FECHA:
CÓDIGO: PRO1-FM03	RESPONSABLE:

No.	FASE	RECURSO	DESCRIPCIÓN	CANTIDAD	DISPONIBILID	OBSERVACIÓN

e) **Investigación preliminar.** esta fase es dedicada a la recopilación de información necesaria para realizar un breve análisis de la organización de la empresa, los formularios, documentos e información relativa a los subsistemas del procesamiento electrónico de datos se recopilarán en el momento en que éstos se evalúen según los requisitos necesarios.

La información mínima para efectuar la investigación es la siguiente:

Controles relativos a la organización de la empresa, los documentos generales a recoger son:

I. Objetivos a corto y largo plazo.

II. Manual de la organización.

III. Antecedentes o historia de los organismos.

IV. Políticas generales.

Estos documentos deben estar estructurados con los elementos siguientes:

i. Definición clara de los objetivos.

ii. Definición de responsabilidades y objetivos funcionales.

iii. Relaciones de las obligaciones y misión de las principales funciones.

iv. Estructura orgánica(organigrama).

v. Manuales de funciones.

vi. Reglamentos o disposiciones oficiales.

vii. Datos de producción de cada unidad.

viii. Estudio de la distribución de oficinas.

ix. Examen de condiciones físicas.

x. Antecedentes de sistemas utilizados.

xi. Evolución paulatina de los sistemas.

xii. Datos históricos (Estadísticas en general)

xiii. Planes antiguos vrs. gestión de control.

xiv. Documentos relativos a la administración del procesamiento electrónico de datos.

f) **Definición de funciones.** Para cada una de las actividades se desarrollará una estructuración de funciones como sigue a continuación:

NOMBRE DEL PUESTO : DIRECTOR DEL DEPTO. DE AUDITORIA	
CÓDIGO: PR01-FM04	DEPENDENCIAS SUPERIORES : GERENTE GENERAL
SUBORDINADOS : AUDITOR DE SISTEMAS Y AUDITOR ADMVO.	
FUNCIONES	

a) Planificar la auditoría, en todo lo que concierne a recursos materiales y humanos; actividades, programación, para lograr ejecutar una auditoría eficiente.

b) Controlar las actividades del grupo de auditoría.

c) Asignar las funciones adecuadas al personal bajo su responsabilidad.

d) Definir los objetivos funcionales de la auditoría y el alcance de la misma así también las metas generales del grupo de auditoría.

e) Diseñar estándares para dirigir la auditoría.

f) Analizar los resultados de la auditoría de cada área.

NOMBRE DEL PUESTO : AUDITOR DE SISTEMAS .	
CÓDIGO: PRO1-FM05	DEPENDENCIAS SUPERIORES : DIR. DEL DEPTO. DE AUDITORIA
SUBORDINADOS : AUDITORES DE SISTEMAS INFORMÁTICOS.	

FUNCIONES

a) Planificar la auditoría, definir áreas a auditar, así como recursos en relación a sistemas, recolectar la información; entrevistas , cuestionarios y observación del sistema.

b) Definir prioridades a evaluar.

c) Desarrollar la auditoría en el área de sistemas utilizando los instrumentos adecuados y evaluando todos los elementos del sistema informático.

d) Analizar la evidencia de auditoría.

e) Preparar documentación que respalde los hallazgos de la auditoría.

f) Preparar un informe de resultados de la auditoría que contenga, conclusiones y recomendaciones.

NOMBRE DEL PUESTO : AUDITOR ADMINISTRATIVO DE S.INF.	
CÓDIGO: PR01-FM06	DEPENDENCIAS SUPERIORES : DIR. DEL DEPTO. DE AUDITORIA
SUBORDINADOS : AUDITOR DE LA FUNCIÓN DE INFORMÁTICA.	

FUNCIONES

a) Planificar la auditoría del Entorno Administrativo, definir los Subsistemas a auditar, así como recursos en relación a la administración de sistemas, recolectar la información; entrevistas , cuestionarios y observación; del área Administrativa. del sistema.

b) Definir prioridades a evaluar.

c) Desarrollar la auditoría del entorno administrativo de sistemas utilizando los instrumentos adecuados y evaluando todos los elementos del área Admva. del Sist. informático.

d) Analizar la evidencia de auditoría.

e) Preparar la documentación que respalde los hallazgos de la auditoría.

f) Preparar un informe de resultados de la auditoría que contenga, conclusiones y recomendaciones.

g) Programación de actividades.

Elementos para desarrollar la programación:

g.1) Actividades a desarrollar. Se toma el documento final de las actividades y se transcriben al cronograma.

g.2) Disponibilidad de recursos.Es importante confirmar los recursos a utilizar.

g.3) Estimaciones históricas. Si existen estimaciones de tiempo de auditorías anteriores, es recomendable revisarlas para lograr una aproximación mas real.

g.4) Estimaciones de tiempo. Este elemento se relaciona al tiempo calculado por el auditor en sí.

Procedimiento para la programación:

- Obtener formularios.
- Anotar las actividades principales al formulario.
- Hacer estimaciones.
- Aprobar estimaciones.
- Distribuir formularios a los auditores respectivos para desarrollar la auditoría.

El formulario para desarrollar la programación es:

CÓDIGO: PRO1-FM07	PROGRAMACIÓN DE ACTIVIDADES.

FECHA	MES 1	MES 2
ACTIVIDAD		

h) Gestión de control.

AVANCE DEL CUMPLIMIENTO	
EMPRESA AUDITOR: CÓDIGO: PRO1-FM08	FECHA: RESPONSABLE:

FA-SE	SIT. AUDITO			PER.AUD		DIAS REAL	AVAN	DIAS HOM.	EXPLIC. CAMBIO
	NO INICIADA	EN PROCE-SO	FINALIZA	INI-CIAD	FINA-LIZAD				

i. **Presupuestación.** Para este paso es necesario estimar un dato económico para desarrollar las actividades.

CÓDIGO: PRO1-FM07			PRESUPUESTO					
ACTIVIDAD	MES				MES			

j) Guía para el adecuamiento de la metodología para un sistema en particular.

Es recomendable revisar que el sistema posea las características mínimas para que la metodología pueda ser utilizada correctamente. Si en dado caso no cumple con dichas características, adquirir los recursos necesarios para que las cumpla. Posteriormente se adecuará la metodología tomando en cuenta todos estos aspectos.

Para cualquier tipo de sistema, la metodología siempre de ajustarse en los instrumentos diseñados. Así pues, para los formularios debe considerarse los siguientes pasos:

1. Leer los formularios.
2. Revalorizar los elementos, esto se realizará si la empresa posee prioridades o escala de valores diferentes.
3. Evaluar el sistema.
4. Dictaminar en base a lo siguiente:
   a) Si el promedio está entre 0..33 entonces el área evaluada indica un grado de eficiencia y eficacia bajo y debe reorientarse.
   b) Si el promedio está entre 34..63 indica que el subsistema es regular pero puede mejorarse mucho en los diferentes elementos evaluados.

c) Si el promedio está entre 64..100 indica que el subsistema es muy bueno, que para perfeccionarlo es necesario mejorar pocos aspectos de forma.

5. Si la empresa desea un grado mayor de detalle del estado del sistema debe subdividir en mas intervalos y describir el significado.

6. Para los centros de procesamiento de datos que carezcan de uno o varios elementos de cada formulario, debe considerarse como falla calificándolo con 0%. En este caso en particular el área evaluada es muy característica en el sentido de que cada elemento es vital y todos debe estar a lo sumo concebidos.

En relación a los cuestionarios seguir el siguiente procedimiento :

1. Leer los cuestionarios.
2. Marcar y contabilizar todas aquellas preguntas que no competen al sistema.
3. Restar del total de preguntas y obtener el nuevo total que representa el 100%.
4. Evaluar el sistema desarrollando el cuestionario.
5. Contabilizar las preguntas.
6. Revisar las respuestas abiertas.
7. Obtener el porcentaje correspondiente.

8. En base al número concluir:

   a) Si el promedio está entre 0..33 entonces el área evaluada indica un grado de eficiencia y eficacia bajo y debe reorientarse.

   b) Si el promedio está entre 34..63 indica que el subsistema es regular pero puede mejorarse mucho en los diferentes elementos evaluados.

   c) Si el promedio está entre 64..100 indica que el subsistema es muy bueno, que para perfeccionarlo es necesario mejorar pocos aspectos de forma.

En el caso de la auditoría la sistema de comunicaciones de los sistemas informáticos, en el cual no se emplea un cuestionario sino que una matriz de controles, no habrá nada que ajustar, ya que la metodología implica dos cosas: 1) identificar todas las amenazas a la red de comunicaciones y 2) identificar todos los componentes o elementos de la red. De acuerdo a cada caso las variables intervinientes serán las encontradas en el lugar, es decir en la empresa que se esté auditando. Así pues en este tipo de instrumento matricial no habrá diferencia si se aplica a X o Y sistema informático.

5.2 ORGANIZACIÖN DE LA AUDITORIA

Esta sección se divide en dos partes: la primera es con respecto a la ubicación del departamento de auditoria de sistemas y la segunda, trata acerca de el perfil del auditor de sistemas

5.2.1 ORGANIZACIÖN DEL DEPARTAMENTO DE AUDITORIA DE SISTEMAS INFORMÄTICOS

Se establecen en este apartado los aspectos relativos a la organización del departamento de Auditòria de Sistemas Informáticos. De acuerdo a lo establecido en esta metodología, la Auditoría de Sistemas se divide en dos grandes aspectos:

1) Auditoría al Sistema Informático y sus aplicaciones
2) Auditoría al entorno Administrativo del sistema Informático

La organización y la ubicación de los departamentos de auditoría del sistemas informático y aplicaciones, y el entorno administrativo, son fundamentales para el buen desarrollo de sus actividades, así como para la consecución de sus objetivos.

Cada uno de los dos departamentos, tiene una ubicación diferente en la estructura organizacional de la empresa, así como

los conocimientos de su personal que les conforman varían de uno a otro.

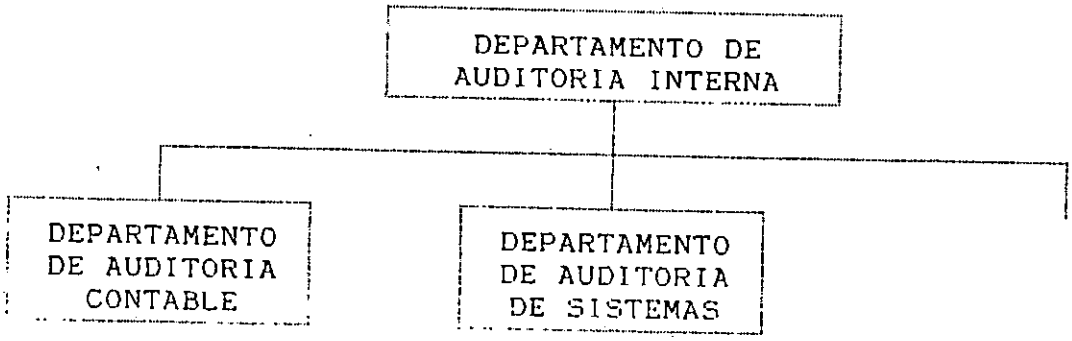
1) Departamento de Auditoría al Sistema Informático y sus aplicaciones

El departamento de Auditoría de sistemas informáticos y sus aplicaciones, debe ser parte integral del departamento de auditoría interna. La ubicación dentro de la estructura orgánica de este último es tema de cuestionamiento por parte de los auditores. Existen dos puntos de vista diferentes:

PRIMER PUNTO DE VISTA:

* El departamento de auditoría de sistemas informáticos y sus aplicaciones, debe ubicarse como una unidad independiente dentro del departamento de Auditoría, contando con su propio gerente.

  El organigrama para este tipo de organización del departamento de auditoría de sistemas y aplicaciones es el siguiente:



Véanse las ventajas de este esquema a continuación

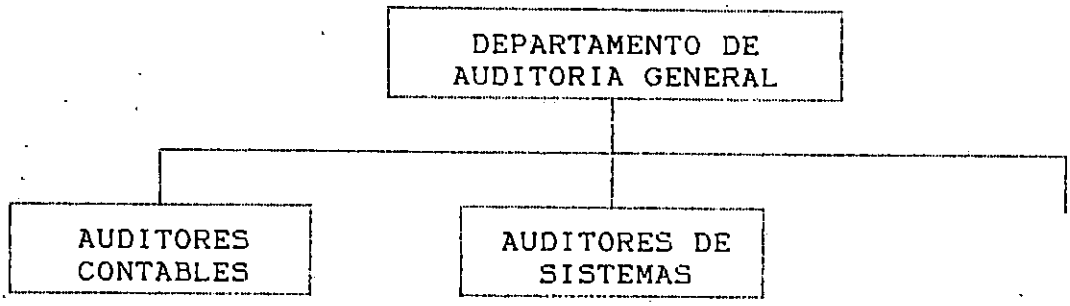
Esta forma de organización del departamento tiene las siguientes ventajas:

- Mejor utilización de los recursos, porque los Auditores de sistemas y aplicaciones se ocuparían únicamente de atender los asuntos relacionados con las aplicaciones, logrando así una especialización de sus funciones.
- El control y coordinación de los auditores de sistemas informáticos y aplicaciones se facilita, porque existe un gerente a cargo de todos ellos.
- Permite una mayor especialización del departamento en diferentes áreas, cubriendo un espectro más amplio de requerimientos. Esta mayor especialización se logra si cada uno de sus miembros está orientado a un área especifica de la Auditoría de sistemas y aplicaciones.

SEGUNDO PUNTO DE VISTA:

* La función de Auditoria de sistemas Informáticos y sus Aplicaciones, como parte integral de la Auditoria interna, que ubica a los auditores de sistemas y aplicaciones formando parte del grupo de Auditores generales.

El organigrama para este tipo de organización es el que se muestra a continuación:



Las ventajas que este tipo de organización presenta son:

- Mayor congruencia en las metas de la Auditoria, porque al formar parte del grupo de auditores generales, el auditor de sistemas informáticos y aplicaciones, tiene una mayor comprensión de los objetivos de la auditoria general y mayores responsabilidades en ello.

- Facilita la comunicación entre los auditores generales y los auditores de sistemas informáticos y aplicaciones. Si ambos se integran en grupo de trabajo, sus labores se complementan y sus diferencias técnicas se superan.
- Mayor motivación para incrementar sus conocimientos. Los auditores generales adquieren más conocimientos del área de sistemas, y los auditores de aplicaciones incrementan sus conocimientos sobre auditoría interna.

En el país, son muy pocas las empresas que puedan tener más de una persona realizando auditoría de sistemas y aplicaciones, las pocas que pueden hacerlo son los bancos o empresas sumamente grandes. Independientemente del número de personas que conformen el departamento de auditoría de sistemas y aplicaciones, se recomienda que este sea ubicado como una unidad independiente dentro del departamento de auditoría interna.

Una empresa pequeña que no pueda absorber a un auditor de sistemas informáticos en forma permanente, puede recurrir a un consultor para que realice estas funciones.

Esta alternativa tiene la ventaja de no incrementar el personal de la empresa, sin embargo, al auditor externo le

llevará más tiempo realizar esta labor, puesto que inicialmente tendrá que obtener un entendimiento de la aplicación a auditar y familiarizarse con las labores de la empresa. Este incremento en el tiempo genera un incremento en el costo para una auditoría específica, que a la larga es siempre menor al que representaría mantener a un auditor de sistemas en forma permanente. Generalmente, una auditoría de sistemas informáticos en este tipo de empresas se solicita para detectar las causas de algún problema que esté afectando el funcionamiento de los sistemas.

2) Departamento de Auditoría al entorno Administrativo del Sistema Informático

El departamento de auditoría de sistemas informáticos que se encarga del entorno administrativo, debe verse como una unidad que está relacionada con el departamento de cómputo y con el de auditoría interna. La ubicación más recomendable para este departamento es junto con el departamento de auditoría de sistemas y sus aplicaciones.

No es probable que en las empresas pequeñas se obtenga a una persona en auditoría de sistemas informáticos y aplicaciones, y otra en auditoría del entorno administrativo del sistema

informático. El auditor de sistemas, podrá realizar ambos tipos de auditoría, por lo que sus conocimientos deberán ser más completos. En esta situación, el auditor de sistemas deberá comunicar los resultados a la persona interesada en los mismos.

Las personas que conforman los departamentos de auditoría de sistemas y aplicaciones, y el departamento encargado del áudito del entorno administrativo deben tener diferentes tipos de conocimientos para el desempeño de sus funciones. El auditor del sistema informático y aplicaciones, deberá poseer un amplio conocimiento sobre computación, controles para aplicaciones y auditoría en general. El auditor del entorno administrativo del sistema informático, deberá tener profundos conocimientos en lo que respecta a controles internos, procesamiento de datos, métodos de análisis, diseño y desarrollo de aplicaciones, elaboración de estándares de trabajo, implantación de sistemas y de todo lo concerniente a las labores propias del centro de cómputo.

Si la persona que efectúa la auditoría de sistemas y aplicaciones, debe realizar además la auditoría del entorno administrativo del sistema informático, ésta deberá tener un amplio conocimiento tanto en el área de auditoría general como también en el área computacional. Estos requerimientos hacen un

tanto difícil la tarea de reclutamiento de personal para cubrir este puesto. Es por ello que en muchas ocasiones se recurrirá a consultores externos para suplir aquellas funciones en las que el auditor de sistemas no está totalmente capacitado.

5.2.2 PERFIL DEL AUDITOR DE SISTEMAS

Para definir las características de el auditor de sistemas, se ha de especificar en primer término las funciones que éste deberá realizar.

a) Funciones en el Area del sistema informático y sus aplicaciones

La función principal de éste es evaluar el impacto de los sistemas en la organización. La extensión del área de participación del auditor de sistemas y aplicaciones varía de una empresa a otra, de acuerdo al tamaño de la empresa o de acuerdo al tamaño del centro de cómputo. Las actividades a desarrollar por cada uno de los miembros del grupo de auditoría dependerá asimismo de la cantidad de personas que lo conformen.

El grupo de Auditoría de Sistemas y Aplicaciones deberá realizar las siguientes funciones:

- Seleccionar la aplicación a auditar
- Definir los objetivos funcionales de la auditoría y el alcance de la misma
- Establecer las metas generales del grupo de auditoría
- Planear y asignar el trabajo a realizar
- Desarrollar estándares para dirigir la auditoría

- Practicar la auditoría (evaluar los controles, realizar las pruebas seleccionadas, recolectar las evidencias, etc.)
- Analizar la evidencia de auditoría
- Preparar la documentación que respalde los hallazgos de la auditoría
- Preparar un informe de resultados de la Auditoría, incluyendo conclusiones y recomendaciones.

b) Funciones en el Area del entorno administrativo del sistema informático

Estas funciones difieren ligeramente de las del área de sistemas y aplicaciones, en aquella área, el énfasis está sobre una aplicación en particular que pertenece al sistema Informático. En el caso del área administrativa del centro de procesamiento electrónico de datos, el interés se centra en evaluar las tareas desarrolladas dentro del centro de cómputo. Las funciones que se desarrollan generalmente en esta área son:

- Evaluación del cumplimiento de planes de trabajo, metodología y estándares de programación y documentación en el proceso de desarrollo e implantación de sistemas de información

- Evaluación de la calidad de la función de procesamiento de datos
- Evaluación del grado de idoneidad del personal que labora en el centro de procesamiento electrónico de datos.
- Evaluación del soporte técnico prestado por el centro de cómputo, tanto a nivel interno como el proporcionado a los demás departamentos de la organización
- Preparar un informe de resultados de la auditoría del entorno administrativo, incluyendo conclusiones y recomendaciones.

PERFIL DEL PUESTO Y DE LA PERSONA

NOMBRE DE LA POSICIÓN: Auditor de Sistemas informáticos

SUPERIOR INMEDIATO: Gerente de Auditoría

PERSONAL SUBORDINADO: Dependerá de la proyección que se le brinde a la unidad

Principales responsabilidades del puesto: Elaborar los planes de trabajo de la unidad, así como planificar y desarrollar todas las actividades de verificación del control de los sistemas informáticos de la empresa. Analizar y verificar en detalle el software de la empresa para velar por el

adecuado control, así como para determinar las fallas en las aplicaciones de los sistemas informáticos. Elaborar e implementar un plan de contingencia que permita salvaguardar los sistemas informáticos e información de la organización. Analizar los nuevos sistemas y sus aplicaciones para autorizar la implantación de los mismos. Elaborar reportes de los hallazgos para el superior inmediato.

REQUISITOS DEL CANDIDATO

Educación: Deberá contar con formación universitaria en las carreras de Ingeniería Industrial, Ingeniería de Sistemas Informáticos o Licenciatura en sistemas, pero más importante es la experiencia obtenida.

Experiencia: 3 años de experiencia en la administración de centros de cómputo, análisis y diseño de sistemas y en la auditoria de sistemas.

Idiomas: Inglés Técnico

Conocimientos y habilidades especificas: Deberá poseer conocimientos de sistemas operativos, de la administración de bases de datos, de programación y lenguajes de cuarta generación. Así mismo requiere contar con conocimientos de equipo digital y de computadores PC's con ambiente DOS, conocimiento de los principios de auditoria interna,

facilidad para la redacción de informes técnicos y capacidad para dirigir personal.

Edad: Mayor de 28 años

Sexo: N/A.

Características de personalidad: Responsable, organizado, con iniciativa, creatividad, habilidades de liderazgo y capacidad para el trabajo en equipo. De elevada capacidad de análisis, para la negociación y para interrelacionarse con otros.

Capacitación (inducción): Conocimiento de las operaciones y sistemas de la empresa, así como capacitación en los sistemas operativos y en áreas que requieran solidez de conocimientos para el adecuado desarrollo de sus funciones.

5.3 PAPELES DE TRABAJO

El auditor de sistemas informáticos realizará su labor con una metodología que le sirva de pauta y que además le ayude a documentar la evidencia encontrada. Estos papeles de trabajo por consiguiente representan tanto las actividades como los resultados. Estos documentos o papeles de trabajo de auditoría deben ser construidos y organizados antes de la ejecución de la auditoría.

Los papeles de trabajo facilitan el cumplimiento de la auditoría al delinear un acercamiento paso por paso al trabajo.

Incluyen desde los registros de legalidad de la empresa y todos las del área bajo investigación, observaciones escritas y la lógica que generó ciertas conclusiones. Las actividades de auditoría que no se lleven a cabo también deben ser anotadas, junto con las razones por las que no fueron incluidas. Además los papeles de trabajo permiten al gerente del equipo de Auditoría de Sistemas Informáticos revisar el progreso y ofrecen una base para generar las recomendaciones.

La extensión y el propósito de los papeles de trabajo varían dependiendo de si la Auditoría la lleva a cabo un auditor interno o un auditor externo. Esta diferencia se debe principalmente al hecho de que el auditor externo o independiente es responsable

financieramente por la exactitud y suficiencia del trabajo de auditoria; los papeles de trabajo son la evidencia de que el trabajo ha sido realizado.

5.3.1 AUDITORIA EXTERNA Y SUS PAPELES DE TRABAJO

Dentro de cualquier auditoria se debe tomar como una norma la siguiente:

> " Se deben obtener suficientes pruebas materiales competentes mediante inspección, observación, preguntas y confirmaciones para formarse una base razonable para una opinión con respecto al estado del sistema informático bajo examen."

Los papeles de trabajo incluyen información obtenida mediante preguntas, observación, inspección y examen fisico; y otra información desarrollada por, o disponible al auditor que le permite llegar a conclusiones basadas en razonamientos válidos.

No hay norma que especifique el contenido detallado de los papeles de trabajo; las necesidades especificas del auditor en cada caso individual dictan esto. Además esta declaración de la

cantidad, tipo y contenido de los papeles de trabajo con proyectos particulares, ellos deben demostrar:

* Que el estado real del sistema informático u otra información sobre la cual el auditor estaba enterado, están de acuerdo con la información que sustentan los registros de la empresa.
* Que el proyecto planificado y que el trabajo de cualesquiera miembros del equipo de auditoría fue supervisado y revisado.
* Cómo se resolvieron o trataron cualesquiera excepciones o asuntos fuera de lo ordinario.
* Comentarios apropiados preparados por el auditor indicando sus conclusiones sobre aspectos significativos de la labor.

5.3.2 AUDITORIA INTERNA Y SUS PAPELES DE TRABAJO

El auditor interno usa papeles de trabajo para los mismos propósitos que el externo. La principal diferencia es que el auditor externo es responsable financieramente por la exactitud y la competencia de la auditoria y el auditor interno no. Los auditores internos, sin embargo, son responsables profesionalmente (debido a que sus carreras profesionales están en juego) de hacer declaraciones y recomendaciones mediante el uso de evidencia documentada.

Hay dos diferencias fundamentales entre el tipo de evidencia usada por auditores internos y externos:
primero, el auditor interno no tiene que retener información general acerca de la organización. Cualesquiera normas, procedimientos, directivos, manuales u otra materia generalmente disponible dentro de la organización no tiene que ser duplicada por el auditor interno (por ejemplo cuadros organizacionales, normas de la nómina de pagos, normas de jubilaciones, etc.).
segundo, la cabalidad de la documentación. Los auditores internos deben proveer la suficiente documentación para sustentar lo razonable de sus conclusiones.

En términos del trabajo actualmente llevado a cabo, el material en los papeles de trabajo tanto para los auditores internos como externos es similar.

5.3.3 SECCIONES DE LOS PAPELES DE TRABAJO

Se sugieren seis secciones para organizar los papeles de trabajo:

* **Planificación de la auditoría.** Aquellos aspectos que delinean los objetivos de la auditoría y los medios de llevar a cabo esos objetivos.
* **Administración de la auditoría.** Son los anexos sustantivos y la información necesaria para llevar a cabo la auditoría, este material incluye presupuestos, itinerarios detallados y organización del grupo de auditoría.
* **Datos permanentes.** La información traída de un año a otro que describe el ambiente en que se han realizado las auditorías.
* **Conducción de la auditoría.** Toda la documentación que sustenta la auditoría en sí.
* **Revisión de la auditoría.** Revisión supervisora de los fallos de auditoría, conclusiones y datos sustantivos.
* **Informe de los resultados de auditoría.** Los informes que son preparados como resultado de la auditoría. los fallos y las conclusiones deben ser comparados con los datos que les sustentan.

6. EJECUCIÓN DE LA AUDITORIA: ENTORNO ADMINISTRATIVO

El diseño de la metodología se desarrolla con una serie de formularios, que cuestionan un conjunto de elementos emitiendo una puntuación en cada uno de ellos que al final se resumen en una sumatoria, que en forma cronológica será analizada. Por ejemplo si en enero para el subsistemas de la Admón. de Datos se obtuvo un 70%, en febrero se espera una mayor puntuación en base a las recomendaciones; de esta manera se observa el desarrollo de las mejoras tomando como base la auditoría.

El detalle de los subsistemas que componen el entorno del sistema informático se muestra en las siguientes páginas.

6.1 AUDITORIA A LA ADMINISTRACIÓN DEL ÁREA DE PROCESAMIENTO DE DATOS.

6.1.1 EVALUACIÓN DEL COMITÉ DE COORDINACIÓN DE ACTIVIDADES.

Este comité se encarga de la administración de todas las actividades del centro de cómputo y generalmente se encuentra formado por el gerente general y el gerente del departamento de informática. Por lo tanto se evaluará de él lo siguiente :

a) Planificación estratégica
b) Objetivos
c) Información tecnológica
d) Definición de prioridades para el desarrollo de labores
e) Monitoreo y cuantificación de resultados obtenidos por el área
f) Plan de recuperación de instalación

Ver su instrumento evaluador en anexo B1.

6.1.2 EVALUACIÓN DE LA ORGANIZACIÓN DEL PROCESAMIENTO ELECTRÓNICO DE DATOS.

Para lograr evaluar la organización es recomendable recopilar el documento manual de la organización el cual deberá comprender como mínimo:

- Organigrama con jerarquías
- Funciones
- Objetivos y políticas
- Análisis, descripción y evaluación de puestos
- Manual de procedimientos
- Manual de normas
- Instrucciones de trabajo o guías de actividad.

Además se debe solicitar:

- Objetivos de la dirección
- Políticas y normas de la dirección.

En base a la documentación establecida

anteriormente contestar el siguiente instrumento, si el rubro no existe, anotar en las observaciones el hecho, para que en las recomendaciones se sugiera implementar. El instrumento evalúa:

a) Niveles jerárquicos

b) Puestos

c) Autoridad

d) Funciones

Ver anexo B2.

6.2 AUDITORIA AL SUBSISTEMA DE DESARROLLO DE SISTEMAS

La base de la auditoria al desarrollo de sistemas se estructura en tres fases o etapas: Desarrollo de aplicaciones, Documentación que sirva como base para control y aplicaciones que ya están en uso.

RIESGOS RELATIVOS AL DESARROLLO DE SISTEMAS

El desarrollo de nuevos sistemas está expuesto a los mismos riesgos generales a que están expuestos los negocios como excesivos costos en el desarrollo, pérdida de control, requerimientos mayores, errores de diseño, posibilidad de cometer fraudes accidental o deliberadamente, diseño inadecuado a las demandas, falta de flexibilidad, etc.

DEFINICIÓN DE TAREAS

El desarrollo de sistemas se divide en una serie de tareas relativamente pequeñas. La intención es hacer que todo el proyecto sea predecible, dividiendo el trabajo en unidades que sean lo bastante pequeñas para que se les pueda analizar, evaluar y presupuestar al iniciar un proyecto.

Así las estimaciones de tiempo y costo para las tareas se pueden predecir con mayor precisión. Los compromisos se efectúan en puntos de revisión previamente establecidos bajo un enfoque

de "compromiso progresivo" en el que solicita autorización de la gerencia para pasos individuales relativamente pequeños.

A continuación se presenta un modelo (no es el único) del compromiso progresivo del desarrollo de sistemas.

Los principios generales son lo bastante generales para que cualquier persona familiarizada con la estructura que aquí se presenta pueda apreciar fácilmente las estructuras alternativas.

EL COMPROMISO PROGRESIVO

ACTIVIDAD DEL PROYECTO	GRADO DE RIESGO DE PROCEDER A LA TERMINACIÓN DEL PROYECTO SIN PUNTOS DE VERIFICACIÓN POSTERIORES	GRADO DE COMPROMISO DE LA ORGANIZACIÓN CON RESPECTO AL PROYECTO	EROGACIONES ACUMULADAS
PLANEACIÓN DEL SISTEMA			
Investig. inicial	100%	0%	0%
Estudio preliminar del sistema	90	10	5
Estudio de la planeación del sistema	75	25	15
DESARROLLO			
Requerimientos del usuario	50	50	25
Especificaciones técnicas	40	60	35
Planeación de la implantación	20	80	40
Programación	15	85	70
Procedimientos y entrenamiento del usuario	15	85	75
Prueba del sistema	10	90	80
IMPLANTACIÓN			
Conversión	5	90	99
Revisión posterior a la implantación	0	95	100
Mantenimiento continuo.			

Esta tabla muestra que:

* La programación es importante, pero representa únicamente el 30% de los compromisos totales del costo y tiempo de un proyecto de desarrollo.

* La programación no se inicia sino hasta después de haberse erogado el 40% del total de recursos requeridos.

* La programación no se inicia sino hasta que los estudios del problema del negocio, sus condiciones y su solución indican que existe un 80% de seguridad respecto al éxito del proyecto.

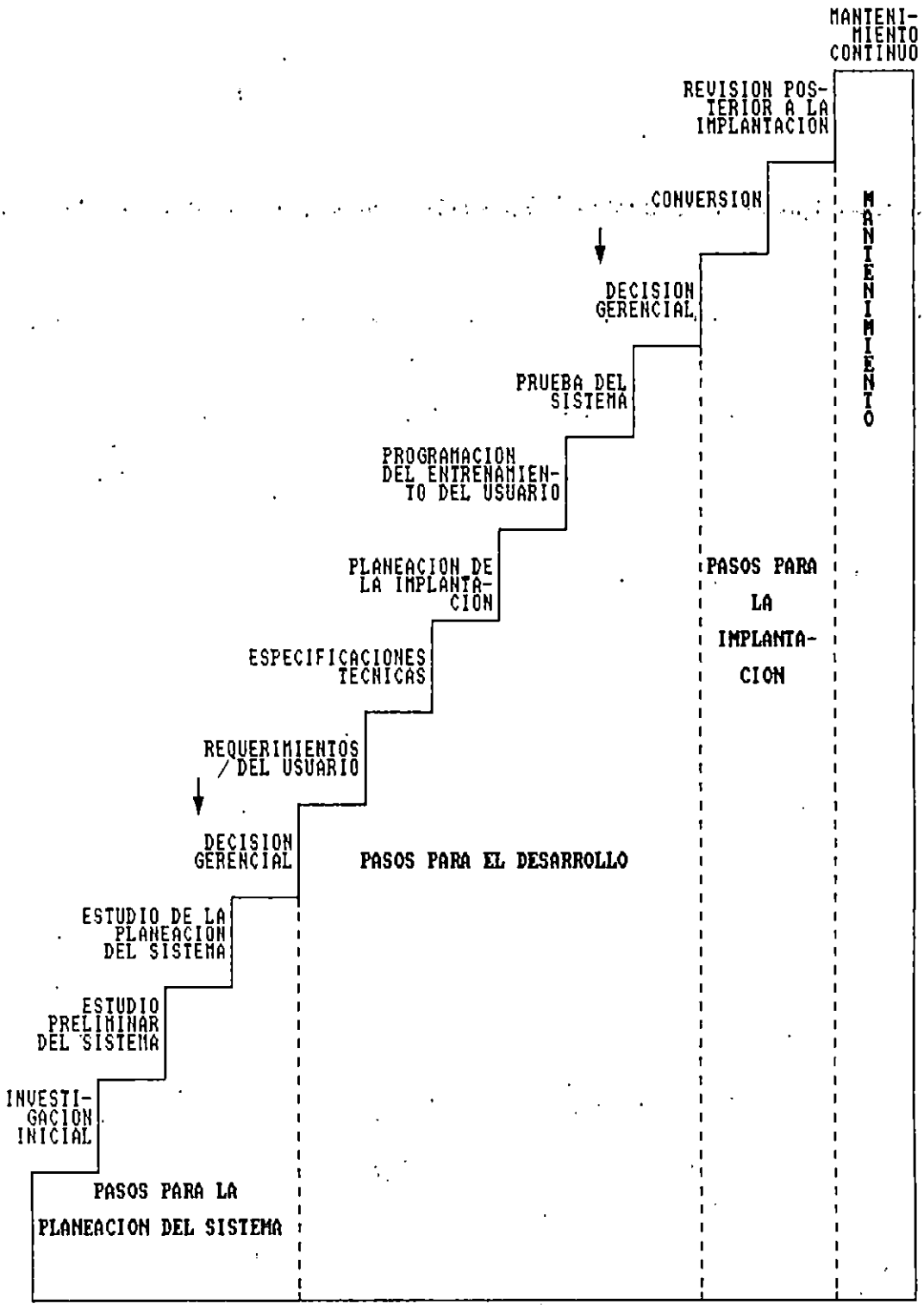
En el anexo C1 se encuentra la evaluación para el compromiso progresivo.

A continuación se encuentra diagramada la estructura de un proyecto de desarrollo de sistemas.

Si es que se cuenta con un proceso definido de desarrollo de sistemas, acá se muestra un proceso estándar con el cual tener una comparación. Vale de nuevo repetir que no es la única manera de hacer el desarrollo de sistemas sino una manera general.

La figura siguiente muestra la estructura de un proyecto de desarrollo de sistemas:

PRINCIPALES PASOS EN EL PROCESO DE DESARROLLO DE SISTEMAS



Esta figura representa a las actividades del proyecto de sistemas como una serie de pasos. El proyecto debe comenzar con una investigación inicial de las ideas respecto a los sistemas potenciales y culmina una vez que se han definido las actividades y se han tomado las decisiones gerenciales apropiadas con un sistema implantado, sujeto a continuo mantenimiento sobre la marcha.

El proyecto debe dividirse en tres principales fases: Planeación, Desarrollo e implantación.

Las flechas en la figura que se encuentran colocadas sobre los pasos a la terminación de cada una de las dos primeras fases indican puntos de revisión importantes. Se evalúan las actividades del proyecto, y se toman decisiones respecto a si debe continuarse con la asignación de recursos y la programación.

Todo proyecto de desarrollo de sistemas se debe estructurar en base a esfuerzos acumulativos, es decir que cada etapa o actividad descansa en gran medida sobre la anterior. El concepto de compromiso progresivo ayuda á asegurar que la asignación de recursos en cada etapa posterior del proyecto sea proporcional a los resultados obtenidos a una fecha determinada, a los beneficios esperados y a las probabilidades de éxito.

En las siguientes figuras se resumen cada una de las áreas de la estructura de los proyectos de sistemas en cuanto a su alcance y objetivo, grado de detalle, conocimientos requeridos y consideraciones respecto al control.

En virtud de que cada área tiene su propia documentación característica, las figuras resumen los requisitos de documentación para cada una de ellas.

Una vez analizadas las actividades del Desarrollo de Sistemas se evalúa si está definido el alcance y objetivo y los requisitos mínimos que plantea el modelo. (Ver anexo C2).

Si una tan sola de las actividades no es satisfactoria completamente en ese momento habrá un dictamen.

ACTIVIDADES DEL DESARROLLO DE SISTEMAS

PLANEACION DEL SISTEMA	ESPECIFICACIONES DEL USUARIO	ESPECIFICACIONES TECNICAS	PLANEACION DE LA IMPLANTACION	PROGRAMACION
Alcance y objetivo Establecer el proyecto, alcance, objetivos, economia y viabilidad al nivel necesario para la decision de la gerencia respecto a la prioridad de los recursos	Establecer especificacion detallada del nuevo sistema desde el punto de vista del usuario	Desarrollar decisiones y documentacion a nivel tecnico Transicion de las soluciones o problemas de mercantiles a tecnicos	Revisar el progreso del desarrollo Planear el equilibrio de la implantacion del nuevo sistema Reintegrar el equipo del proyecto como una unidad de trabajo una vez hecha la planeacion tecnica	Preparar la logica detallada, escribir la codificacion y probar los programas
Grado de detalle Depende de: La importancia de los costos y beneficios Su impacto sobre otras operaciones de PED El grado de alcance tecnico requerido Su posicion dentro de la actividad general de desarrollo de sistemas de la compania	Preparar documentacion completa del sistema existente y del nuevo desde el punto de vista del usuario	Diseno y documentacion detallados finales, para las porciones computarizadas de la nueva aplicacion Programas especificados a nivel del modulo para su codificacion y control Preparacion de calendarios para la programacion	Desarrollar planes y calendarios especificos para: Coversion Prueba del sistema Entrenamiento del usuario Revisar y validar el plan de programacion, modificandolo segun sea necesario	Entregar los programas de operacion que han sido probados y documentados
Habilidades requeridas Participacion de la gerencia del negocio y tecnica a nivel senior (con experiencia)	Analistas de sistemas Orientacion respecto al negocio del usuario	Casi totalmente tecnicas a nivel de supervision	Rango completo de habilidades de proyectos Revision y aprobacion de la gerencia	La actividad es totalmente tecnica La gerencia y los supervisores de programacion preparan modulos de trabajo para los programadores
Consideraciones de control Revisar el concepto de control Llevar un reporte de la planeacion de sistemas para su revision posterior Esfuerzo de auditoria limitado	La documentacion de los requerimientos sirve como principal fuente para la revision de los controles especificados para el nuevo sistema	Controles incluidos en las especificaciones tecnicas Las especificaciones de la logica del procesamiento incluyen controles La revision del control frecuentemente se pospone hasta la actividad siguiente	Punto de revision mayor de control, ya que todos los controles han sido especificados para la conversion y operacion sobre la marcha Revisar las guias para participacion y examen de auditoria posterior a la implantacion Las pruebas de auditoria pueden ser especificas	

ACTIVIDADES DEL DESARROLLO DE SISTEMAS

PROCEDIMIENTO Y ENTRENAMIENTO DEL USUARIO	PRUEBA DEL SISTEMA	CONVERSION	REVISION POSTERIOR A LA IMPLANTACION	MANTENIMIENTO CONTINUO
Alcance y objetivo Se llevan a cabo simultaneamente a la programacion Los usuarios son entrenados para operar el nuevo sistema Se preparan los manuales para los usuarios	Pruebas completas del sistema integrado Certifica que esta listo para ser usado	Implantar el nuevo sistema para uso continuo Lograr los beneficios previstos	Determinar que tan bien logro los objetivos el sistema Medir y evaluar los beneficios obtenidos	Cambiar el sistema segun sea necesario para hacer frente a los requerimientos externos y hacelo mas util
Grado de detalle Todo el personal usuario debe ser entrenado	Prueba: Programas Operaciones del computador Actividades del usuario Grupo de control	Los usuarios toman posecion del sistema El personal de operaciones y control de PED inician sus funciones normales	El personal de auditoria y de supervision o de la gerencia participan	Generalmente es llevado a cabo por personal tecnico de PED
Habilidades requeridas Principalmente los usuarios Analistas de sistemas, apoyo y supervision	Los usuarios efectuan las funciones finales El personal de PED opera las funciones del computador Los analistas y programadores de sistemas toman nota de las excepciones y se encargan de ella	Todo el personal del ususario, los analistas de sistemas y el de operaciones de PED esta activo	La gerencia y supervision del usuario, PED y auditoria	Supervision del usuario y personal tecnico de PED
Consideraciones de control Revisiones de control de: Manuales de procedimientos Descripciones funcionales del trabajo	Intereses de control: Resultados de las pruebas Documentacion y manejo de las excepciones Aprobaciones	Documentos de control de la conversion de archivos Reportes iniciales de operacion del nuevo sistema Aprobacion de la operacion o "desiciones de compra"	Auditoria Operacional?	Asegurar un control y documentacion continuos

Si se tienen definidas las actividades del desarrollo de sistemas el siguiente paso de evaluación es conocer de que manera se está haciendo. Para ello se tomará en cuenta cada una de las actividades de desarrollo:

a) **PLANEACIÓN DE SISTEMAS**

La actividad de planeación de sistemas puede implicar del 10 al 15 % del trabajo de todo el proyecto y puede dividirse en tres actividades (investigación inicial, estudio preliminar del sistema y estudio de la planeación del sistema). Tal división de las actividades parecería particularmente cuando un nuevo sistema promete un impacto importante y cuando la probabilidad de continuar con su desarrollo es proporcionalmente alta.

Cuando sea un proyecto sencillo desde el punto de vista técnico y los usuarios estén bien versados en aplicaciones, la planeación de sistemas puede convertirse en una sola actividad corta que no exceda del 5 % de los gastos totales del proyecto. Ver anexo C3.

b) ESPECIFICACIONES DEL USUARIO

La actividad de especificaciones del usuario está encaminada al desarrollo de un planteamiento de los problemas del negocio y las especificaciones para su resolución.

La actividad se realiza mediante esfuerzos conjuntos de los usuarios y de los analistas como miembros del equipo de proyectos. Este equipo examina todos los procedimientos manuales y computarizados relativos y las relaciones entre la aplicación que se está desarrollando y otras aplicaciones adyacentes a la misma.

En esta actividad *se consulta al supervisor o gerente de programación respecto a la viabilidad técnica y las estimaciones de los requerimientos de tiempo y de programación*; pero las especificaciones técnicas del equipo de computación, los programas de operación todavía no se tratan en detalle.
Ver anexo C4.

c) ESPECIFICACIONES TÉCNICAS

La actividad relativa a las especificaciones técnicas sirve de enlace entre los niveles de negocios y técnicos de la actividad de proyectos. El proyecto se lleva hacia el punto en

donde se genera la lógica del procesamiento y manejo de archivos que requieran el computador y el programador. Los productos finales de esta actividad incluyen la documentación que cubre una serie de restricciones técnicas y operacionales para el sistema. Las tareas dentro de esta actividad son llevadas a cabo por especialistas o gerentes de alto nivel, en las áreas de equipo de computación y programas de operación del departamento de sistemas.

Los resultados de esta fase deben consistir en una serie completa de especificaciones que podrían ser adecuadas para el desarrollo total del programa detallado y las instrucciones del usuario.

Ver anexo C5.

d) PLANEACIÓN DE LA IMPLANTACIÓN

Una vez que se han concluido las especificaciones técnicas es aconsejable una actividad de planeación de implantación por separado, particularmente en los proyectos grandes.

La planeación de la implantación es el último punto planeado para la evaluación, el análisis y los cambios a la aplicación que se está desarrollando, antes de que se lleve a cabo el desarrollo real del nuevo sistema. En las actividades inmediatas

posteriores a la planeación de la implantación. El proyecto sigue simultáneamente dos caminos, en los que (1) Se describen los programas de aplicación finales y se lleva a cabo el entrenamiento del usuario y (2) El trabajo empieza con la creación de archivos maestros para soportar las porciones del procesamiento computarizado de la nueva aplicación.

La actividad de planeación de la implantación, es en cierto sentido un punto crítico de la estructura del proyecto. Aún ha de invertirse el 60 % del tiempo y del costo, pero las porciones más creativas del proyecto ya se encuentran básicamente terminadas. Además ya se han realizado la mayoría de consideraciones de filosofía y control gerenciales. Una vez que se concluye la planeación de la implantación, el proyecto se orienta a los aspectos mecánicos. Por esta razón una vez terminada esta fase deben quedar pocas incertidumbres.

El no invertir el tiempo necesario para efectuar esta importante actividad es probablemente la razón principal de las desilusiones y fallas en proyectos grandes de desarrollo de sistemas. (esta como las otras etapas, tienen también límite de tiempo. Pero de ser necesario, debe tomarse el tiempo que se considere necesario para finalizar esta actividad)

Ver anexo C6

e) PROGRAMACIÓN

La programación es una actividad totalmente técnica que se inicia en base a la documentación obtenida de las especificaciones técnicas. Esta actividad da como resultado programas de aplicación terminados que han sido compilados del lenguaje de programación al lenguaje objeto, y que han sido probados. Otros productos finales incluyen las instrucciones de operación necesarias para correr los programas, y el enlace entre los programas de aplicación y los elementos asociados de los programas de operación del sistema, incluyendo las rutinas de utilería y el sistema operativo.

Ver anexo C7.

f) PROCEDIMIENTOS Y ENTRENAMIENTO DEL USUARIO

Simultáneamente a la actividad de programación, se preparan procedimientos y materiales de entrenamiento para que el usuario pueda convertir y operar la nueva aplicación. Se pretende la participación máxima de los usuarios para asegurar que entiendan la aplicación y que estén preparados para llevarla a cabo según lo especificado.

Ver anexo C8.

g) PRUEBA DEL SISTEMA

Sobre una base planeada, todos los elementos funcionales de la nueva aplicación (programas, procedimientos manuales, archivos de prueba y el personal), se combinan para probar la aplicación completa. El objetivo es presionar al sistema en un intento de hacerlo fallar. Después se analizan las deficiencias para determinar las acciones correctivas apropiadas.

Una prueba concentrada, durante la cual el sistema se sobrecarga concientemente, maximiza el número de "errores" que pudieran aparecer.

Ver anexo C9.

h) CONVERSIÓN

La actividad de conversión comprende la transición de todo el equipo de archivos y procedimientos manuales, de la aplicación anterior a la nueva. La magnitud de esto puede variar muchisimo. Con frecuencia la conversión requerirá un mayor trabajo respecto a la adquisición de datos especiales y los programas de computador. El no reconocer la cantidad de trabajo involucrado en la conversión y el no dar secuencia y programar con cuidado las tareas obstaculizarán seriamente el éxito de todo el

proyecto. En esta fase se implanta la nueva aplicación.

Ver anexo C10.

i) REVISIÓN POSTERIOR A LA IMPLANTACIÓN

Una vez que el sistema de procesamiento de datos ha sido implantado y se encuentra funcionando debe establecerse una práctica para efectuar una revisión encaminada a alcanzar los logros alcanzados, contra los planes originales. El objetivo de este punto es medir el grado de eficiencia del proyecto, así como utilizar esta actividad como una experiencia de aprendizaje.

La revisión posterior a la implantación con frecuencia se efectúa aproximadamente de tres a seis meses después de la conversión. Con base en los resultados, puede ser deseable programar una segunda revisión para asegurar que se hayan resuelto todos los puntos pendientes..

La práctica de las revisiones posteriores a la implantación sirve para:

* Afinar los conocimientos relativos al desarrollo de sistemas.
* Identificar posibles áreas de modificación o mejoras a los métodos de desarrollo de sistemas.
* Sugerir posibles técnicas de control de proyectos, a fin de

minimizar los problemas encontrados en los trabajos anteriores.

Ver anexo C11.

j) MANTENIMIENTO CONTINUO

El especificar una actividad y un mecanismo para el mantenimiento continuo es reconocer que el cambio siempre se da en este medio. Cada proyecto deberá producir documentación e integrar la opción de modificar la aplicación implantada conforme cambien los requerimientos.

Las razones para modificar los sistemas implantados pueden clasificarse en dos amplias categorías:*cambios obligatorios y mejoras*.

Los *cambios obligatorios* en las aplicaciones existentes normalmente se inician por una de dos razones: se descubren discrepancias o errores en la aplicación según fue implantada originalmente, o bien los requerimientos del negocio exigen modificaciones. Las discrepancias saldrán a la luz a través del ejercicio de los controles establecidos en la aplicación, o a través de incidentes que pongan de manifiesto que han ocurrido errores.

Los cambios obligatorios para satisfacer las necesidades del negocio se derivan principalmente de regulaciones gubernamentales o de cambios en otras aplicaciones adyacentes, como el caso de cambios en los porcentajes de deducción de las nóminas.

Las *mejoras* a las aplicaciones que ya están en uso se originan por las mismas razones básicas que dieron lugar al proyecto de desarrollo para la aplicación misma.

Una segunda razón para el mejoramiento de la aplicación radica en las modificaciones que se efectúan para mantenerse al día o para desarrollar los nuevos desarrollos relativos a los equipos de computación o los programas de operación.

Ver anexo C12.

6.3 AUDITORIA AL SUBSISTEMA DE ADMINISTRACIÓN DE DATOS

La administración de datos tiene una característica importante que debe ser considerada al practicar una auditoría de sistemas en esta área: La función del administrador de datos (DA) y del administrador de la base de datos (DBA).

Si alguna de estas funciones no está definida formalmente en la instalación, debe procederse a realizar las recomendaciones del caso para crear estos cargos y definir sus responsabilidades. En toda área de procesamiento de datos, sin embargo estas tareas son ejecutadas en alguna medida por el personal de la misma.

Es posible que en algunos sistemas no se cuente con un sistema de administración de bases de datos, en cuyo caso las funciones del DBA no serán definidas. También es factible que en algunas instalaciones esta área no requiera de personal destinado a tiempo completo para ejecutar las funciones, por lo que se puede compartir esta labor con el desempeño de otras tareas relacionadas.

La calidad de la administración de datos depende directamente de la existencia y de la calidad del DA y el DBA.

Así se evalúa la integridad de la base de datos y las funciones del DA y DBA.

Ver anexo D.

6.4 AUDITORIA AL SUBSISTEMA DE ADMINISTRACIÓN DE SEGURIDAD

La seguridad en los centros de cómputo es de suma importancia, esto se debe a que un sistema necesita que sea custodiado con profesionalismo para asegurar la confidencialidad y resguardar los equipos de cualquier eventualidad, por el grado de importancia que el sistema informático representa.

CRITERIOS NECESARIOS PARA EVALUAR EL SUBSISTEMA

6.4.1 SEGURIDAD FÍSICA

En el anexo E1 se encuentran los criterios necesarios para poder evaluar la seguridad; de tal forma que se pueda comparar con las condiciones existentes en relación al tema.

6.4.2 SEGURIDAD A LOS ARCHIVOS Y PROGRAMAS

Es necesario obtener una seguridad razonable sobre el nivel de protección de la información y de los programas que se encuentran en medios magnéticos, para evitar su destrucción, modificación parcial o total es el objetivo de esta evaluación. Ver anexo E2.

6.4.3 PLANES DE CONTINGENCIA.

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

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia se tenga la seguridad que funcionará.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se han de utilizar respaldos(posiblemente en otras instituciones).Hay que cambiar la configuración y, posiblemente se tengan que usar algunos métodos manuales, no sólo simulando un ambiente ficticio cercano a la realidad sino considerando que la emergencia existe.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo; en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración y el sistema operativo, en discos, etc.

Las revisiones al plan se deben realizar cuando se haya efectuado algún cambio en la configuración del equipo o bien en periodos semestrales. Una de las principales objeciones al plan

de emergencia es su costo; pero como en el caso de un seguro contra incendio, sólo podemos evaluar sus ventajas si desafortunadamente el desastre ocurre.

El plan de emergencia, una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia. La estructura del plan debe ser tal que facilite su actualización.

Algunas emergencias pueden no afectar a toda la instalación, sino a algunas partes tales como la discoteca y la cintoteca.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática (por ejemplo, el

jefe de análisis y programación y de auditoría interna). Cada uno de ellos debe tener tareas especificas como la operación del equipo de respaldo, la interfaz administrativa, de logística; por ejemplo, el proporcionar los archivos necesarios para el funcionamiento adecuado. Cada miembro del grupo debe tener asignada su tarea con una persona de respaldo para cada uno de ellos. Se deberá elaborar un directorio que contenga los nombre, direcciones y números telefónicos.

Ver instrumento en anexo E3.

6.5 AUDITORIA AL SUBSISTEMA DE ADMINISTRACIÓN DE OPERACIONES

La administración de operaciones es responsable por el funcionamiento de las instalaciones de procesamiento de datos, de tal manera que las aplicaciones puedan funcionar correctamente, y el personal del área realice normalmente sus funciones.

Ver anexo F.

6.6 AUDITORIA AL SUBSISTEMA DE SOPORTE TÉCNICO

El subsistema de soporte técnico es responsable por el desarrollo y mantenimiento de programas y procesos que interactuan con los programas de soporte del sistema, es decir utilitarios, que proveen de funciones generales en la instalación.

Este grupo es responsable de lidiar con errores que se presenten con relación al sistema operativo, el funcionamiento de la red de comunicaciones, en las herramientas de desarrollo de sistemas, en el paquete administrador de la base de datos, etc.

Ver anexo G.

7. EJECUCIÓN DE LA AUDITORIA: EL SISTEMA INFORMÁTICO

7.1 AUDITORIA DE LOS ACCESOS AL SISTEMA INFORMÁTICO

7.1.1 CONSIDERACIONES PREVIAS ACERCA DEL SISTEMA DE ACCESOS

Recuerde que el acceso restringido al centro de cómputo, no significa que los accesos al Sistema Informático están controlados al 100%, esto es claro especialmente cuando se usan terminales o procesamiento on-line.

El elemento clave para accesar un sistema consiste en **la autorización**. Autorización del usuario y autorización de los usos que dicho usuario puede hacer del sistema.

Básicamente se deben evaluar:

a) **la seguridad física de las terminales**, cuando sea posible.

- terminales en cubículos con llave

(Idem a la seguridad de el centro de cómputo)

b) **Los controles de autorización**

- Los usuarios, deben ser restringidos en los usos del sistema, de acuerdo a las políticas de la gerencia.

TERMINALES AUTORIZADAS El sistema debe estar provisto de un listado de terminales autorizadas a fin de detectar aquellas terminales "piratas". Una terminal puede tener accesos de acuerdo con la localización física dentro de la organización.

USUARIOS AUTORIZADOS Puede basarse en la autoridad y responsabilidad de el usuario dentro de la organización. Tomándose en cuenta por ejemplo que el gerente de personal, aunque tiene acceso a la planilla de salarios de todos los miembros de la organización, no podría accesar al registro del vicepresidente.

COMO ESTA IMPLEMENTADO UN SISTEMA DE AUTORIZACIONES

A través de una tabla de autorizaciones. Es decir una lista de los programas y datos que a cada terminal y cada usuario le es permitido accesar, en dicha lista se identificarán actividades que cada usuario esta autorizado a desarrollar con cada programa y grupo de datos. Esta tabla debe ser consultada cada vez que un usuario cualquiera desee usar un programa o dato, para verificar que el usuario tiene la apropiada autorización.

Enllavado de datos de registros. Son controles que indican cual terminal o usuario puede leer un registro o campo y para que propósito. El enllavado puede estar ubicado en el registro como un campo separado, en una tabla separada o en un índice usado para las direcciones del registro.

COMO CONTROLAR LA IDENTIFICACIÓN

A fin de ser efectivo, el esquema de autorización, **debe ser obligatorio.** El proceso de identificación es llevado a cabo por un método de identificación de la terminal y el usuario, de tal forma que el acceso pueda garantizado con base en el esquema de autorización.

Identificación de la terminal. Asegurarse que el computador está unido con una terminal autorizada. De no realizarse esta comprobación, podría existir la posibilidad de que una terminal pirata se haga pasar por una terminal autorizada del sistema. En algunos sistemas, la identificación de la terminal es proporcionada en respuesta a una petición del sistema operativo del computador. En otros sistemas, es dado por la misma terminal cuando esta entra en línea.

Identificación del usuario. Puede realizarse a través de la indagación de uno o varios de los aspectos siguientes:

- Características personales y fisiológicas, tales como las huellas dactilares, el tono de la voz, forma y tamaño de las manos, la firma.
- Objetos poseídos, tales como tarjetas plásticas, códigos barras (con lectores ópticos), llaves. etc.
- Información memorizada (passwords), el cual es un método sumamente económico, que consiste en expresar un código que permite identificar la identidad del usuario o su autoridad. Dichos códigos pueden ser simples o complejos. Los passwords son más efectivos cuando se utilizan procedimientos para reducir la oportunidad de descubrir y utilizar el código.
    - Los passwords simples son almacenados en un archivo de passwords. El password se asigna al sistema de recursos y actividades, a través de ellos se le permite al usuario las libertades de acuerdo con el esquema de autorizaciones. La inclusión de los passwords en las instrucciones del control del trabajo, requiere que se ejecute un programa que permita o niegue al usuario, el acceso a programas y archivos, y la autorización para desarrollar actividades específicas tales

como lecturas, modificaciones, adiciones o borrado de datos.

- Los passwords pueden ser mejorados al incrementar la complejidad de el código. Un ejemplo es el uso de una secuencia de preguntas y respuestas (dialogo) entre el usuario en la terminal y el computador. En forma aleatoria el sistema solicita información previamente archivada sobre datos personales (algunos triviales y otros complejos), tales como su fecha de nacimiento, números de identificación, nombres de familiares, gustos personales, etc.

Los passwords son inefectivos cuando

* son muy fáciles de descubrir, así como lo sería la fecha de el cumpleaños del usuario.
* se publican en periódicos murales.
* se despliegan en la pantalla al momento de su introducción.
* se encuentran en un archivo de passwords que está desprotegido.

* sino se está cambiando periódicamente. (especialmente cuando alguien cambia de puesto o deja de trabajar en la organización)

- Cuando el sistema será accesado por un sistema de comunicación de datos, pueden ser recomendables el uso de técnicas como la comunicación por fragmentación, intermezclado y encriptamiento.

Ver metodología de evaluación en anexo H.

7.2 AUDITORIA AL SUBSISTEMA DE ENTRADA

La evaluación a los controles sobre la entrada de datos puede estar combinada entre procesos manuales y automatizados.

Los procesos manuales presentan un mayor riesgo de modificaciones a los datos fuente, al poder suprimir u omitir datos, adicionar datos, alterar datos o duplicar procesos.

Los procesos automatizados pueden presentar este riesgo, para lo cual habrá de establecerse controles; pero el énfasis del control dependerá del lugar donde se han generado estos datos (es

ahi donde deberá existir un mayor sistema de control de calidad de esos datos).

Para poder evaluar este subsistema de entrada deberán considerarse los elementos siguientes:

* La dirección del sistema.
* Evaluación de datos de entrada directa.
* Evaluación de la codificación.
* Evaluación de los documentos fuente.
* Evaluación al ingreso y validación.
* Control de recuperación de datos.
* Pistas de auditoria.
* Control de los datos y cifras de control.

Ver instrumento en anexo I.

7.3 AUDITORIA AL SUBSISTEMA DE PROCESO

La evaluación al subsistema de proceso se hará en cuatro partes: control de las operaciones, control de asignación de trabajo, control de medios de almacenamiento y control de mantenimiento.

7.3.1 CONTROL DE LAS OPERACIONES

La eficiencia y el costo de operación de un sistema se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso. Los instructivos de operación proporcionan al operador información sobre los procedimientos que debe seguir en situaciones normales y anormales en el procesamiento. Si la documentación es incompleta o inadecuada lo obliga a improvisar o suspender los procesos mientras investiga lo conducente, generando probablemente errores, reprocesos, desperdicio de tiempo de máquina, incrementándose pues, los costos del procesamiento de datos.

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

Ver anexo J1

7.3.2 CONTROL DE ASIGNACIÓN DE TRABAJO

Esta evaluación se relaciona con la dirección de las operaciones en términos de la eficiencia y satisfacción del usuario. Esta evaluación debe ser comparada con la opinión expresada por el usuario.

La función clave del programador está relacionada con el logro eficiente y efectivo que:

*Satisfaga las necesidades de tiempo del usuario.

*Sea compatible con los programas de recepción y transmisión de datos.

*Permiten niveles efectivos que utilización de los equipos y sistemas de operación,

*Es ágil la utilización de los equipos en línea.

Los mejores resultados se logran en organizaciones que utilizan sistemas formales de programación de actividades, los cuales intentan balancear los factores y medir resultados.

Ver anexo J2

7.3.3 CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO

Los dispositivos de almacenamiento representan para cualquier sistema, archivos extremadamente importantes, cuya pérdida parcial o total podría tener repercusiones muy serias, no solo en la unidad de informática, sino en la dependencia de la cual se presta servicio.

Un buen control debe garantizar la protección de estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Ver anexo J3.

7.3.4 CONTROL DE MANTENIMIENTO

Este instrumento consta de tres partes: Control del mantenimiento, control de fallas y evaluación del mantenimiento.

7.3.4.1 CONTROL DE MANTENIMIENTO

Existen 3 tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes del contrato y el que no incluye las partes. El contrato que incluye refacciones es prácticamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente el más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de los daños por negligencia en la utilización de los equipos (este tipo de mantenimiento normalmente se emplea en equipos grandes).

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

El tercer tipo de mantenimiento es el que se conoce como "en banco", y es aquel en el cual el cliente lleva a las oficinas del

proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura mas las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Ver anexo J4.

7.3.4.2. CONTROL DE FALLAS

La evaluación al control de fallas puede verse en el anexo J5. Este evalúa fallas en dispositivos del sistema y servicios auxiliares, actividades de las personas de servicios, tiempo involucrado, efectividad del control y fallas.

7.3.4.3 EVALUACIÓN DEL MANTENIMIENTO

Cuando se evalúa la capacidad de los equipos, no se debe olvidar que la capacidad bruta disponible se deberá disminuir por las actividades de mantenimiento preventivo, fallas internas o

externas no previstas e instalación de nuevos sistemas.

El enfoque de esta parte del instrumento se orienta a evaluar, a través de los controles que se tengan en la dirección, la utilización del sistema. Un control adecuado permitirá sustentar sólidamente cualquier solicitud de expansión de la configuración presente.

Ver anexo J6.

7.4 AUDITORIA AL SUBSISTEMA DE SALIDA

La auditoría al subsistema de Salida evalúa el control de presentación de los informes generados por cada uno de los programas, control a los informes, controles a la posible inferencia, controles a la producción y controles de preparación.

Ver anexo K.

7.5 AUDITORIA AL SISTEMA DE BASES DE DATOS

La auditoría a los sistemas de bases de datos se desarrolla en cuatro categorías: los criterios de funcionamiento, las características necesarias, características deseables y los controles indispensables.

7.5.1 CRITERIOS DE FUNCIONAMIENTO

TIEMPOS DE ACCESO Debe evaluarse el tiempo de acceso, es decir el tiempo que transcurre entre la petición de datos y su aparición en pantalla. Si, por ejemplo en un banco, pregunta por el saldo de la cuenta del cliente 114-045213-9, habría una ligera demora antes de que aparezca el valor en colones. Tome en cuenta que los tiempos de acceso dependen del hardware de la computadora y particularmente del disco duro. Cuando se comparen sistemas de bases de datos diferentes, hay que asegurarse de que la configuración del hardware es la misma para cada uno. Además el número de Hertz de una configuración con respecto a otra influye en la rapidez en que un programa pueda ser ejecutado. Otro criterio del tiempo de acceso es el método de acceso: directo, indexado o secuencial (el hacer comparaciones significativas depende del conocimiento del método de acceso que se esté empleando in situ). Debe tomar en cuenta que el método de acceso directo no depende del sistema de gestión de base de datos (DBMS será usado en adelante para referirse a un sistema de gestión de base de datos, por sus siglas del Inglés Data Base Management System), el método directo es el más rápido y depende entonces únicamente de la velocidad del disco. El hecho de

que un sistema de base de datos sea lento debería ser compensado con algunas ventajas para merecer su consideración.

VELOCIDAD DE PROCESAMIENTO Las consideraciones de la velocidad del disco se aplican a la velocidad del procesamiento y al tiempo de acceso, siendo la clasificación y la indexación las pruebas más importantes de velocidad. Debe practicar con archivos grandes que estén fuera de servicio para medir conscientemente los tiempos de clasificación. Se puede adquirir un programa de clasificación exterior si la clasificación incorporada es demasiado lenta. No debe olvidarse que el tipo de DBMS de red o jerárquico no requiere intrinsecamente ninguna clasificación. El conocer las preguntas que se hagan con más frecuencia puede ayudar a que los datos se dispongan para un acceso más rápido.

CAPACIDAD DE ALMACENAMIENTO DE LOS DATOS En algunos casos el sistema operativo podría tener ciertas limitaciones incorporadas para los archivos. Debe considerarse el tamaño del disco duro y si no fuera suficiente, evaluar la compresión de los datos dentro del espacio del disco de que se dispone.

Debe evaluar las definiciones de las longitudes de los

campos (remitiéndose al diccionario de datos).

Para determinar el espacio requerido por cada archivo basta añadir todas las longitudes requerida por todos los campos de un registro y multiplicar por el número de registros por archivo. Hay que doblar este número para permitir la disposición de espacios para indices y algún espacio de trabajo para clasificación, extracción y reorganización.

LIMITACIONES INCORPORADAS DE ALGUNOS DBMS Las limitaciones entre un DBMS y otro varían mucho, y deben examinarse a la luz de sus aplicaciones específicas. Podrían ser de interés en una aplicación particular un máximo de campos por registro, o cierto número de dígitos (p.e. un sistema de contabilidad para manejo de balances superiores a 99,999,999.99), debe considerar si están permitidos los exponentes, cuantos archivos puede utilizar a la vez. Debe considerar los tipos de datos que están permitidos: casi todos ofrecen los tipos lógicos, de carácter y numéricos; otros ofrecen el signo de colón, fecha del calendario juliano, sonidos, imágenes, etc.

7.5.2 CARACTERÍSTICAS NECESARIAS

DICCIONARIO DE DATOS Debe verificarse existe, se espera que sea el corazón de la base de datos, y que en ella se explique casi todo lo relacionado a los datos, así como la descripción de los archivos simples o de los archivos de base de datos.

Cada acampo tiene una entrada de diccionario de datos con la información mínima siguiente: -El nombre o número del campo, -El tipo de datos que contiene el campo, -La longitud de dicho campo.

MEDIOS DE CONSULTA Debe haber una forma, para personas que no sean programadores, de ver y actualizar los datos, cuanto más potentes sean estos medios, tanto mejor, pero la potencia no deberá comprometer la facilidad de su empleo. En algunos casos pueden realizarse a través de menús o a través de órdenes (realmente un lenguaje especial de consulta) para tener acceso a la base de datos.

GENERADOR DE INFORMES La demanda más común en un departamento de procesamiento electrónico de datos es la de informes especiales que muestren los datos en un cierto orden con totales y subtotales, más los encabezamientos de columnas

en cada página. Un programador contratado podría cobrar muy altos honorarios por escribir un programa en COBOL para escribir un informe de extensión media, pero puede utilizar un DBMS para hacer el trabajo en menos de una hora.

Un buen generador de informes deberá permitir seleccionar ciertos datos para la impresión, tanto de los campos como de los registros. Puede considerarse que el generador de informes es una extensión del lenguaje de consulta pero orientado al papel.

COMPATIBILIDAD DE ARCHIVOS CON OTROS PROGRAMAS Es importante la característica de poder importar y/o exportar datos desde o hacia otros sistemas, esta característica no debe olvidar evaluarse.

CAPACIDAD DE REESTRUCTURACIÓN Muchos datos son dinámicos, como el caso de un precio de venta. Si las definiciones originales de los campos no permiten cierta flexibilidad en cuanto a la re-definición de la estructura de la base de datos, entonces a un corto plazo se tendrán serias dificultades. Al ménos debe preverse que la definición actual haya sido considerada para un periodo mínimo de cinco años.

MANIPULACIÓN EFECTIVA DE ERRORES Cuando se comete un error, el DBMS no ha de destruir todos los datos de la base de datos. Debe evaluarse si el sistema de gestión realiza copias de seguridad frecuentemente. Otro aspecto que debe evaluar es el que el sistema proporcione mensajes de error útiles y claros y que permitan corregir el problema. Tome en cuenta que es difícil la recuperación a partir de problemas de hardware, pero sí debe admitirse directorios y discos completos, impresoras fuera de línea, etc. Si el disco está lleno, el sistema debe avisarle y permitirle el borrado de los archivos innecesarios. Todo DBMS debe estar orientado a recuperase después de un fallo del sistema. Evalúe además si a medida que se actualiza la base de datos, registros de transacciones especiales han de ser grabados en cinta o discos. Después de una circunstancia desastrosa, los archivos de disco han de ser recargados a partir de la copia de seguridad anterior y las transacción se reproduce en un programa especial de recuperación que reconstruye la base en el punto del fallo. por lo general el problema que ocurre es que aproximadamente la mitad de los esfuerzos de programación del proyecto se van a la planificación de esta recuperación, pero suele ocurrir que el programa no trabaja cuando llega el momento oportuno.

BUENA DOCUMENTACIÓN Y APOYO DEL SOFTWARE A todo DBMS debe acompañarle un manual, el cual ofrece ciertos conocimientos que el permiten al usuario recorrer el sistema paso a paso. El manual debe tener también un sección de referencia organizada por orden o función. Lo deseable sería recibir cierta capacitación por el diseñador del sistema o el distribuidor del mismo.

7.5.3 CARACTERÍSTICAS DESEABLES

Existen muchos DBMS que no poseen las siguientes características, sin embargo, en algunos lugares serán necesarias y no se dispondrán.

ARCHIVOS MÚLTIPLES Debe poder trabajarse con más de un archivo de datos a la misma vez. El punto es que se pueda y no se haga.

EDICIÓN DE PANTALLA COMPLETA Debe evaluarse que se haga buen uso de la pantalla durante la interacción con el DBMS. Por ejemplo el paso desde las boletas de capturas de datos hasta la introducción de los datos en el computador puede que no sea adecuada. Esto implica que el auditor deberá echar a andar el sistema y ejecutar algunas transacciones. Es necesario evaluar con buen juicio crítico la

distribución de los datos e la pantalla, que sea agradable, no saturada ni difícil de encontrar los datos mas importantes, además no deberá contener adornos que dificulten la lectura de los datos, evalúe los colores en las pantallas, sólo deben aparecer en las pantallas de información (salidas) lo necesario; igual en las entrada, sólo captura de los datos indispensables.

Es en las pantallas de edición se deben validar los datos introducidos, esto para mantener la integridad de los datos.

GENERACIÓN DE FORMATOS DE PRESENTACIÓN VISUAL EN PANTALLA Debe evaluar los formatos de visualización, ya que es lo que se ve cuando se comienza a introducir o a cambiar datos para un registro base de datos dado. está constituido por las etiquetas descriptivas y por los espacios en blanco para los campos, todo dispuesto de una manera agradable. Un buen generador de formatos le permitirá utilizar gráficas, video inverso subrayados y otros medios de terminal y también permitirá la gama de funciones de inserción y borrado comunes a los procesadores de texto. También le permitirá cambiar una pantalla antigua.

SEGURIDAD CON PALABRAS DE PASO Existen muchos campos confidenciales en toda base de datos, algunos de ellos se pueden consultar por algunas personas, y será posible modificarlos por otras. Si el sistema de gestión de base de datos no cuenta con esta característica importante, entonces no se puede garantizar la confidencialidad ni la privacidad de los datos.

Puede recomendar un sistema de seguridad basado en códigos de seguridad: 0 es una seguridad baja y 3 es una seguridad alta. Si usted es el encargado de personal y si recordar su palabra de paso podría utilizar su código de seguridad (por ejemplo 1) para examinar todos los campos con su nivel de seguridad o más bajo. Tendría asignado un código de seguridad para actualizaciones (suponga 1) entonces no sólo podría examinar (consultar/accesar) sino modificar el contenido de los campos que estén marcados con este código o menor.

Ya que se habría hecho mucho esfuerzo por proteger ciertos campos, se debe estar seguro que el DBMS no permitirá a personas desautorizadas hacer una lista de datos que involucre a los campos confidenciales.

No solamente los valores de los datos, sino también las relaciones están sometidas a la seguridad.

Toda esta capacidad de palabras de paso deberá ser

correctamente incorporada al DBMS, los niveles de seguridad para campos se introducen en el diccionario de datos junto con la longitud del campo, tipo de dato, etc. Las palabras de paso se introducen en una sección especial del diccionario sobrentendiendo que se necesita un código especial para de alta seguridad para tener acceso a ellas y modificarlas.

CAPACIDAD DE MULTIUSUARIOS Debe verificarse que se puedan realizar cierres de los registros, es decir, cuando un registro es solicitado, debe quedar automáticamente bloqueado para otros usuarios que posiblemente desean utilizarlo. El DBMS debe hacer esperarles hasta que esté disponible. Existen dos formas de bloquear un registro: activa y pasiva. En la pasiva, siempre que un registro esté siendo objeto de acceso por un sólo usuario, puede ser leído por otros pero no escrito por otros. El cierre activo evita que otro usuario lea o escriba un registro, se acciona y bloquea por órdenes especificas del DBMS.

7.5.4 CONTROLES INDISPENSABLES

ACCESOS Evalúe que sean realizados controles para prevenir ingresos no autorizados a la base de datos. Debe existir una política de seguridad.

PROGRAMAS DE APLICACIONES Verifique que los programas que utilizan la base de datos, mantengan la integridad de la base de datos.

CONCURRENCIA verificar que se mantenga la integridad de la base de datos, permitiendo a diferentes usuarios los mismos recursos en forma simultanea (evitando los deadlooks o abrazos mortales).

ENCRIPTAMIENTO/CIFRADO Evaluese este aspecto, si es que se realiza por el dbms para aquellos módulos de comunicación de datos.

ADMINISTRACIÓN DE ARCHIVOS Debe evaluarse que se cuenta con adecuados controles parar prevenir la destrucción accidental de los datos contenidos en un medio de almacenamiento. Indague si se cuentan con recursos de hardware, del sistema operativo o del DBMS.

CONTROLES DE RECUPERACIÓN Evalúe que existan controles de recuperación, que permitan la restauración de la base de datos en el evento de una falla o pérdida de información. Esto involucra pérdidas totales o parciales. Evalúe si el proceso de copias de respaldo es el adecuado a las necesidades de cada medio en particular.

PISTAS DE AUDITORIA Verifique la existencia de un módulo en la base de datos que permita mantener la cronología de eventos que ocurren durante la definición de la base de datos, y la manipulación de la misma. En este sentido debe procurarse que el conjunto completo de eventos deba ser registrado: adiciones, modificaciones, eliminaciones y consultas sobre los datos. Si esta información no se logra registrar adecuadamente, es imposible determinar cómo la base de datos llegó al estado en que se encuentra actualmente.

Ver en el anexo L, la forma en que se debe evaluar el sistema de bases de datos.

7.6 AUDITORIA AL SISTEMA DE COMUNICACIONES DE LOS SISTEMAS INFORMÁTICOS

Para tener la certeza de que la red de comunicación de datos y las estaciones de trabajo de las microcomputadoras cuentan con todos los controles necesarios y que estos controles ofrecen protección adecuada, se construirá una matriz bidimensional en la que se incorporarán todos los controles que se encuentren presentes en ese momento en la red.

La matriz se construye identificando primero todas las amenazas que enfrenta la red y, después, todos los componentes de la red.

- Una amenaza a la red de comunicación de datos es cualquier evento adverso potencial que pueda dañar la red, interrumpir los sistemas que se encuentran utilizando la red, o provocar pérdidas económicas a la organización. Por ejemplo, la pérdida de mensajes es una amenaza potencial.
- Un componente es una de las partes individuales que, cuando se ensamblan juntas, integran la red de comunicación de datos. Un componente puede considerarse un bien que se encuentra sometido a revisión o un bien sobre el que se está intentando mantener control. Así, los componentes son Hardware, Software, Circuitos, y otras piezas de la red.

Para la identificación y la documentación de los controles de una red es necesario identificar las amenazas y componentes específicos que se relacionan con cualquier red que esté utilizando la organización. Una vez que se han identificado las amenazas y componentes específicos de la organización, entonces es posible relacionar con tales amenazas y componentes los controles individuales que se encuentran en el lugar.

Las amenazas generales a las redes de comunicación son:

.Errores y omisiones. Transmisiones accidentales o intencionales de datos que contienen errores, incluyendo las omisiones accidentales o intencionales de datos que se debieron introducir o transmitir en el sistema en línea. En este tipo de riesgo se incluyen entre otras cosas datos inexactos, datos incompletos, malfuncionamiento del hardware, etc.

.Pérdida o cambio de mensajes. Pérdida de mensajes al ser transmitidos por el sistema de comunicación de datos, o su cambio accidental o intencional durante la transmisión.

.Desastres y siniestros (naturales u ocasionados por el hombre). Interrupción temporal o a largo plazo de la comunicación normal

de datos. Con este riesgo se hace inoperante el sistema normal de comunicación de datos en línea de la organización.

.Pérdida de privacia. Entrega accidental o intencional de datos acerca de un individuo, suponiendo que tal entrega de información no es parte de las actividades normales de negocios de la organización.

.Extravio/robo. Extravio o robo de información que se debe mantener confidencial a causa de la naturaleza de su propietario. En cierto modo, ésta es una forma de pérdida de privacia, pero la información que se extrae no pertenece a un individuo. La información se puede divulgar de manera inadvertida (accidental) o ser objeto de un robo intencional. En este riesgo también se incluye el robo de bienes como en los casos de malversaciones, fraude o desfalco.

.Confiabilidad (tiempo de funcionamiento). Confiabilidad de la red de comunicación de datos y su "tiempo de funcionamiento". En esto se incluye la capacidad de la organización de mantener la red de comunicación de datos en operación y el tiempo medio entre fallas (TMEF), así como el tiempo para reparar el equipo cuando funciona mal. La confiabilidad del hardware y del

software y el mantenimiento de estas dos partes son de gran interés.

.Reparación y rearranque. Capacidades de recuperación y reinicio en la red de comunicación de datos en caso de falla. En otras palabras, cómo opera el software en modo de falla? En este concepto de recuperación y rearranque se incluye el respaldo para porciones clave de la red de comunicación de datos y el plan de contingencia para respaldo, en caso de falla en cualquier punto de la red de comunicación de datos

.Manejo de errores. Metodología y controles que se utilizan para manejar los errores en un sitio remoto distribuido o en un sitio de computadora centralizada. En este concepto se incluyen los procedimientos para el manejo de errores en un sistema de procesamiento distribuido (en el sitio distribuido). El objetivo de esto es asegurar que cuando se encuentren errores, se corrijan rápidamente y los datos se introduzcan en el sistema para su procesamiento.

.Validación y verificación de datos. Validación de datos, ya sea al momento de su introducción o durante la transmisión. La validación puede efectuarse en el sitio remoto (terminal inteligente), en el sitio central (procesador de comunicación de

entrada) o en un sitio de inteligencia distribuida (concentrador o procesador de comunicación de entrada remota).

Los componentes generales de una red de comunicación son:

.Computadora principal. Su forma más común es la de una computadora central a la que transmite la red de comunicación de datos y de la que ésta recibe información. En un sistema distribuido con igual capacidad de procesamiento en cada modo distribuido, puede no haber una computadora central identificable, sino sólo otra computadora distribuida del mismo tamaño.

.Software. Programas logísticos con los que opera la red de comunicación de datos. Estos programas pueden residir en la computadora central, en un sistema de computadoras distribuidas, en el procesador de comunicación de entrada, en un concentrador o un multiplexor estadístico remotos o en una terminal remota inteligente (o en una combinación de ellos). En este software se pueden incluir los métodos de acceso, un monitor de teleproceso completo, programas que residan en los procesadores de entrada y programas que residan en terminales inteligentes.

.Procesador de comunicación de entrada. Dispositivo de hardware que interconecta todos los circuitos (líneas) de comunicación de datos con la computadora central o las computadoras distribuidas y realiza algunas de las siguientes funciones: conversión de código y velocidad, protocolo, detección y corrección de errores, verificación de formato, autenticación, validación de datos, agrupación de estadísticas de datos, exploración/direccionamiento, inserción/borrado de códigos de control de línea y funciones semejantes

.Multiplexor, concentrador, conmutador. Dispositivo de hardware mediante los cuales la red de comunicación de datos opera de manera más eficiente. El multiplexor es un dispositivo que combina en una corriente de datos, varias señales de datos simultáneas de estaciones independientes. El concentrador realiza las mismas funciones que el multiplexor, a excepción de que aquél tiene "inteligencia" y por tanto puede desarrollar algunas de la funciones del procesador de comunicación de entrada. Un conmutador es un dispositivo con el que se hace la interconexión de dos circuitos (líneas) cualesquiera conectados a él. Puede haber dos tipos distintos de conmutador: uno que realiza la conmutación de mensajes entre estaciones (terminales) y que se puede ubicar en las instalaciones de la red de comunicación de datos que pertenecen a la organización y son operadas por ella;

otro que realiza la conmutación de líneas o circuitos, con el cual se interconectan varios circuitos y que se puede localizar en la oficina central de la compañía telefónica y ser propiedad de ella. Por ejemplo, la conmutación de mensajes es realizada por las organizaciones, y la compañía telefónica se encarga de la conmutación de circuitos.

.Circuitos (líneas) de comunicación. Medios de transmisión de la empresa de comunicaciones que se utiliza como enlace (un enlace es la interconexión de cualesquiera dos terminales/estaciones) para interconectar las terminales/estaciones de la organización. Entre estos circuitos de comunicación se incluyen medios para satélite, instalaciones de conmutación pública con marcación, líneas privadas punto a punto, líneas multiplexadas, líneas privadas en configuración multipunto o de abonado y muchos otros.

.Línea de abonado (local). Medio de comunicación entre las instalaciones del usuario y el equipo central de la compañía telefónica o la central de cualquier otra empresa especial de comunicaciones. Generalmente se supone que la línea local consiste en pares de alambres metálicos.

.Modem. Dispositivo de hardware utilizado para convertir las señales de datos provenientes de las terminales (señal digital) a una forma eléctrica (señal analógica) que se acepta para su transmisión por los circuitos de comunicación que la compañía telefónica u otra empresa especial de comunicaciones posee y mantiene.

.Personal. Individuos responsables de introducir los datos, operar y mantener el equipo de la red de comunicación de da tos, escribir los programas de software para comunicación de datos, y administrar toda la red de comunicación de datos; también aquellos que se encuentran en las estaciones/terminales remotas.

.Terminales/inteligencia distribuida. Algunos o todos los dispositivos de entrada o salida que se utilizan para interconexión en línea con la red de comunicación de datos. En este recurso se incluyen específicamente, entre otros dispositivos, las terminales de teletipo, de video, de entrada remota de trabajo, de transacciones, inteligentes y cualquier otro dispositivo que se utilice con las redes distribuidas de comunicación de datos; entre éstos se pueden citar las microcomputadoras o minicomputadoras cuando funcionan como dispositivos de entrada/salida o si se utilizan para controlar partes de la red de comunicación de datos.

Una vez que se han identificado las amenazas y las partes componentes, el paso que sigue es colocar una breve descripción de cada amenaza en la parte superior de la matriz.

De igual manera, en el eje vertical izquierdo de la matriz se escribe una breve descripción de cada componente, como se muestra en la figura de la siguiente página.

Una vez que se han etiquetado los ejes horizontal y vertical, el paso siguiente es identificar todos los controles específicos que se están utilizando actualmente en la red de comunicación de datos. Estos controles *in situ* deben describirse y colocarse en una lista numerada. Por ejemplo, supóngase que se han identificado 24 controles que estaban utilizándose en la red. Se describe cada uno, además de numerarlos consecutivamente del 1 al 24. La lista de controles numerados no tienen clasificación alguna: el primer control es el número 1 sencillamente porque es el primer control identificado. Luego, cada uno de los controles identificados se coloca en el cuadro apropiado de la matriz.

Esto se logra leyendo la descripción de cada control en la lista de control y luego planteando las dos preguntas siguientes:

1. Cuál o cuáles amenazas mitigará o detendrá este control?
2. Cuál o cuáles componentes salvará o preservará este control?

AMENAZAS

COMPONENTES	ERRORES Y OMISIONES	PERDIDA O CAMBIO DE MENSAJES	DESASTRES Y SINIESTROS	PERDIDA DE PRIVACIA	EXTRAVIO, ROBO	CONFIABILIDAD	REPARACION REARRANQUE	MANEJO DE ERRORES	VALIDACION VERIFICACION DE DATOS
COMPUTADOR PRINCIPAL									
SOFTWARE									
PROCESADOR DE COMUNICACION DE ENTRADA									
MULTIPLEXOR, CONMUTADOR, CONCENTRADOR									
LINEAS DE COMUNICACION									
LINEAS DE ABONADO									
MODEMS									
PERSONAL									
TERMINALES									

AUDITORIA AL SISTEMA DE COMUNICACIONES. MATRIZ DE CONTROLES, CON AMENAZAS Y COMPONENTES GENERALES EN UNA RED DE COMUNICACION DE DATOS

Por ejemplo, si la descripción del control 1 es "asegurar que el sistema pueda conmutar mensajes de una estación/terminal caída hacia una estación/terminal alternativa", entonces se debe escribir el número 1 en la primera entrada (cuadro) en el ángulo superior izquierdo. Se asignó esta posición porque un control que asegura que el sistema puede conmutar mensajes cuando una estación se ha caído ayuda a controlar errores y también es un control que salvaguarda la computadora principal o el procesador de entrada (o ambos) o reside en ellos. Un control también puede aparecer en varios otros cuadros. La cuestión es que al responder a las dos preguntas anteriores sea posible colocar cada control en los cuadros idóneos de la matriz.

La matriz terminada con los controles mostrará la relación que tiene cada control *in situ* con respecto a la amenaza que se supone que dicho control mitiga y el componente al que salvaguarda o controla.

El último paso en el diseño de una matriz de controles para una red de comunicación de datos específica es evaluar la idoneidad de los controles. Esto se logra revisando cada subconjunto de controles según se relaciona con dada área de amenaza y de componente de la matriz. Por ejemplo, se evalúa el subconjunto de controles que constituye una columna abajo de una

amenaza. El objetivo de este paso es responder la pregunta especifica "se tienen los controles especificos y son adecuados con respecto a cada amenaza especifica?".

Este tipo de revisión también puede efectuarse para otros diferentes subconjuntos de controles. Por ejemplo, es posible evaluar subconjuntos individuales de controles según se relacionen con amenazas (columnas), componentes (filas), cuadro individuales y cuadros vacios. El método matricial constituye una herramienta perfecta para efectuar un microanálisis de controles en una red de comunicación de datos. La matriz muestra claramente la relación entre diferentes subconjunto de controles y áreas de amenazas especificas, componentes, cuadros individuales y cuadros vacios.

Algunas casillas individuales pueden ser de especial interés para una red o compañia, y por lo tanto tales casillas se deben revisar con cuidado.

Las casillas vacias significan falta de control, lo que puede ser un serio problema.[2]

El instrumento de evaluación para el sistema de comunicaciones se encuentra en el anexo M.

---

[2]Todo el procedimiento para diseñar y elaborar una matriz de controles ha sido automatizado para su uso en una microcomputadora. Existen a su disposición 3 paquetes llamados Control Matrix Methodology for Microcomputers (está disponible un disco DEMO gratis). Escribir a Jerry FitzGerald & Associates, 506 Barkentine Lane, Redwood City, California 94065.

LISTAS DE CONTROLES
PARA REDES DE COMUNICACIÓN DE DATOS

A continuación se muestran tres listas de controles en las que el auditor se puede basar para iniciar su auditoría en los siguientes aspectos:

CONTROLES DE SOFTWARE EN LA COMUNICACIÓN DE DATOS
(componente)

CONTROLES ANTE DESASTRES E INTERRUPCIONES EN LA COMUNICACIÓN DE DATOS.
(amenaza)

CONTROLES A LOS MODEMS EN LA COMUNICACIÓN DE DATOS.
(componente)

El detalle de estos controles se muestra en las páginas a continuación; por supuesto que el auditor diseñará las restantes listas de controles para todas las amenazas y componentes que hacen falta.

CONTROLES PARA REDES DE COMUNICACIÓN DE DATOS

Controles de Software

1. Asegurarse de que el sistema puede conmutar apropiadamente cualesquiera mensajes destinados de una estación/termina caida a una estación/terminal alternativa.
2. Para evitar la pérdida de mensajes en un sistema de conmutación de mensajes, contar con funciones de almacenamiento y envío, donde un mensaje destinado a una estación sea almacenado en el conmutador central y se envíe más tarde cuando la estación ya no esté ocupada.
3. Revisar làs capacidades de registro de mensajes o transacciones para reducir la pérdida de mensajes, contar con un rastreo de intervención, restringir mensajes, prohibir mensajes ilegales, etc. Tales mensajes pueden alojarse en la estación remota (terminal inteligente), en un concentrador remoto/procesador de entrada remoto, o en el procesador de comunicación de entrada central/computadora central.
4. Identificar cada mensaje por medio de la contraseña del usuario individual, la terminal y el número de secuencia del mensaje individual.
5. Reconocer la recepción exitosa o no de todos los mensajes.

6. Considerar si la lista de configuración de la exploración puede cambiarse durante el día para excluir o incluir terminales específicas. Esto permite la exclusión positiva de una terminal, así como el que varias terminales estén en línea y fuera de línea durante el día de trabajo.
7. Considerar el que concentradores y procesadores de entrada realicen dos niveles de revisión ("edición). En el primero, el procesador de entrada puede efectuar adiciones a un mensaje, reenrutar el mensaje o reordenar los datos para su trasmisión ulterior. También puede verificar la dirección de un mensaje para fines de exactitud y efectuar verificaciones de paridad. En el segundo nivel, el concentrador o el procesador de entrada se programan para efectuar revisiones (ediciones) específicas de las diferentes transacciones que ingresan al sistema. Esta revisión es un tipo de sistema de aplicación de "edición" que se ocupa del contenido del mensaje, en vez de su forma, y es específica de cada programa de aplicación que se ejecute.
8. Asegurarse de que los mensajes son verificados en cuanto a dirección de destino válida.
9. Asegurar que se cuenta con las capacidades de detección y control de errores adecuadas. Entre ellas pueden incluirse la verificación tipo eco, en la cual un mensaje se

transmite a un sitio remoto y éste regresa el mensaje (como un eco) para su verificación, la corrección de errores hacia delante en la que cajas especiales de hardware corrigen automáticamente algunos errores luego de la recepción, del mensaje, o la detección con retransmisión. Esta última es la forma más común y efectiva en cuanto a costo para detectar y corregir errores. Puede incluir la identificación de errores mediante la revisión del bit de paridad o el empleo de un código especial para identificar errores en caracteres individuales durante la transmisión. Una forma más común es el empleo de un polinomio (algoritmo matemático) para detectar un error en el mensaje, éste debe retransmitirse hasta que se reciba correctamente.

10. Asegurarse de que haya rutinas de software adecuadas de rearranque y recuperación a fin de eliminar problemas como entrampamiento de la verificación de una máquina, donde en lugar de bajar todo el sistema de comunicación de datos sea posible efectuar una rápida recuperación y solamente se requiera retransmitir la última transacción.

11. Asegurarse de que se cuente con procedimientos adecuados de rearranque y recuperación para efectuar tanto arranques en caliente como arranques en frío. En otras palabras, un sistema de comunicación de datos jamás debe fallar por

completo, de modo que el usuario deba efectuar un arranque en frio (empezar como si fuese un nuevo dia, con todos los contadores de mensajes en blanco). El sistema debe llegar a un procedimiento de arranque en caliente, en el que solamente estén inhabilitadas partes del sistema y la recuperación pueda efectuarse mientras el sistema esté operando en un modo degradado.

12. Asegurarse de haya una capacidad para registro del rastreo de intervención a fin de auxiliar en la reconstrucción de archivos de datos y transacciones provenientes de las diversas estaciones. Debe existir la capacidad de rastrear retrospectivamente hasta el usuario terminal.
13. Contar con algunas tablas para verificar el acceso de terminales, personas, bases de datos y programas. Tales tablas deben estar en áreas protegidas de la memoria.
14. Disponer de mantenimiento adecuado para los programas de software.
15. Identificar todas las opciones por omisión en el software y su impacto en caso de que no funcionen apropiadamente.
16. Asegurarse de que todos los datos y programas de comunicación delicados se almacenen en áreas protegidas de la memoria o en almacenamiento en disco.
17. Revisar las técnicas utilizadas para la prueba de validación de la operación del hardware y software, a fin

de asegurar su integridad. La prueba, incluyendo la del personal, debe revelar desviaciones con respecto a la operación especificada.

18. Revisar el registro de errores a fin de reducir la pérdida de mensajes. Es necesario registrar todos los errores en la transmisión de mensajes. Esta bitácora debe incluir tipo de error, hora y fecha, terminal, circuito, operador de la terminal, y número de veces que se retransmitió el mensaje antes de que fuese recibido correctamente.

19. Llevar un conteo de la suma de verificación de los bits en los paquetes de software. Esto permite una rápida verificación para saber si hay la misma cantidad de bits. Si corresponde, entonces probablemente la organización puede estar segura de que no ha habido modificaciones de software.

20. Cuando sea factible, realizar ya sea comparaciones del código fuente o comparaciones del código objeto (algunas organizaciones han efectuado comparaciones de código de fuente a objeto). Esto es para determinar si ha habido algún cambio desde que se efectuó la última comparación de fuente o de objeto. Este control consume mucho tiempo y es bastante costoso, debido a que implica la validación de un programa específico sobre una base de línea por línea. Se

compara el mismo programa, en el futuro, con la versión validada.

21. Cuando se utilice software delicado en sitios distribuidos, considerar la descarga del software desde el sitio central. Esto proporciona la seguridad de que en el sitio remoto no se hayan hecho cambios ilegales de programa. Asimismo, es posible descargar nuevos programas cada vez que un proveedor realice mantenimiento.

22. Utilizar software generalizado de auditoria para revisar funciones de los paquetes de software del sistema. Distribuir tales paquetes al personal en sitios remotos. En el sitio central, los auditores o diseñadores del sistema realizan esta función.

23. Revisar regularmente las bitácoras de los reinicios del sistema y las explicaciones del tiempo de reejecución provocado por malfuncionamiento del sistema.

24. Asegurarse de que se cuente con una bitácora de problemas con respecto al software. Debe contener el diagnóstico de cada problema y persona, componente de software o dispositivo que haya provocado el malfuncionamiento. Considerar el desarrollo de informes estadisticos a partir de tales bitácoras e iniciar acciones apropiadas en caso de que aparezca algún patrón. Es necesario aislar cada malfuncionamiento.

25. Asegurarse de que todas las características de seguridad integradas en cualquiera de los paquetes de software del sistema hayan sido tomadas en consideración. Si hay alguna que no se utilice, entonces determinar la o las razones de ello.

26. Determinar si existen interfases bien programadas y bien definidas entre cualesquiera paquetes de software del sistema, como entre sistemas operativos, software de comunicación de datos, software de inteligencia distribuido, sistemas de administración de bases de datos, etc.

27. Determinar si los programadores del sistema de software han enumerado todos los "agujeros" en cualesquiera elementos del software conocidos. Debe averiguarse el grado de exposición atribuible a cada uno de tales agujeros y efectuarse las correcciones posibles.

28. Si el sistema está ejecutando cualquier tipo de sistema de filas, como paginación o transacciones de entrada/salida de comunicación de datos, revisar las filas, el espacio de administración y otros espacios de asignación dinámica a fin de asegurar que un usuario no salga de su espacio de dirección y viole el espacio de otro usuario o el sistema operativo.

29. Forzar a que el sistema de filas falle para determinar si deja información delicada distribuida a lo largo de todo el sistema computarizado.

30. Después de una catástrofe del sistema, asegurarse de que una terminal que no entró al sistema antes de la catástrofe no pueda hacerlo luego de ella sin toda la secuencia de autentificación.

Desastres e Interrupciones

1. Asegurarse de que el sistema sea capaz de conmutar mensajes destinados de una estación/terminal caída a una estación/terminal alternativa.

2. Utilizar controles de seguridad físicos a lo largo de toda la red de comunicación de datos. Esto incluye el empleo de cerraduras, protecciones, chapas, detectores, alarmas y medidas administrativas para proteger las instalaciones físicas, redes de comunicación de datos y equipo de comunicación de datos relacionado. Tales protecciones se requieren para el monitoreo de acceso y el control a fin de proteger equipo de comunicación de datos y software contra daños por accidentes, incendios y riesgos ambientales, intencionales o no.

3. Considerar la utilización de modems que cuenten con conmutadores de prueba hacia atrás manuales o remotos para el aislamiento de fallas, a fin de asegurar la inmediata identificación de equipo que no está funcionando correctamente. Esto es de suma importancia para incrementar el tiempo de funcionamiento e identificar fallas.
4. Utilizar luces en el panel frontal de los modems para indicar si el circuito/línea está funcionando correctamente (si se está manteniendo la señal portadora). Esto puede no ser una opción viable para organizaciones que cuenta con cientos de modems.
5. Considerar un modem con funciones alternativas de voz para rápida detección de fallas entre la central y un sitio remoto importante.

6. En cuanto al equipo de comunicación de datos, verificar el tiempo medio entre fallas (TMEF) del fabricante para asegurarse de que el equipo de comunicación de datos presente el mayor TMEF.
7. Considerar la colocación de modems de respaldo no utilizados en áreas críticas de la red de comunicación de datos.

8. Considerar el empleo de modems que tengan la capacidad de respaldo automática o semiautomática en caso de que falle la línea rentada.

9. Revisar el contrato de mantenimiento y el tiempo medio de compostura (TMC) para todo el equipo de comunicación de datos. El mantenimiento debe ser rápido y estar disponible. Determinar de dónde será despachado el mantenimiento y si es posible efectuar pruebas desde un sitio remoto (por ejemplo, en muchos casos los modems cuentan con capacidades remotas de prueba de línea hacia atrás).

10. Considerar modems con ecualización automática (microprocesadores integrados para la ecualización y el balanceo del circuito) a fin de compensar las distorsiones de amplitud y fase en la línea. Esto reduce el número de errores de transmisión y posiblemente la necesidad de líneas acondicionadas.

11. Verificar que se cuente con seguridad física adecuada en sitios remotos, especialmente para terminales, concentradores, multiplexores y procesadores de comunicación de entrada.

12. Determinar si el hardware de multiplexor/concentrador/procesa-
dor de entrada remoto tiene lógica redundante y fuentes de alimentación de respaldo con capacidades de retiro

automático en caso de falla del hardware. Esto incrementa el tiempo de funcionamiento de las muchas estaciones/terminales que pueden estar conectadas a este equipo.

13. Considerar fuentes de alimentación ininterrumpibles en grandes sitios remotos de multiplexaje/concentración.
14. Considerar el uso de equipo de multiplexaje/concentración que cuente con luces para diagnóstico, capacidades de diagnóstico, etc.
15. Revisar el aislamiento/diagnóstico de fallas con que cuenta la organización, incluyendo las técnicas utilizadas para averiguar la integridad de los diversos componentes de hardware/software que constituyen toda la entidad de comunicación de datos. Tales técnicas se utilizan para auditar, revisar y controlar todo el medio de comunicación de datos y para aislar los elementos perturbadores en una base periódica o según la detección de fallas.
16. Asegurarse de que haya un medio para el registro del retiro de intervención a fin de auxiliar en la reconstrucción de archivos de datos y transacciones provenientes de las diversas estaciones. Debe existir la capacidad de rastrear retrospectivamente hasta el usuario de la terminal.
17. Almacenar en forma segura todos los mensajes. Todas las transacciones/mensajes deben protegerse en caso de alguna

situación de desastre, como la interrupción de la energía eléctrica.

18. Asegurarse de que se cuenta con medios o capacidades (o ambos) de recuperación adecuados para falla de un sistema, pérdida de piezas clave del hardware y pérdida de diversos circuitos/líneas de comunicación.

19. Asegurarse de que haya medios de respaldo (local y remoto) adecuados para piezas clave de hardware y circuitos/líneas de comunicación.

20. Cerrar con llave los recintos en que haya equipo telefónico, e instalar alarmas en las puertas de los recintos de equipo telefónico que contengan circuitos de comunicación de datos.

21. No colocar líneas de comunicación a través de los conmutadores públicos, a menos de que se trate de un nuevo tablero electrónico (EES) y se intente la identificación verbal de las llamadas de comunicación de datos por marcación recibidas.

22. Proteger todos los circuitos eléctricos contra vandalismo, en el que alguna persona pueda abrir los circuitos y cortar la corriente. Esto significa contar con cajas de control de circuitos bajo llave y colocar tales cajas en recintos baja llave.

23. Revisar el mantenimiento preventivo y las pruebas diagnósticas programadas, como limpieza, reposición y revisión de equipo a fin de evaluar su exactitud, confiabilidad e integridad. Esto puede incluir calendarizaciones para efectuar pruebas y reparaciones, probar adecuadamente cambios en los programas de software presentados por el proveedor, inventario de piezas de repuesto (tableros de circuitos), registros de mantenimiento efectuados en el pasado, etc.

Modems

1. Considerar la utilización de modems que cuenten con conmutadores de prueba hacia atrás de activación manual o remota para el aislamiento de fallas, a fin de asegurar la identificación inmediata del equipo que no esté funcionando correctamente. Esto es de extrema importancia para incrementar el tiempo de funcionamiento e identificar fallas.
2. Utilizar luces en el panel frontal de los modems para indicar si el circuito/línea está funcionando apropiadamente (si la señal portadora) se está manteniendo. Esto puede no ser una alternativa viable para organizaciones que tienen cientos de modems.

3. Considerar un modem con capacidades de voz alternativa, para detección rápida de fallas entre el sitio central y un sitio remoto importante.
4. Cuando sea factible, utilizar transmisión digital de datos, porque presenta menor frecuencia de errores que la transmisión analógica de datos.
5. Considerar la colocación de modems de apoyo no utilizados en áreas críticas de la red de comunicación de datos.
6. Considerar el empleo de modems que tengan capacidad de marcación automática o semiautomática en caso de que falle la línea rentada.
7. Incrementar la eficiencia de transmisión de datos. Mientras más breve sea el tiempo de sincronización del modem, menor será el tiempo de cambio y de este modo el sistema tendrá mayor rendimiento.
8. Considerar modems con ecualización automática (microprocesadores integrados para ecualización y balanceo de circuitos) a fin de compensar distorsiones de amplitud y de fase en la línea. Esto reduce el número de errores de transmisión y posiblemente la necesidad de líneas acondicionadas.
9. Con respecto a la eficiencia de los modems, ver que éstos cuenten con conmutadores de varias velocidades, de modo que

la velocidad de transmisión pueda reducirse cuando las frecuencias de errores en la línea sean altas.

10. Utilizar circuitos de cuatro hilos en modo de transmisión pseudo duplex completo. En otras palabras, mantener la onda portadora en cada sentido sobre pares alternativos de alambres, a fin de reducir el tiempo de cambio y ganar eficiencia durante la transmisión.
11. De ser necesario, utilizar la transmisión duplex completa en circuitos de dos hilos con modems especiales que dividen las frecuencias para lograr transmisión duplex completa.
12. Incrementar la velocidad de transmisión. Mientras mayor sea la velocidad de transmisión del modems, más efectivas en cuanto a costos serán las comunicaciones de datos. Dado que las frecuencias de errores pueden aumentar con la velocidad, podrían ser necesarios más medios para detectar y corregir errores.
13. Utilizar una capacidad de inversión de canal para las señales de control (de supervisión) y para mantener la onda portadora en ambos sentidos.
14. Considerar los siguientes controles especiales sobre los modems de marcación cuando la red de comunicación de datos permita conexiones de marcación de entrada: cambiar los números telefónicos a intervalos regulares; mantener confidenciales los números telefónicos; retirar los números

telefónicos de los modems que se hallan en el área de operaciones de la computadora; no permitir la recepción y conexión automática de llamadas (hacer siempre que una persona intercepte la llamada y efectúe una identificación verbal); hacer que el sitio central llame a las diversas terminales a las que se permite conectarse con el sistema.

15. Asegurarse de que los procesadores de entrada, concentradores, modems, etc. puedan manejar contestación automática y marcación de llamadas automáticas. Esto incrementa la eficiencia y exactitud cuando se tiene preprogramado un sistema.

8. ELABORACIÓN DEL INFORME FINAL

8.1 ELABORACIÓN DE UN BORRADOR

El informe de la Auditoria de Sistemas Informáticos es el informe que hace oficial los criterios del auditor sobre el estado del Sistema Informático. Constituye el vinculo entre el Auditor de Sistemas y el sistema auditado, además de ser la evidencia del trabajo realizado.

Sin restar su importancia, la elaboración del informe no está regida por una norma determinada por una metodología en particular, es por ello que muchos informes son infértiles, quedando archivados y en el olvido. La falta de habilidad para vender ideas es una de las causas por las que más se eleva el índice de recomendaciones no tomadas en cuenta. La realización incorrecta del informe puede traer como consecuencia disminución de la credibilidad profesional del auditor de sistemas informáticos.

La elaboración del informe acerca de la Auditoría de Sistemas Informáticos debe perseguir los siguientes objetivos:

- Facilitar la comprensión de las situaciones encontradas mediante una relación ordenada de hechos.
- Motivar la implantación de las soluciones para conseguir los beneficios esperados.

- Informar cuales son las bases sobre las que se formulan recomendaciones a utilizar en la solución de problemas similares o futuros.
- Servir de guía para llevar a la práctica las soluciones y alternativas propuestas.

Evidentemente, existirán más objetivos de acuerdo con las necesidades y circunstancias; pero básicamente los planteados ayudarán a dirigir de mejor manera la presentación de un informe.

8.2 TÉCNICAS PARA LA ELABORACIÓN DE INFORMES

Existe una infinidad de recomendaciones y técnicas de presentación de un informe, sin embargo en un sentido general, algunas recomendaciones que el auditor de sistemas informáticos debe tomar son:

- Darle un titulo al informe en función de la naturaleza del trabajo.
- Elaborar un indice que permita a cualquier lector localizar rápidamente el material deseado.
- El estilo de redacción debe ser firme pero a la vez cortez y enfatizando los aspectos relevantes.
- Utilizar gráficas, diagramas o anexos, ilustraciones y ejemplos para evitar largas explicaciones.
- El informe debe estar completo y carente de errores.

- El contenido debe ser suficiente y necesario.
- Su redacción debe hacer referencia a la situación actual y a las acciones a tomar.
- Debe destacar los beneficios presentes y futuros que se obtendrían con la implantación de las recomendaciones.

Las sugerencias citadas anteriormente podrán ser depuradas según el criterio y experiencia de auditor que haga uso de ellas.

8.3 PRESENTACIÓN DE COMENTARIOS

La forma y temática de presentar un comentario depende del criterio del auditor, sin embrago tomando como base el tiempo de los ejecutivos, se debe buscar la forma de interesarlos en la esencia del problema, o en su caso la recomendación.

Un comentario es la observación a un hecho, a una actuación, etc, y el auditor debe ser imparcial y objetivo al redactarlos. La redacción de comentarios debe presentar una relación de hechos concretos que permitan apreciar lo que sucede, lo que debería suceder, el efecto, las desviaciones o consecuencias que puedan producirse y las razones por las que existen esas desviaciones; un comentario debe redactarse de tal manera que sea comprensible.

Al respecto puede utilizarse la siguiente técnica que reúne aspectos importantes en la redacción comprensible de los

comentarios, se tarta de la forma **SEPS**, cuyas siglas tienen el siguiente significado:

Sistema : La forma actual de realizar las operaciones en el sistema auditado.

Error : La deficiencia detectada, el hallazgo, el problema o las fallas del sistema.

Prueba : El respaldo a la desviación, el efecto que causa esa desviación, porcentajes, calificación del problema, la proporción del problema, las repercusiones que pueden traer consigo las causas.

Sugerencia: Las alternativas para evitar, enmendar, etc. la desviación; la recomendación para mejorar el sistema.

Uno de los puntos cruciales para que la presentación de los resultados sea un éxito, y que por ende quede evidencia de la calidad profesional de los trabajos, es la forma como redacte el informe. Esto deja al descubierto que en la práctica profesional de Auditoría de Sistemas Informáticos necesita una formación que le permita establecer una comunicación adecuada con los ejecutivos, a fin de que cada trabajo y cada comentario sea atendido en la forma en que se trató de expresar.

8.4 PRESENTACIÓN DE RECOMENDACIONES

La elaboración del resumen de recomendaciones es el punto crucial de la elaboración del informe. Es en esta parte del trabajo donde se pone en juego toda la capacidad del auditor, ya que está vendiendo ideas que llevadas a la práctica, permitirán obtener mejores resultados a los empresarios. Por tanto las recomendaciones a presentar deben contener los datos necesarios que no sólo vuelvan interesante al informe, sino también aplicable.

En la elaboración de las recomendaciones deben tomarse en cuenta los siguientes puntos:

- Evaluar el antiguo y nuevo sistema bajo las mismas circunstancias y definir sus beneficios.
- Evaluar los beneficios o ventajas del cambio, cuantificándolos o cualificándolos según la necesidad.
- Identificar los aspectos trascendentes de los intrascendentes.
- Elaborar conclusiones que obedezcan a consideraciones básicas sustentadas en hechos reales.
- Mantener imparcialidad y objetividad, evitando dañar la integridad de las personas que se ven involucradas en la implantación de las recomendaciones.

- Evaluar el costo frente al beneficio que se obtendrá al implantar las recomendaciones.
- Cubrir todos los aspectos del cambio propuesto.
- Motivar una actitud positiva y constructiva del personal frente al cambio a realizar, esto es:
  - Adaptar el cambio al personal disponible.
  - Adatar al personal las necesidades del cambio.
  - Preparar un plan de entrenamiento de ser necesario.

El apego a los puntos anteriores da como resultado un informe de calidad profesional: dirigido a quien lo va a leer, eliminando términos demasiado técnicos, cuadros muy complicados y recomendaciones generales.

8.5 OPORTUNIDAD EN LA ELABORACIÓN

En una administración dinámica, la oportunidad y la confiabilidad de la información es muy importante, por lo que la Auditoría de Sistemas Informáticos se convierte en un apoyo importante para la gerencia moderna, y para llenar esa necesidad el auditor debe elaborar sus informes a la mayor brevedad posible, a fin de que las decisiones a tomar por parte de los ejecutivos sean oportunas.

La comunicación de resultados debe realizarse lo más pronto posible, luego de finalizada la auditoria, con el fin de que las acciones correctivas sean iniciadas sin demora. En algunas ocasiones es tan urgente hacer las correcciones que el informe de los resultados debe irse ejecutando paralelamente a la ejecución del trabajo.

8.6 DISCUSIÓN DEL BORRADOR DEL INFORME

Una vez escrito y revisado el borrador del informe se procede a convocar a una reunión para comentar su contenido. El objetivo de esta reunión es el de dar la oportunidad al auditor de aclarar, definir o modificar sus apreciaciones evitando presentar sugerencias irreales. Esto es debido a que el personal de la empresa conoce bien sus aciertos y desaciertos en los sistemas. En esta reunión se persigue que quede perfectamente entendido lo que en el informe está plasmado.

8.7 EL INFORME FINAL

Una vez pasada la etapa de discusión se procede a depurar el informe, esto es suprimir lo intrascendente, aclarar los comentarios, modificar la redacción y lo más importante: incluir los comentarios de los participantes.

Luego de producir el informe y los ejemplares necesarios, el jefe de la unidad firma el original y las copias para luego ser distribuidas entre los diferentes funcionarios involucrados.

El formato y contenido del informe, varía de acuerdo al criterio del auditor que lo escribe, sin embargo, un informe de auditoría debe reunir ciertos requisitos o elementos básicos:

- Carta de envio
- Carta de presentación
- Indice
- Introducción
- Cuerpo del informe
- Plan de trabajo
- Anexos (en caso de ser necesarios)

Por último debe verificarse de alguna manera si se están tomando en cuenta las sugerencias o recomendaciones emitidas, y de acuerdo a lo observado en el seguimiento, desviará la atención u orientación de los trabajos futuros, siendo además factible un ajuste del plan actual. Esta actividad debe constar en el plan de la auditoría, así como producir informes de lo realizado.

CUARTA PARTE

EVALUACION

9.0 EVALUACIÓN ECONÓMICA

Es de sumo interés para las entidades que poseen sistemas informáticos, conocer las ganancias que recibirán a raíz de su inversión en la ejecución de la Auditoría a los Sistemas Informáticos que poseen. Actualmente los sistemas de información se encuentran dando soporte en lo referente a mercadeo (pronósticos de ventas, planeación de ventas, análisis de clientes y ventas), manufactura (planeación de la producción y horarios, análisis de control de costos), logística (planeación y control de compras, distribución, inventarios), finanzas y contabilidad (análisis financiero, análisis de costos, planeación de los requerimientos de capital, medición del ingreso), personal (planeamiento de los requerimientos de personal, análisis del desempeño, administración de salarios), procesamiento de información (planeación del sistema de información, análisis de la efectividad), alta gerencia (planeación estratégica, asignación de recursos). Estas aplicaciones se realizan de acuerdo a la naturaleza de las actividades en el procesamiento de transacciones, el control operacional,el control administrativo y la planeación estratégica.

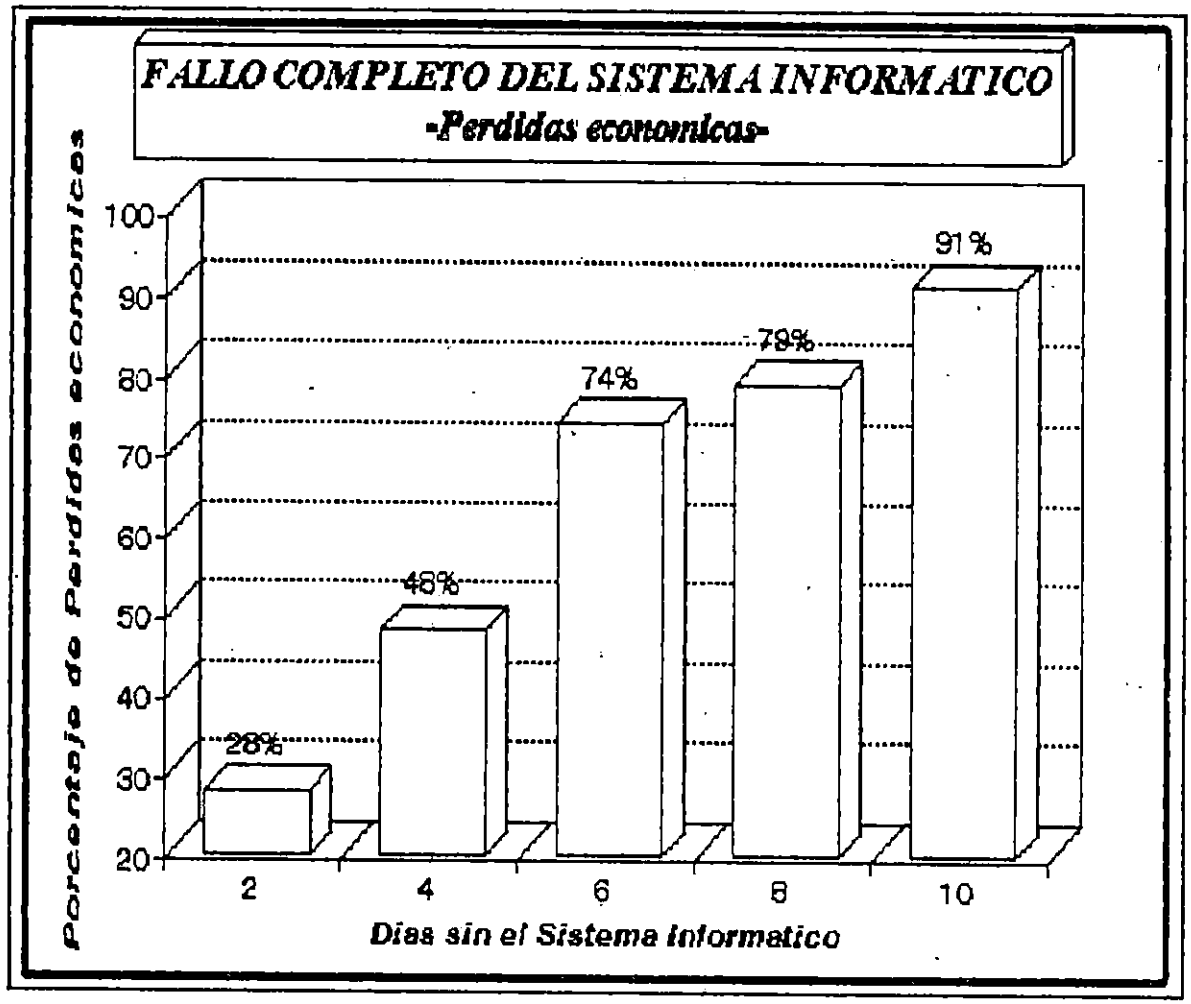
Un fallo completo en el sistema informático ocasionará indiscutiblemente una enorme pérdida económica.

Tomando en consideración únicamente empresas que en un 40% mas y menos 15% dependen de sistemas que han sido mecanizados, se han establecido las cuantías de dinero que a causa del fallo completo de los sistemas informáticos, ellas pierden en razón del tiempo que permanezcan sin el soporte de los sistemas mecanizados.

En términos de porcentajes, a los dos días de operar sin el computador, los ingresos se ven afectados en una reducción del 28%, a los cuatro días, se afectan los ingresos en un 48%, a los diez días más del 90%.

Considere que hay empresas como los bancos que dependen en mayor grado de los sistemas informáticos, para estas, al segundo día de operación sin los sistemas mecanizados, el 75% de los ingresos dejan de ser percibidos.

El porcentaje de pérdidas por fallo completo del sistema informático se puede ver en el gráfico de la siguiente página.



Fuente: Aasagaard-Cheung-Hubbert y M.C. Simpson "Una evaluación del procesamiento de datos 'cuarto de máquina' pérdidas y estrategias seleccionadas para su recuperación. Universidad de Minessota. Centro de investigación de sistemas de información. Página 70

La tabla siguiente, muestra la cuantía de dinero que pierde una empresa determinada (de acuerdo a sus ingresos), por el fallo completo del sistema informático (según el número de días).

INGRESOS(MES) (¢)	PERDIDA (¢) 2 DÍAS	PERDIDA (¢) 4 DÍAS	PERDIDA (¢) 6 DÍAS	PERDIDA (¢) 8 DÍAS	PERDIDA (¢) 10 DÍAS
50000	12500	24000	37000	39500	45500
100000	25000	48000	74000	79000	91000
225000	56250	108000	166500	177750	204750
300000	75000	144000	222000	237000	273000
450000	112500	216000	333000	355500	409500
540000	135000	259200	399600	426600	491400
630000	157500	302400	466200	497700	573300
910000	227500	436800	673400	718900	828100
1010000	252500	484800	747400	797900	919100
2060000	515000	988800	1524400	1627400	1874600
3960000	990000	1900800	2930400	3128400	3603600
6810000	1702500	3268800	5039400	5379900	6197100
7760000	1940000	3724800	5742400	6130400	7061600
10610000	2652500	5092800	7851400	8381900	9655100

Vistas las pérdidas en dinero por fallo del sistema informático como un AHORRO o beneficio por haber invertido en la Auditoría de sistemas informático, se establece que para

determinar el beneficio económico de la realización de la auditoría, deberá utilizarse la siguiente fórmula:

BENEFICIO = AHORRO PRODUCIDO - COSTO DE IMPLANTACIÓN DE LA AUDITORIA

El AHORRO PRODUCIDO puede ser calculado en base a interpolación de los datos en la tabla anterior, el número de días sin el sistema informático que se debe considerar, dependerán específicamente de las consultas realizadas al personal técnico del departamento de sistemas de la empresa: puede realizarseles la pregunta: En caso de un siniestro grave, si se echara a perder todo el sistema, en cuanto tiempo garantizarían que se volviera a restituir el sistema informático, exactamente como estaba antes de la catástrofe ?. (todo considerado, es decir compra del equipo, instalación del software, etc).

Es necesario conocer una cuantía de beneficios para una empresa pequeña, mediana o grande. Con base en el costo de implantación de el departamento de auditoría de sistemas en cada uno de estos tamaños de empresas. Por lo anterior se ha realizado la siguiente tabla de beneficios (cuatro días únicamente sin el computador).

La tabla a continuación muestra los beneficios económicos para los tres tipos de empresa (ubiquese de acuerdo a los ingresos mensuales)

EMPRESA	PEQUEÑA	EMPRESA	MEDIANA	EMPRESA	GRANDE
INGRESOS(¢)	BENEFICIOS(¢)	INGRESOS(¢)	BENEFICIOS(¢)	INGRESOS(¢)	BENEFICIOS(¢)
50000	6785	200000	61569	500000	188354
55000	9185	210000	66369	750000	308354
60000	11585	220000	71169	1000000	428354
65000	13985	230000	75969	1250000	548354
70000	16385	240000	80769	1500000	668354
75000	18785	250000	85569	1750000	788354
80000	21185	260000	90369	2000000	908354
85000	23585	270000	95169	2250000	1028354
90000	25985	280000	99969	2500000	1148354
95000	28385	290000	104769	2750000	1268354
100000	30785	300000	109569	3000000	1388354
105000	33185	310000	114369	3250000	1508354
110000	35585	320000	119169	3500000	1628354
115000	37985	330000	123969	3750000	1748354
120000	40385	340000	128769	4000000	1868354
125000	42785	350000	133569	4250000	1988354
130000	45185	360000	138369	4500000	2108354
135000	47585	370000	143169	4750000	2228354
140000	49985	380000	147969	5000000	2348354
145000	52385	390000	152769	5250000	2468354

Obtenido del plan de implantación y los costosa asociados. Se aplica la fórmula:

BENEFICIOS = AHORRO - COSTO DE IMPLANTACIÓN

(4 días sin el sistema informático)

10. PLAN DE IMPLANTACIÓN

INTRODUCCIÓN

Un plan de implantación se establece con el objeto de preparar todas aquellos aspectos que se necesitan para hacer uso efectivo de la metodología, es decir, predeterminar el momento y los requisitos mínimos para la instalación de la metodología, para que ésta funcione eficientemente.

El plan se constituye con los objetivos, estrategias, funciones, actividades y programación del mismo. Las acciones concretas de ejecución de la implantación serán consumadas por el responsable encargado del proyecto. Este documento contiene la figura del organigrama para la implantación; además de la descripción de cada unidad.

El plan se consolida con la gestión de control de actividades, supervisión y análisis de las desviaciones, experimentadas a través del desenvolvimiento de la implantación.

OBJETIVOS

OBJETIVO GENERAL

Planear, programar y controlar todas aquellas actividades para implantar la metodología de sistemas informáticos.

OBJETIVOS ESPECÍFICOS

- Determinar actividades a desarrollar.
- Establecer el escenario en el tiempo y representarlo en un cronograma que aclare los momentos en que una actividad determinada debe ejecutarse.
- Instituir la estructura organizativa para el desarrollo de la implantación.
- Determinar los mecanismos necesarios para la gestión de control de dicha implantación.

ESTRATEGIAS DE IMPLEMENTACIÓN

a) Establecer el equipo de implantación en el menor tiempo posible.

b) Estudiar todas las actividades a desarrollar.

c) Ejecutar todas las actividades observando el tiempo predeterminado para su desarrollo y anotando su valor en la hoja de control de actividades. El desarrollo de estas actividades debe respetarse el orden cronológico establecido por el diagrama.

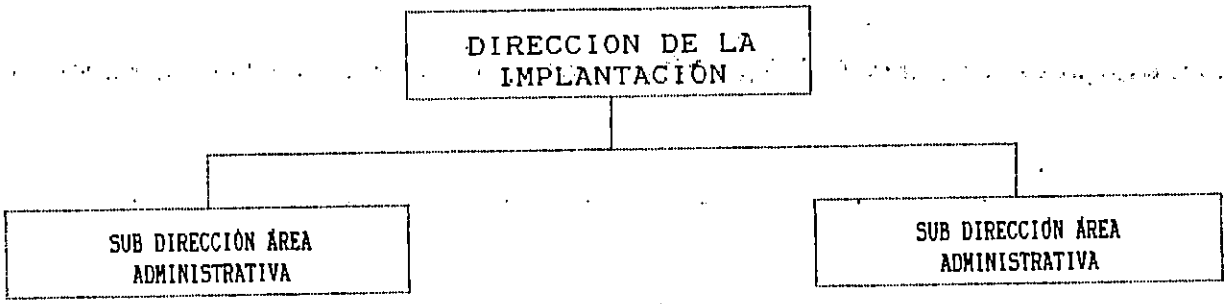
d) Actualizar los valores de los elementos considerados en el costo de la implantación con el valor actual en el mercado.

ORGANIZACIÓN PARA LA IMPLANTACIÓN

Para que todas las actividades se realicen de una manera coordinada y eficaz, es saludable determinar el responsable y sus funciones. La implantación de la metodología necesita de definir las actividades en el área administrativa y técnica por lo tanto

el primer paso será establecer la estructura organizativa que queda constituida de la manera siguiente:

ORGANIGRAMA DE LA IMPLANTACIÓN



Este equipo es de carácter transitorio y es responsable de guiar el proceso de instauración de la metodología por todas sus áreas.

Descripción de funciones.-

a) Dirección de la implantación, esta unidad es la responsable de todo el proceso de instalar la metodología, además de supervisar la trayectoria de las etapas, debe proporcionar apoyo técnico en la fase posterior a la implantación, es decir, en el preciso momento en que la metodología es puesta en marcha.

b) Sub-dirección del área técnica, está relacionado con todas aquellas actividades de índole técnico que necesita la metodología en su implantación. El trabajo en esta sub-dirección se desarrolla en 2 aspectos de mucha importancia tales como soporte técnico al momento de la implantación y asistencia técnica posterior cuando la instalación ha sido concluida.

COSTO DE LA IMPLANTACIÓN

El objeto de este rubro es mostrar todos aquellos elementos que se utilizará en la implantación y estimar en términos económicos el valor de ellos.

ESPECIFICACIONES DE LAS FUNCIONES DE IMPLANTACION POR UNIDAD

IDENTIFICACION DE LA UNIDAD :

Direccion de implantacion.

OBJETIVO DE LA UNIDAD :

Planificar, programar, coodinar, controlar y dirigir todas las actividades requeridas para la implantacion.

FUNCIONES CONCRETAS :

* Establecer las actividades a desarrollar.
* Programar dichas actividades.
* Coordinar a las unidades subordinadas en la implantacion.
* Controlar el trabajo en ejecucion.
* Dirigir el equipo en paralelo en relacion al progreso de la implantacion.

ESPECIFICACIONES DE LAS FUNCIONES DE IMPLANTACION POR UNIDAD

IDENTIFICACION DE LA UNIDAD :

Sub-Direccion del area administrativa.

OBJETIVO DE LA UNIDAD :

Planificar, programar, coodinar, controlar y ejecutar todas las actividades requeridas en el entorno administrativo para la implantacion.

FUNCIONES CONCRETAS :

* Planificar las actividades y recursos administrativos necesarios para la la implantacion.
* Programar las actividades.
* Coordinar los esfuerzos de los recursos materiales y los humanos.
* Controlar el trabajo en proceso.
* Adiestrar el personal administrativo.

ESPECIFICACIONES DE LAS FUNCIONES DE IMPLANTACION POR UNIDAD

IDENTIFICACION DE LA UNIDAD :

Sub-Direccion del area tecnica.

OBJETIVO DE LA UNIDAD :

Planificar, programar, coodinar, controlar y ejecutar todas las actividades tecnicas requeridas en la implantacion de la metodologia.

FUNCIONES CONCRETAS :

* Planificar las actividades y recursos tecnicos necesarios para la implantacion.
* Programar las actividades.
* Capacitar al personal en aspectos tecnicos de la metodologia.
* Coordinar los esfuerzos de los recursos materiales y los humanos.
* Controlar el trabajo en proceso.
* Garantizar el buen funcionamiento de la metodologia brindando soporte tecnico posterior a la instalacion.

COSTO ESTIMADO DE LA IMPLANTACION

ELEMENTOS	VAL(Col.)
MATERIALES DIRECTOS	
Texto de la metodologia	276.75
Diskettes con sistema	184.50
MANO DE OBRA DIRECTA	
Director de la implantacion	58579.61
Sub-director administrativo	14760.22
Sub-director tecnico	14760.22
COSTOS INDIRECTOS	
Supervision	2767.54
Papeleria y suministros de oficina	1815.51
Energia electrica	922.51
Depreciacion de equipo	9225.14
TOTAL	103292.00

ACTIVIDADES PARA LA IMPLANTACIÖN

Este apartado contiene las actividades a desempeñar en la implantación de la metodología; todas ellas están agrupadas en un cuadro que contiene el tiempo estimado en días que consume la actividad (por efectos de la programación); esta tabla muestra el costo de por cada actividad; este dato es calculado en base al costo total de toda la implantación dividido por el número de días que dicho trabajo requiere.

Para manejar mas fácilmente el problema de la programación se ha recurrido al uso del paquete QBS y los resultados se muestran después del listado de las actividades, para que al final se presente el diagrama PERT de la implantación.

ACTIVIDADES DE IMPLANTACION

DDI : Director de implantacion

SDAA : Sub-director del area administrativa

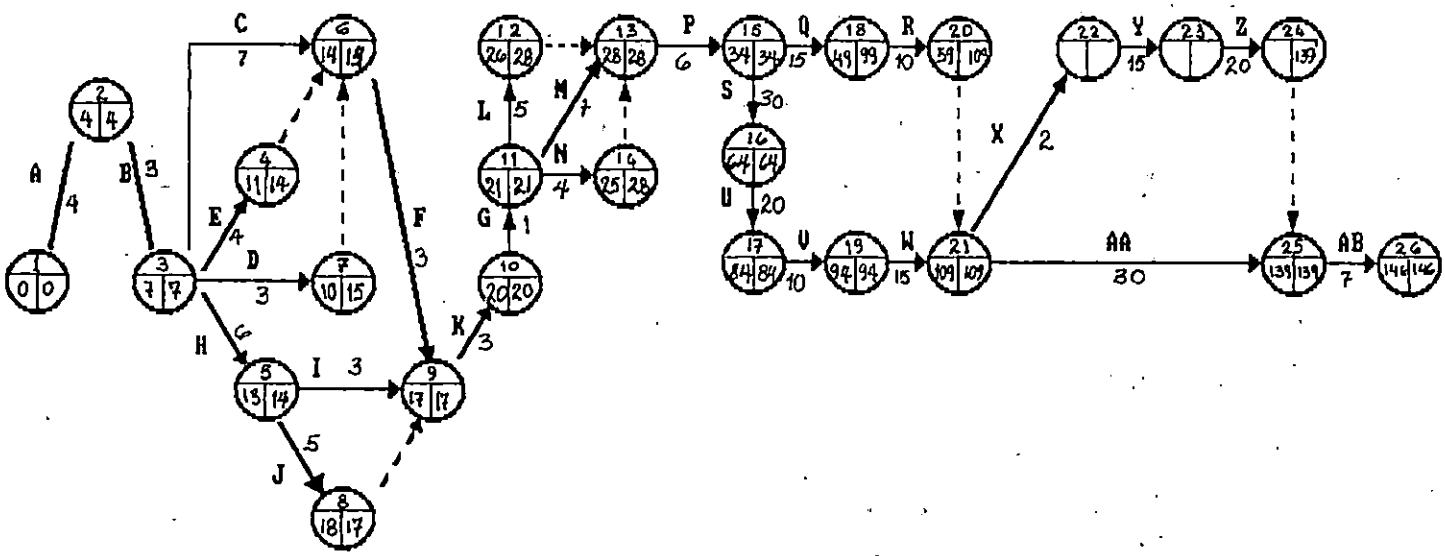
SDAT : Sub-director del area tecnica.

L.	Actividad	T	Resp.	Cost
A	Propuesta y autorizacion de la implantacion de la met.	4	DDI	1736
B	Formacion de la comision de implantacion	3	DDI	1302
C	Estudio de las actividades generales a desarrollar	7	DDI	3038
D	Estudio de las actividades administrativas a desarrollar	3	SDDA	1302
E	Estudio de las actividades tecnicas a desarrollar	4	SDAT	1736
F	Revision de los objetivos de impl.	3	COM	1302
G	Evaluacion de actividades ejecutadas.	1	DDI	434
H	Establecimiento de estrategias generales	6	DDI	2604
I	Establecimiento de estrategias de caracter administrativa	3	SDAA	1302
J	Establecimiento de estrategias de caracter tecnico	5	SDAT	2170
K	Revision y acuerdo de actividades de implantacion	3	DDI	1302
L	Planificacion de los recursos humanos.	5	DDI	2170
M	Planificacion del equipo y materiales	7	DDI	3038
N	Calculo estimado del presupuesto	4	DDI	1736

CONTINUACION

L.	Actividad	Perf	Resp.	Cost
P	Evaluacion general del ambiente	6	DDI	2604
Q	Adquisicion de recursos	15	DDI	6510
R	Instalacion de equipo(si requiere)	10	DDI	4340
S	Seleccion y contratacion del personal	30	SDAA	13020
U	Adiestramiento del personal	20	SDAA	8680
V	Estudio de la metodologia	10	SDAA	4340
W	Instalacion y prueba del software	15	SDAT	6510
X	Asignacion de puestos	2	DDI	868
Y	Prueba coordinada de todos los elementos en conjunto	15	DDI	6510
Z	Supervision y control del comienzo de la metodologia	20	SDAT	8680
AA	Soporte y asistencia tecnica a la metodologia en marcha	30	SDAT	13020
AB	Elaboracion del imforme de el desarrollo de la implantaci	7	DDI	3038

DIAGRAMA CPM PARA LA IMPLANTACION



RUTA CRITICA : A - B - C - F - K - G - L
P - S - U - V - W - AA - AB

REQUERIMIENTOS GENERALES

a) Requerimientos de Hardware.

Estos requerimientos se han considerado por el motivo de que en muchos centros de procesamiento de datos, carecen del equipo mínimo necesario para que el sistema mecanizado de la metodología funcione.

Las especificaciones técnicas que se presentarán a continuación han sido posible en base a los siguientes características :

1. Cantidad de memoria en disco consumida por el sistema mecanizado de la metodología.
2. Cantidad de memoria en disco para almacenar el manejador de base de datos. Para el caso FOXPROLAN.
3. Capacidad de memoria RAM.
4. Velocidad promedio del computador.
5. Tipo de microprocesador.
6. Accesorios y periféricos.

Las especificaciones técnicas de la máquina son:

CANTIDAD DE MEMORIA DE FOXPROLN: 2,933530 Bytes

CANTIDAD DE MEMORIA DE METODOLOGÍA: 997 KBytes

TARJETA MOTHER BOARD : 386SX-33MHZ

DISCO DURO : 80MB

DISK DRIVE : 5 1/4 1.2MB

DISK DRIVE : 3 1/2 1.44KB

MEMORIA RAM : 2MB

IMPRESOR : solo que sea compatible.

b) Requerimientos de software.

SISTEMAS OPERATIVOS : MS-DOS Versiones desde 3.0, 5.0, 6.0 y mayores.

SISTEMAS MANEJADOS DE BASE DE DATOS: Tales como foxproln, foxbase+ multiusuario 2.10

UTILITARIOS: No necesarios pero deseables, Word perfect, norton comander, cpav 2.1 y scan 108.

GESTIÓN DE CONTROL DE LA IMPLANTACIÓN.

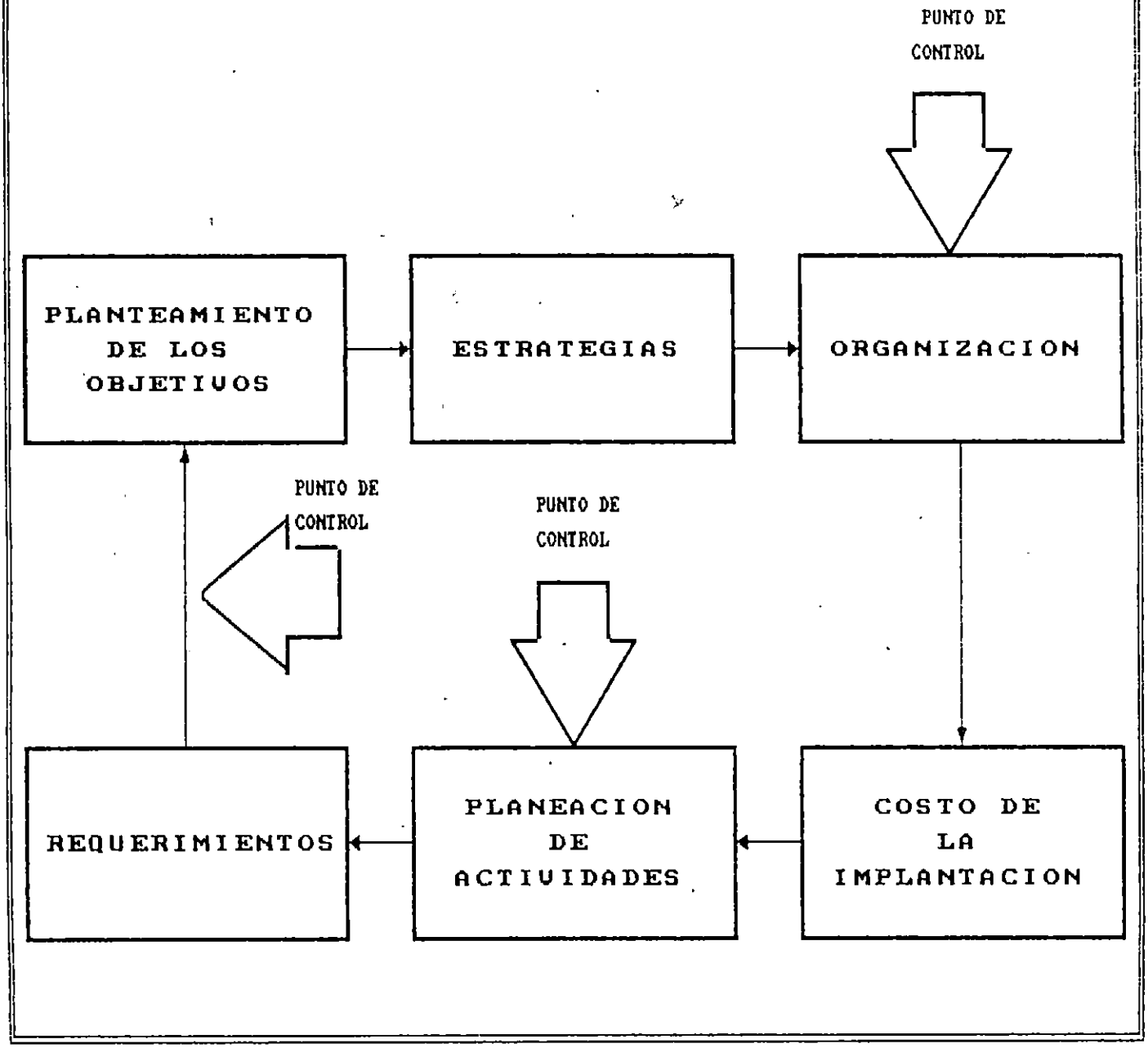
La importancia del control de cada actividad es relativa a la perfección de la planificación de la implantación, ya que en ella se pueden descubrir problemas o deficiencias de la misma, además de aspectos no considerados.

La gestión de control se divide en etapas, según está estructurada la implantación, y se identifican los puntos claves en donde se hará la función de control.

Etapas del control:

1. Revisión de la planeación.
2. Supervisión de actividades.
3. Recopilación de información.
4. Análisis de los cambios, deficiencias, problemas y desviaciones.

PROCESO DE LA IMPLANTACION



INSTRUMENTO PARA EL CONTROL EN EL PRIMER PUNTO

Datos preliminares:

EMPRESA OBJETO DE LA IMPLANTACION		FECHA	
		RESPONSABLE	

COMPLETE LA INFORMACION

	RESPONSABLE	FORMA	OBSERVACION
PLANEAR			
SUPERVISAR			
PROGRAMAR			

DESCRIBA LAS ACCIONES CONCRETAS

1.-
2.-
3.-
4.-
5.-
6.-
7.-
8.-
9.-

CONTROL DE LOS COSTOS

ELEMENTO	VALOR
COSTO TOTAL ESTIMADO	
COSTO TOTAL REAL	
DIFERENCIA	

RUBRO	COST.IN.	COST.FINAL	DIFERENCIA
Texto de la metodologia			
Diskettes con sistema			
Director de la implantacion			
Sub-director administrativo			
Sub-director tecnico			
Supervision			
Papeleria y suministros de oficina			
Energia electrica			
Depreciacion del equipo			

CONTROL DE ACTIVIDADES DE IMPLANTACION

FECHA:

L	Actividad	REVISA	FECHA		PERIODO		DESVIACION
			INICIO	FINAL	PLANIF	REAL	
A	Propuesta y autorizacion de la implantacion de la met.						
B	Formacion de la comision de implantacion						
C	Estudio de las actividades generales a desarrollar						
D	Estudio de las actividades administrativas a desarrollar						
E	Estudio de las actividades tecnicas a desarrollar						
F	Revision de los objetivos de impl.						
G	Evaluacion de actividades ejecutadas.						
H	Establecimiento de estrategias generales						
I	Establecimiento de estrategias de caracter administrativas						
J	Establecimiento de estrategias de caracter tecnico						
K	Revision y acuerdo de actividades de implantacion						
L	Planificacion de los recursos humanos.						
M	Planificacion del equipo y materiales						
N	Calculo estimado del presupuesto						
P	Evaluacion general del ambiente						
Q	Adquisicion de recursos						
R	Instalacion de equipo(si requiere)						
S	Seleccion y contratacion del personal						
U	Adiestramiento del personal						
V	Estudio de la metodologia						
W	Instalacion y prueba del software						
X	Asignacion de puestos						
Y	Prueba coordinada de todos los elementos en conjunto						
Z	Supervision y control del comienzo de la metodologia						
AA	Soporte y asistencia tecnica a la metodologia en marcha						
AB	Elaboracion del informe de el desarrollo de la implantacion						

INSTRUMENTOS PARA EL ANALISIS

MACRO ACTIVIDAD : PLANTEAMIENTO DE LOS OBJETIVOS

CAMBIOS DE FONDO		PROBLEMAS	
CAMBIOS DE FORMA		CAUSAS	
DEFICIENCIAS		SOLUCIONES	
DESVIACIONES		OBSERVACIONES	

MACRO ACTIVIDAD: ESTRATEGIAS

CAMBIOS DE FONDO		PROBLEMAS	
CAMBIOS DE FORMA		CAUSAS	
DEFICIENCIAS		SOLUCIONES	
DESVIACIONES		OBSERVACIONES	

MACRO ACTIVADAD: ORGANIZACION

CAMBIOS DE FONDO		PROBLEMAS	
CAMBIOS DE FORMA		CAUSAS	
DEFICIENCIAS		SOLUCIONES	
DESVIACIONES		OBSERVACIONES	

INSTRUMENTOS PARA EL ANALISIS

MACRO ACTIVIDAD : COSTO DE LA IMPLANTACION

CAMBIOS DE FONDO		PROBLEMAS	
CAMBIOS DE FORMA		CAUSAS	
DEFICIENCIAS		SOLUCIONES	
DESVIACIONES		OBSERVACIONES	

MACRO ACTIVIDAD: PLANIFICACION DE ACTIVIDADES

CAMBIOS DE FONDO		PROBLEMAS	
CAMBIOS DE FORMA		CAUSAS	
DEFICIENCIAS		SOLUCIONES	
DESVIACIONES		OBSERVACIONES	

MACRO ACTIVADAD: REQUERIMIENTOS

CAMBIOS DE FONDO		PROBLEMAS	
CAMBIOS DE FORMA		CAUSAS	
DEFICIENCIAS		SOLUCIONES	
DESVIACIONES		OBSERVACIONES	

CONCLUSIONES
RECOMENDACIONES
ANEXOS Y BIBLIOGRAFIA

CONCLUSIONES

* Los elementos que componen un sistema informático son tantos, que se optó por agruparlos por subsistemas, identificando así las relaciones entre todos esos elementos. Fue por ello que a través de la Teoría General de Sistemas se estableció que un sistema informático agrupa a todos sus elementos dentro de los siguientes subsistemas:

  1- Subsistema de acceso al sistema informático.
  2- Subsistema de entrada al sistema informático.
  3- Subsistema de proceso del sistema informático.
  4- Subsistema de salida del sistema informático.
  5- Subsistema de bases de datos del sistema informático.
  6- Subsistema de comunicaciones del sistema informático.
  7- Entorno del sistema informático.

* El entorno del sistema informático, es lo que está fuera del computador: Personas y ambiente físico. Las personas de su entorno, son quienes lo administran y por ello, se concluye que, hablar del entorno de un sistema informático es referirse a los aspectos de su administración.

* El entorno del sistema informático, es tan amplio, y se obtuvieron tantos elementos en el, que se agrupó a todos

sus elementos en subsistemas, los cuales son:

1- La administración del área de procesamiento de datos.

2- El desarrollo de sistemas informáticos.

3- La administración que se hace a los datos.

4- La administración de la seguridad del sistema informático.

5- La administración de las operaciones del sistema informático.

6- El soporte técnico al sistema informático.

* Existen ciertos enfoques acerca de la auditoría de sistemas informáticos. Un 70% de éstos, afirman que la auditoría debe hacerse únicamente en los procesos del sistema. El 20% aseguran que la auditoría debe hacerse en algunas áreas, únicamente de la administración del sistema informático. El restante 10% creen que la auditoría de sistemas informáticos se refiere a la evaluación de la contabilidad a través del computador.

* Los antecedentes sobre auditoría de sistemas informáticos carecen de validez, no solo para nuestro país, sino en general.

* Una verdadera auditoría de sistemas informáticos debe referirse no solo a evaluar el computador, sino también evaluar la administración del sistema informático.

* La conceptualización del diseño de la metodología para auditar sistemas informáticos, se basa en la evaluación de la administración del sistema informático y luego la evaluación de los procesos del computador.

* A pesar de que se trata de el diseño de una metodología, se consideró adecuado incluir junto con el diseño detallado los aspectos previos a la ejecución de la Auditoría: planeación y organización.

* Dar a conocer los resultados de la ejecución de la

Auditoría de Sistemas Informáticos, es tan importante que, de no hacerse adecuadamente podría echar a perder todo el trabajo realizado, y más aún poniendo en duda el profesionalismo del equipo de trabajo.

* Respecto a los beneficios sociales que se logran a través de la aplicación de la metodología para auditar sistemas informáticos se pueden ver desde dos perspectivas: atendiendo al período de tiempo en el que serán tangibles o a las personas o instituciones que se beneficiará.

* Un beneficio social a corto plazo es la creación de un nuevo puesto de trabajo que cuenta con una metodología completa de el desempeño de sus funciones. Este puesto de trabajo de auditor de sistemas, absorverá a muchos de los profesionales de las carreras de ingeniería industrial con especialización en sistemas de información, a ingenieros en sistemas informáticos y a licenciados en ciencias de la computación, administradores de empresas y licenciados en contaduría pública. El refinamiento de la carrera de Ingeniería de sistemas informáticos proporcionándole una opción de especialización. Abriendo nuevos expectativas en el cambio curricular de las carreras de licenciatura en

contaduría pública, Licenciados en administración de empresas y otras.

* En beneficio social, a mediano plazo habrán mejoras en los ingresos de los auditores de sistemas. Los niveles de ingresos económicos de los auditores de sistemas serán mucho más atractivos a causa de mejoras en los niveles de ingreso económico de las empresas en las que ellos laboran. Un áudito permanente, garantiza una información confiable y oportuna. La efectividad y eficiencia de los negocios aumenta notablemente al trabajar con sistemas que operan sin desviarse de los objetivos para los cuales fueron creados.Incremento de la informática en las actividades cotidianas de las empresas, a raíz de la confianza de los resultados de los sistemas. La confidencialidad, integridad de los datos, eficiencia y efectividad de los procesos mecanizados, habrán demostrado que muchos más negocios se pueden realizar en un mismo período, cuando se tiene soporte de sistemas mecanizados. En resumen habrá mayor confianza en los resultados de los sistemas mecanizados y por ende mayor difusión de los mismos.
* A largo plazo, con respecto a los beneficios sociales, mejoras en la competitividad de las empresas, con información real y oportuna, sistemas de información

gerencial que dan soporte en niveles táctico, operativo y estratégico. Mejoras en la eficiencia de las instituciones públicas (hospitales, ministerios, etc) y del sector privado. La nación entera se ha de volver competitiva logrando aprovechar un mayor número de oportunidades, aumentando con ello el número de empresas, salarios y por ende el nivel de vida de los habitantes de la nación.

RECOMENDACIONES

* El diseño de la metodología para auditar sistemas informáticos se debe enmarcar en un enfoque sistémico, como el de la teoría general de sistemas, ya que son muchas las variables de evaluación en una auditoría de esta naturaleza.

* Debe tomarse en cuenta que la metodología para auditar sistemas informáticos será vista por el consumidor final como una caja negra, en la que solo le interesan los resultados, por ello, debe presentarse especial interés en la fase de la metodología que se refiere a la presentación de resultados.

* El trabajo de la ejecución de la metodología presentada en este documento, debe ser realizada por un equipo multidisciplinario y no por una sola persona.

* Antes de realizar la auditoría, no sólo se debe conocer a profundidad el sistema informático a auditarse, sino que

antes, debe conocerse concienzudamente el contenido de la metodología para Auditar Sistemas Informáticos que se presenta en este informe.

* Por aspectos de objetividad, los miembros del equipo de auditoria deben ser lo suficientemente independientes del sistema sujeto al áudito.

ANEXOS

Los anexos se han clasificado por letras del alfabeto y su orden de presentación es la siguiente:

ANEXO A Declaración sobre las normas de auditoría de sistemas de información.

ANEXO B Instrumento para la auditoría a la Administración del área de procesamiento de Datos.

ANEXO B1 Instrumento para evaluar al Comité Coordinador de Actividades.

ANEXO B2 Instrumento para evaluación de la organización de PED.

ANEXO C Instrumento para la auditoría al subsistema de Desarrollo de Sistemas.

ANEXO C1 Instrumento para evaluación del compromiso progresivo para el desarrollo de sistemas.

ANEXO C2 Instrumento para evaluación a las actividades del desarrollo de sistemas.

ANEXO C3 Instrumento para evaluación de la planeación de sistemas.

ANEXO C4 Instrumento para la evaluación de las especificaciones del usuario.

ANEXO C5 Instrumento para la evaluación de las

ANEXO A

DECLARACIÓN SOBRE LAS NORMAS DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

PREFACIO A LAS NORMAS GENERALES PARA LA AUDITORÍAS DE SISTEMAS DE INFORMACIÓN Y DECLARACIONES SOBRE LAS NORMAS DE AUDITORIA DE SISTEMAS DE INFORMACIÓN

PUBLICADO POR THE EDP AUDITORS FOUNDATION

La Asociación de Auditores EDP y la fundación de Auditores EDP

El concepto de una asociación profesional de auditores de computadores se originó los Angeles California, USA, a finales de la década de los 60 con un pequeño grupo de auditores que se encontraban trabajando en el área de sistemas computarizados, los cuales se estaban convirtiendo en parte integral de las operaciones gerenciales o financieras de la organización y con el crecimiento en tamaño y complejidad de tales sistemas, existía una gran necesidad de desarrollar capacidad de auditoría en esta área. Se encaminaron a llenar dicha necesidad compartiendo experiencias e ideas con compañeros en la materia, y desarrollado cursos de entrenamiento y material educativo para asesorar a aquellos a los que se les asignaran responsabilidades de auditoría similares.

Siendo esa su idea, en la actualidad se observa cierta, por el hecho que la organización que fundaron, la Asociación de Auditores EDP, se ha convertido en una organización mundial de profesionales en Auditoría de sistemas de información, representando tanto auditoría interna como externa, trabajando en las áreas de la industria privada y gubernamental.

Desde su fundación en 1969, la Asociación de Auditores EDP (EDPAA) se ha dedicado a la promoción de investigación, educación y la certificación de la auditoría de sistemas de información. Sus objetivos primarios son proporcionar un foro a sus miembros, que los impulsa a un intercambio libre de conocimientos acerca de la auditoría de sistemas de información y asesorar a sus miembros en su crecimiento y desarrollo profesional.

La fundación de auditores EDP (EDPAF), fundada en 1967 fue establecida para involucrarse en actividades educacionales y de investigación en el campo de auditoría de sistemas de información.

Los objetivos de la fundación son:

* *Desarrollar y mantener las normas profesionales de auditoría de sistemas de información.*
* *Conducir investigaciones en la auditoría de sistemas de información y controles de computadora, y*
* *Asesorar profesionales en el estudio de auditoría y de sistemas de información.*

En su reunión anual en 1985, llevada a cabo durante la conferencia internacional de la asociación en Salt Lake City, Utha, USA, los miembros generales de EDPAA aprobaron el establecimiento de una junta de normas y le dio a dicha junta la responsabilidad de establecer normas para la practica profesional de la auditoría de sistemas de información.

Generalidades

Los sistemas computacionales son herramientas útiles aplicada en el manejo y operación de muchas organizaciones. Dichos sistemas pueden afectar el control en muchas facetas y operaciones de la organización. El desarrollo y soporte de dichos sistemas puede requerir de una parte significativa de los recursos totales de la organización. Cuando estas condiciones existen, la misión del auditor puede incluir la auditoría del desarrollo, mantenimiento y operación de los sistemas.

El trabajo de un auditor, tanto externo como interno, está regido por las normas desarrolladas para un número de organizaciones, profesionales, cada uno de los cuales busca asegurar la calidad de trabajo de auditoría que se está ejecutando.

Necesidad de normas de Auditoría de sistemas de información.

Las normas de estas organizaciones profesionales se aplican en relación al trabajo de sus miembros, relacionándolos con la naturaleza del trabajo de auditoría involucrada. La EDPAF ha determinado que la naturaleza especializada del trabajo de auditoría de sistemas de información, y las técnicas necesarias para realizar dicha auditoría, requiere que el desarrollo y promulgación de las normas de auditoría las cuales se aplican específicamente a la auditoría de sistemas de información.

Definición de auditoría de sistemas de información.

Para el propósito de estas normas, la auditoría de sistemas de información se define como cualquier auditoría que involucra la revisión y evaluación en todos los aspectos (o cualquier porción) de sistemas automatizados de información, incluyendo los procesos no automatizados relacionados, así como las interfases relacionadas.

Los auditores de sistemas de información revisan y evalúan el desarrollo, mantenimiento y operación de los diferentes componentes en los sistemas automatizados (o dichos sistemas como un todo) y sus interfases con las áreas no automatizadas de las operaciones de la organización. Los objetivos de dicha auditoría son generalmente asesorar hasta que punto dichos sistemas o componentes producen información precisa y confiable y determinan si dicha información está de acuerdo con los requerimientos gerenciales y cualquier provisión aplicable.

La junta de normas y sus operaciones.

La junta de normas es un comité permanente de la EDPAF, y se compone de puestos electos. De sus nueve miembros, cinco con miembros de la fundación que desempeñan su labor tiempo completo y cuatro son miembros externos. El vicepresidente para normas de la EDPAF (un miembro de la fundación y presidente de la junta de normas), propone los miembros externos a participar en la junta ; dichas proposiciones son efectivas bajo la confirmación de la junta de miembros de la fundación. El término de participación de un miembro externo es de 3 años, sujeto a renovaciones anuales.

La misión adoptada formalmente por la junta es la siguiente:

> *"Para incrementar la calidad de la auditoría de sistemas de información, una responsabilidad de la junta de normas es promulgar y mantener normas de práctica. Estas normas se aplican a miembros de la asociación de auditores EDP y a los poseedores de certificados de auditoría de sistemas de información" .*

La junta por lo tanto define, desarrolla y promulga normas, interpretaciones de normas, guías, procedimientos, y otras informaciones relacionadas con normas para la práctica profesional de auditoría de sistemas de información. Realiza este trabajo a través del comité de normas (compuesto por miembros

seleccionados por la asociación de auditores EDP), a través de trabajo y de grupos de control y revisión, que constituyen una interrelación representativa de la profesión de auditoria de sistemas de información.

Procedimientos de la junta.

Antes de la promulgación de las normas, se distribuye un documento borrador expositor en varias fases a un amplio grupo de profesionales en la auditoría de sistemas para solicitar comentarios. El propósito de brindar un documento borrador a los practicantes es poner a prueba las normas y determinar si están cumpliendo con su propósito, es responsabilidad de la junta, a través del comité de normas, asegurar que todos los comentarios escritos sean revisados y tomados en consideración. La última decisión con respecto a los formatos, alcance y día efectivo de las normas son responsabilidad de la junta. La promulgación de las normas requiere de la aprobación de dos tercios de la junta.

Autoridad asociada a las normas.

La autoridad asociada a las normas proviene del código de ética profesional (una copia se anexa a este documento), el cual asegura que los miembros de la Asociación de Auditores EDP y los poseedores del certificado de auditoría de sistemas de información cumplirá con las normas de auditoría de sistemas de información adoptadas por la EDPAF. El no cumplimiento de estas normas

podría resultar en la cancelación de la membresía del individuo en la asociación de auditores EDP, y en el caso de auditores certificados en sistemas de información, la revocación del certificado.

Relación entre las normas de auditoría de sistemas de información y otras normas de auditoría.

Las normas de auditoría de sistemas de información promulgadas por la EDPAF, no intentan pasar sobre las normas o regulaciones de auditoría desarrolladas por otras organizaciones profesionales o instituciones gubernamentales. En cualquier situación en la que se perciba discrepancia entre las normas de la fundación de auditoría EDP y los de otra organización, sea responsabilidad del auditor usar su criterio profesional, basado en factores específicos de la situación, para resolver el conflicto.

Lenguaje

El texto oficial de estas normas y otras relacionadas con la información promulgada por la EDPAF, es un texto aprobado por la junta en idioma inglés. Los diferentes capítulos y regiones de la asociación de auditores EDP están autorizados a preparar traducciones de este material en su lenguaje materno, como tenga sentido para ellos, pero dichas traducciones deben indicar el nombre del grupo que las realiza. El documento traducido debe contener una sentencia explícita que es una traducción del texto original en inglés.

NORMAS GENERALES

DE

AUDITORIA DE SISTEMAS DE INFORMACIÓN

Introducción

La fundación de auditores EDP, Inc., ha determinado que la naturaleza especializada de la auditoría de sistemas de información, y las técnicas necesarias para desarrollar dicha auditoría, requieren del desarrollo y promulgación de las normas de auditoría de sistemas de información que se aplican específicamente a dicha auditoría.

La auditoría de sistemas de información se define como cualquier auditoría que coadyuva a la revisión y evaluación de todos los aspectos (o en cualquier porción) de sistemas automatizados de información, incluyendo los procesos no automatizados relacionados, así como las interfases relacionadas.

Las normas promulgas por la EDPAF son aplicables al trabajo de auditoría de sistemas de información desarrolladas por miembros de la asociación de auditores EDP y por miembros poseedores de certificados en auditoría de sistemas de información.

Mayor reseña histórica de la asociación de auditores EDP, la fundación de auditores EDP y su promulgación de normas de auditoría de sistemas de

información se encuentra "Prefacio a normas Generales para Auditoría de Sistemas de Información y Declaración sobre las Normas de Auditoría de Sistemas de Información.

Objetivos.

Los objetivos de estas normas es informar a los auditores del nivel mínimo aceptable de funcionamiento requerido para llenar la responsabilidades profesionales planteadas en el código de ética profesional, e informar a la gerencia y otras partes interesadas de las expectativas de la profesión concernientes con el trabajo de practicantes.

Normas Generales de Auditoría de sistemas de información.

Las siguientes diez normas son aplicables a la auditoría de sistemas como se definen a continuación:

Independencia.

Norma General No.1 : Actitud y apariencia. En todos los aspectos relacionados con auditoría, el auditor de sistemas de información debe ser independiente de lo auditado en actitud y apariencia.

Norma General No.2 : Relación organizacional. La función de auditoría de sistemas de información debe ser lo suficientemente independiente del área auditada de manera que permita la realización objetiva de la auditoría.

Norma General No.3 : Código de la ética Profesional. El auditor de sistemas de información debe referirse al Código de Adecué Profesional EDPAF.

Competencia Técnica.

Norma Genera No.4 : Habilidades y Conocimientos. Los auditores de sistemas de información debe ser técnicamente competente poseedor de las técnicas y conocimientos necesarios para la ejecución del trabajo de auditor.

Norma General No. 5 : Educación Profesional continua. El auditor de sistemas de información debe mantener competencia técnica a través de la educación apropiada y continua.

Ejecución del trabajo.

Norma General No.6 : Planeación y Supervisión. La auditoría de sistemas de información debe ser planeada y supervisada para asegurar que los objetivos de la auditoría se están logrando y se están respetando las normas establecidas.

Norma General No.7 : Requerimiento de la Evidencia. Durante la ejecución de la auditoría el auditor de sistemas de información debe obtener evidencia para respaldar los hallazgos y conclusiones reportadas.

Norma General No.8 : Cuidado Profesional. Cuidado profesional debe observarse en todos los aspectos del trabajo del auditor de sistemas de información incluyendo la observancia en la aplicación de estas normas de auditoría.

Comunicación de Resultados.

Norma General No.9 : Informando sobre la Cobertura de la Auditoría. Al preparar los reportes el auditor de sistemas de información debe establecer los objetivos de la auditoría, su período de validez, la naturaleza y extensión del trabajo de auditoría desarrollado.

Norma General No. 10 : Informando sobre los Hallazgos y Conclusiones. Al preparar los reportes el auditor de sistemas de información debe mencionar sus hallazgos y conclusiones referentes al trabajo de auditoría desarrollada y cualquier reserva o calificación que el auditor tenga respecto a lo auditado.

Fecha Efectiva.

Estas normas son efectivas para la auditoría de sistemas de información con período de validez comenzando el 1o. de enero de 1988.

A- 12

EDP AUDITORS FOUNDATION

Código de Ética Profesional

La fundación de auditores, pone en práctica este código de Ética Profesional para guiar a profesionales miembros de la Asociación de Auditores EDP y/o poseedores de certificado en auditoría de sistemas de información .

Los auditores de sistemas de información deben:

1. *Respaldar el establecimiento de procedimientos y controles para sistemas de información de conformidad con las normas apropiadas.*
2. *Cumplir con las normas de Auditoria de Sistemas de información tal como fueron adoptadas por la fundación de Auditores EDP.*
3. *Servir al interés de patronos, accionistas, clientes y público en general en un forma leal y honesta y de ninguna forma ser parte de una actividad y legal o impropia .*
4. *Mantener la confidencialidad de la información obtenida a través de sus actividades. Esta información no debe ser utilizada para beneficio propio o dar a conocer a las partes inapropiadas.*
5. *Realizar sus actividades de manera independiente y objetivas y debe evitar actividades que amenacen, o aparenten amenazar, su independencia.*

6. *Mantener la competencia en aquellas áreas que interrelacionan la auditoría y los sistemas de información, a través de la participación en actividades de desarrollo profesional .*

7. *Tener el debido cuidado de obtener y documentar suficiente material confiable en el cual basar conclusiones y recomendaciones.*

8. *Informar a las partes adecuadas de los resultados obtenidos del trabajo de auditoría realizados.*

9. *Apoyar la educación de la gerencia, clientes y público en general para enriquecer el conocimiento de éstos sobre auditoría y sistemas de información.*

10. *Mantener una conducta intachable y un carácter firme tanto en las actividades profesionales como personales.*

ANEXO B

INSTRUMENTO PARA LA AUDITORÍA A LA ADMINISTRACIÓN DEL ÁREA DE PROCESAMIENTO DE DATOS.

ANEXO B1

INSTRUMENTO PARA EVALUAR AL COMITÉ COORDINADOR DE ACTIVIDADES.

a) **Planificación estratégica**; si el comité no posee planes estratégicos pasar al tercer formulario; en caso contrario desarrollar desde el primer formulario.

EMPRESA:	GERENTE:
CÓDIGO:PR02-FM01	OBJETIVO: Evaluar la Planificación estratégica

EVALUADO POR:	FECHA:	HORA:

INSTRUCCIONES: Estime una calificación en base a la ponderación que posee cada sección y si existe documentación anexar al formulario. (E1 significa evaluación No.1)

ELEMENTOS	%	E1	E2	E3	OBSERVACIONES
PLANES ECONÓMICOS					
Grado de claridad	15				
Objetividad en metas	15				
Períodos estimados	10				
Definición de responsables.	10				
Recursos necesarios	5				
Acciones concretas	10				
Se utiliza software para la planificación	10				
Tiempo de ejecución del Software.	5				
Eficiencia de ejecuciones	5				
Utilización eficaz de máquinas	5				
Eficiencia del sistema	10				
TOTAL DE PUNTUACIÓN					

CONCLUSIONES:

RECOMENDACIONES:

EMPRESA:	GERENTE:
CÓDIGO:PRO2-FM02	OBJETIVO: Evaluar Planes estratégicos

EVALUADO POR:	FECHA:	HORA:

INSTRUCCIONES: Estime una calificación en base a la ponderación que posee cada sección y si existe documentación anexar al formulario.(E1 significa evaluación No. 1)

ELEMENTOS	%	E1	E2	E3	OBSERVACIONES
PLANES DE PRODUCCIÓN					
Grado de claridad	15				
Objetividad en metas	15				
Periodos estimados	10				
Definición de responsables.	10				
Recursos necesarios	5				
Acciones concretas	10				
Se utiliza software para la planificación	10				
Tiempo de ejecución del Software.	5				
Eficiencia de ejecuciones	5				
Utilización eficaz de máquinas	5				
Eficiencia del sistema	10				
TOTAL DE PUNTUACIÓN					

CONCLUSIONES:

RECOMENDACIONES:

b) **Objetivos,** En base al formulario se evaluarán los objetivos del comité coordinador.

EMPRESA:	GERENTE:	
CÓDIGO:PRO2-FM03	OBJETIVO: Evaluar los Objetivos generales	
EVALUADO POR:	FECHA:	HORA:

INSTRUCCIONES: Estime una calificación en base a la ponderación que posee cada sección y si existe documentación anexar al formulario. (E1 significa evaluación No.1)

ELEMENTOS	%	E1	E2	E3	OBSERVACIONES
OBJETIVOS GENERALES					
Conceptualización	20				
Documentación	5				
Aprobación total	10				
Grado en que el objetivo representa un solo juicio o afirmación	15				
Claridad en fecha de finalización del Objetivo	5				
Claridad en objetivos	15				
Precisos y específicos	10				
Concordancia con políticas, planes y programas	5				
Autoridad de responsables para ejecutarlos	5				
Efectividad de los controles de los objetivos	10				
TOTAL DE PUNTUACIÓN					

CONCLUSIONES:

RECOMENDACIONES:

EMPRESA:	GERENTE:
CÓDIGO:PR02-FM04	OBJETIVO: Evaluar Objetivos especificos

EVALUADO POR:	FECHA:	HORA:

INSTRUCCIONES: Estime una calificación en base a la ponderación que posee cada sección y si existe documentación anexar al formulario.(E1 significa evaluación No.1).

ELEMENTOS	%	E1	E2	E3	OBSERVACIONES
OBJETIVOS ESPECÍFICOS					
Conceptualización	20				
Documentación	5				
Aprobación total	10				
Grado en que el objetivo representa un solo juicio o afirmación	15				
Claridad en fecha de finalización del Obj.	5				
Claridad en objetivos	15				
Precisos y especificos	10				
Concordancia con politicas, planes y programas	5				
Autoridad de responsables para ejecutarlos	5				
Efectividad de los controles de los objetivos	10				
TOTAL DE PUNTUACIÓN					

CONCLUSIONES:

RECOMENDACIONES:

c) **Información tecnológica,** En esta parte se pretende evaluar la tecnología en cuanto a su eficiencia y documentación técnica. En base al formulario siguiente

EMPRESA:	GERENTE:
CÓDIGO:PRO2-FH05	OBJETIVO: Evaluar la información tecnológica

EVALUADO POR:	FECHA:	HORA:

INSTRUCCIONES: Estime una calificación en base a la ponderación que posee cada sección y si existe documentación anexar al formulario. (E1 significa evaluación No.1)

ELEMENTOS	%	E1	E2	E3	OBSERVACIONES
Actualización de la documentación técnica:					
a)Sist. de aire acondicionado	5				
b)Fuentes de energía.	5				
c)Reguladores de voltaje.	10				
d)Fuentes de energía del Dpto.	10				
e)Sist. de iluminación	10				

ELEMENTOS	%	E1	E2	E3	OBSERVACIONES
f)Sist. de comunicación	10				
Personal técnico calificado para el Mantto. y admón de la función:					
a)Profesional	30				
b)técnico	10				
c)otros estudios	10				
TOTAL DE PUNTUACIÓN					

EMPRESA:	GERENTE:
CÓDIGO:PR02-FM06	OBJETIVO:Evaluar la factibilidad de la infraestructura técnica.

EVALUADO POR:	FECHA:	HORA:

INSTRUCCIONES:Coloque el dato del resumen del estudio de factibilidad para cada elemento, y para cada estudio de factibilidad realizado. (EST1 significa es el número de estudio)

ELEMENTOS	EST1	EST2	EST3	OBSERVACIONES
Capacidad instalada				
Inversión total:				
a)Fondos propios				
b)Financiamiento				
Producción del equipo				
Ventas esperadas				
Precio Unit. de Merc.				
Costo unitario				
Utilidad esperada				
Rentabilidad				
Tasa mínima aceptable				
Sist. de equilibrio				

d) **Alcance de las funciones de procesamiento de datos con respecto a la aplicación a auditar (Controles de contratación del servicio)**, esta parte evaluará la contratación, controles de la planificación de actividades del departamento y la planificación de los recursos a utilizar.

Por lo tanto recopilar la siguiente información:

i. **El formulario para la contratación del** servicio de auditoria posee:

i.1 Nombre del contratista._____(5% de puntuación)

i.2 Nombre del contratado._____(5%)

i.3 Información general de cada uno._____ (5%)

i.4 Tiempo de contratación._____ (25%)

i.5 Actividades a cumplir._____ (15%)

i.6 Honorarios o cantidad del cobro por el servicio. _____ (15%).

i.8 Recursos a utilizar _____ (15%).

i.9 Obligaciones en caso de no cumplir _____ (15%).

e) **Definición de prioridades para el desarrollo de labores.**

En esta parte se evaluará la forma de priorización de labores del departamento de sistemas.

Para lograr este objetivo es necesario anexar los formularios en donde se definen las actividades del departamento y luego responder la siguiente información :

i. La clasificación de las actividades se define como:

i.1 Por orden de importancia.____

i.2 Por orden cronológico___

i.3 Por orden alfabético___

i.4 otros ___ (0-30)

ii. Se justifica el orden. si.(30) no.(0)

iii. Posee la aprobación de las autoridades del departamento.(0-40)

f) **Monitoreo y cuantificación de resultados obtenidos por el área.** Para lograr una gestión administrativa eficiente es necesario monitorear y cuantificar los resultados obtenidos en relación a los objetivos, políticas y planes de trabajo establecidos en un principio por la auditoria.

* **Objetivos** (0 - 40)

- Anexe los tipos de controles en relación a los objetivos planteados.
- Los controles son:
  * Cuantificables.
  * Cualitativos.
- Claridad de los controles (se entiende lo que se pide)._____
- Alcance de los controles. _____

- Representan las desviaciones existentes en las áreas que controla._____
- Los mecanismos y metodologías de la gestión son adecuados._____
- Se logran corregir las desviaciones _____

_____

- Mecanismos de corrección adecuados _____

_____

* **Políticas** (0 - 30)

- Anexe los tipos de controles en relación a las políticas planteadas.
- Los controles son:
    * Cuantificables.
    * Cualitativos.
- Claridad de los controles (se entiende lo que se pide)._____
- Alcance de los controles. _____
- Representan las desviaciones existentes en las áreas que controla._____
- Los mecanismos y metodologías de la gestión son adecuados._____
- Se logran corregir las desviaciones _____

_____

- Mecanismos de corrección adecuados _____

_____

* **Planes** (0 - 40)

- Anexe los tipos de controles en relación a los planes planteados.
- Los controles son:
  * Cuantificables.
  * Cualitativos.
- Claridad de los controles (se entiende lo que se pide)._____
- Alcance de los controles. _____
- Representan las desviaciones existentes en las áreas que controla._____
- Los mecanismos y metodologías de la gestión son adecuados. _____
- Se logran corregir las desviaciones _____

_____

_ Mecanismos de corrección adecuados _____

_____

g) **Plan de recuperación de instalación (Fallas y desastres).** En esta parte se evaluarán los planes .que desarrolla el comité en caso de contingencias en relación a los activos del centro de cómputo, para el caso información, equipo y personal.

Por lo tanto es necesario responder los siguientes literales:

i. Anexe los planes de recuperación en vigencia:

En cuanto a la información.

- Se encuentra asegurada. _____
  (0 - 20)
- Existe información en otra institución para ser recuperada. _____
  (0 - 10)
- El lugar físico es seguro. _____
  (0 - 10)
- La información se actualiza constantemente. _____
  (0 - 20)
- El plan contempla presupuestación _____
  (0 - 20)
- Existe planificación de materiales y personal._____
  (0 - 20)

ANEXO B2

INSTRUMENTO PARA EVALUACIÓN DE LA ORGANIZACIÓN DE PED.

NIVELES JERÁRQUICOS(es conveniente conocer los niveles jerárquicos para poder evaluar si son los necesarios y si bien están definidos).

1.- ¿ Los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área?

SI NO

2.- ¿ Permiten los niveles jerárquicos actuales que se desarrolle adecuadamente la :

Operación? SI NO

Supervisión? SI NO

3.- ¿ Los niveles actuales permiten que se tenga una ágil :

Comunicación ascendente? SI NO

Comunicación descendente? SI NO

Toma de decisiones? SI NO

4.- ¿Se considera que algunas áreas deberían tener:

Mayor jerarquía ? SI NO

Menor jerarquía ? SI NO

PUESTOS(Se debe tener cuidado de que estén bien definidas las funciones de cada puesto, ya que desafortunadamente existe mucha confusión en los nombres que se dan a los puestos dentro del medio de la informática).

1.- ¿Los puestos actuales son adecuados a las necesidades que tiene el área para llevar a cabo las funciones? SI NO

NO,¿porqué razón?

2.- ¿El número de empleados que trabajan es adecuado para cumplir con las funciones encomendadas?

SI NO

AUTORIDAD

1.- ¿Se encuentra definida adecuadamente la línea de autoridad ? SI NO

2.- ¿Su autoridad va de acuerdo a su responsabilidad?

SI NO,¿Porqué razón?

3.- ¿En su área se han presentado conflictos por el ejercicio de la autoridad?

SI, Explique en que casos NO

4.- ¿Existe en el área algún sistema de sugerencias y quejas por parte del personal?

FUNCIONES (Las funciones en informática pueden diferir de un organismo a otro, aunque se designen con el mismo nombre; por ejemplo, la función del programador en un organización puede ser diferente en otra organización).

Existencia de las funciones.

1.- ¿Se han establecido funciones del área? SI NO ¿Porqué no?

2.- ¿Están por escrito en algún documento las funciones del área?¿Cuál es la causa de que no estén por escrito?

3.- ¿Cuál es la forma de darlas a conocer?

4.- ¿Quién elaboró las funciones?

5.- ¿Quién las autorizó?

6.- ¿Las funciones están determinadas a la consecución de los objetivos institucionales e internos?

7.- ¿Las funciones del área están acordes al reglamento interno? SI NO, ¿En que considera que difieren?

8.- ¿A qué nivel se conocen las funciones del área?

9.- ¿Son adecuadas a la realidad las funciones? SI NO, ¿Porqué no son adecuadas?

10.- ¿Son adecuadas a las necesidades actuales?

11.- ¿Están adecuadas a las cargas de trabajo? SI NO

12.- ¿Existen conflictos por las cargas de trabajo desequilibradas? SI NO

13.- ¿Participó la dirección de informática en su elaboración? SI NO, ¿Porqué no?

14.- ¿Están delimitadas las funciones? SI NO ¿A nivel de departamento? ¿A nivel de puesto?

15.- ¿Las actividades que realiza son acordes a las funciones que tiene asignadas? SI NO, ¿Qué tipo de actividades realiza que no están acordes a las funciones asignadas?

16.- ¿Quién es el responsable de ordenar que se ejecuten las actividades?

17.- ¿Para cumplir con sus funciones requiere de apoyos de otras áreas? SI NO SI, ¿de qué tipo?

ANEXO C

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE DESARROLLO DE SISTEMAS.

ANEXO C1

INSTRUMENTO PARA EVALUACIÓN DEL COMPROMISO PROGRESIVO PARA EL DESARROLLO DE SISTEMAS.

1. ¿Existe un plan claro y detallado para el desarrollo de sistemas?

SI ( ) NO ( ) DICTAMEN

2. ¿Se encuentra definido el grado de compromiso de la organización con respecto al proyecto?

SI ( ) NO ( )

3. ¿Se encuentra definido el grado de riesgo para cada una de las actividades?

SI ( ) NO ( )

*4. Determinar con hechos comprobables las erogaciones para cada una de las actividades de los proyectos de desarrollo de sistemas y por cada desviación que se encuentre acumule el grado de riesgo y súmelos. Total _____ DICTAMEN

ANEXO C2

INSTRUMENTO PARA EVALUACIÓN A LAS ACTIVIDADES DEL DESARROLLO DE SISTEMAS.

1. ¿La planeación y el desarrollo son manejados por un equipo de proyectos integrado por personal del usuario y del departamento de sistemas?

SI ( ) NO ( )

2. ¿El personal usuario desempeña un papel crítico en la definición de los requerimientos y la identificación de los beneficios para cada nueva aplicación?

SI ( ) NO ( )

3. ¿Las personas del departamento de sistemas actúan como coordinadores o jefes del proyecto?

SI ( ) NO ( )

4. ¿Las personas del departamento de sistemas proporcionan apoyo técnico?

SI ( ) NO ( )

5. Verificar que existan cada una de las actividades del desarrollo de sistemas. Si llega a hacer falta una, es una situación crítica y de su dictamen.

¿Falta al menos una de estas actividades?

SI ( ) NO ( )

6. Verificar que existan los alcances y objetivos, grado de detalle, habilidades requeridas y consideraciones de control de cada una de las actividades de sistemas y de su dictamen.

¿Falta al menos una de estas actividades?

SI ( ) NO ( )

ANEXO C3

INSTRUMENTO PARA EVALUACIÓN DE LA PLANEACIÓN DE SISTEMAS.

1. ¿Se identifican el alcance y los objetivos del proyecto?

SI ( ) NO ( )

2. ¿Se identifican claramente preliminarmente los siguientes aspectos?

( ) Costo

( ) Beneficios

( ) Presentaciones de diseño

( ) Decisiones relativas a los presupuestos de inversión

( ) Grado de conocimiento técnico

3. ¿Se estudian los procedimientos existentes de la organización?

SI ( ) NO ( )

4. ¿Se determina que situaciones pueden mejorarse?

SI ( ) NO ( )

5. ¿Se identifican los métodos de procesamiento aplicables?

SI ( ) NO ( )

6. ¿Se evalúa la viabilidad de las técnicas computarizadas para la aplicación en estudio?

SI ( ) NO ( )

7. ¿Se identifican y cuantifican los costos y beneficios proyectados?

SI ( ) NO ( )

8. Debido al alto riesgo involúcrado en la planeación de sistemas. ¿Se generan juicios sobre la marcha para determinar el alcance o profundidad de los esfuerzos o erogaciones que van a comprometerse?

SI ( ) NO ( )

9. ¿Se busca que las tareas relativas a la planeación de los proyectos de sistemas deban ser efectuadas por gerentes de alto nivel?. (la razón es que deben poseer madurez y criterio necesarios, además de tener suficiente jerarquía para que sus recomendaciones tengan peso)

SI ( ) NO ( )

10. ¿Se produce un reporte de la planeación del sistema?

SI ( ) NO ( )

11. ¿Incluye recomendaciones del equipo de proyectos sobre si debe continuar o no?

SI ( ) NO ( )

12. ¿Existe una decisión gerencial respecto a si debe continuarse un proyecto?

SI ( ) NO ( )

nota:	Por lo general los juicios más críticos se hacen en los inicios del proyecto aplicándose la regla de relevancia 80/20. Significa que el 80 % de la importancia y el interés de la gerencia se centrará en el 20 % de los documentos y esfuerzos.

ANEXO C4

INSTRUMENTO PARA LA EVALUACIÓN DE LAS ESPECIFICACIONES DEL USUARIO.

1. ¿Se logra que los analistas se familiaricen ampliamente con el medio del usuario?

SI ( ) NO ( )

2. ¿Se analizan los procedimientos que se llevan a cabo?

SI ( ) NO ( )

3. ¿Se hace entender al usuario que su información será la base de las recomendaciones de los analistas?

SI ( ) NO ( )

4. ¿Es el usuario quien comunica sus propias necesidades?

SI ( ) NO ( )

5. ¿Se desarrolla un manual detallado que describa

( ) El nuevo sistema

( ) Servicios y procesamiento que se efectuarán por y para el usuario

( ) Criterios de actuación que habrán de observarse

comentario:
Este manual es básico para examinar el proceso de desarrollo o auditar aplicaciones, así como para establecer las características especificas de las medidas de calidad que van a aplicarse a las operaciones y controles.

6. ¿Se establece la responsabilidad respecto a la implantación y operación del nuevo sistema?

SI ( ) NO ( )

7. ¿Se establece documentación formal y escrita de los requerimientos?

SI ( ) NO ( )

8. ¿Se establece un diagrama de flujo del sistema existente?

SI ( ) NO ( )

9. ¿Se estudian los documentos existentes del sistema actual?

SI ( ) NO ( )

10. ¿Se documenta el sistema en uso?

SI ( ) NO ( )

11. ¿Se describe:

( ) El trabajo de cada persona

( ) Su flujo a través del sistema

( ) Fuente de datos de entrada

nota:	No debe dedicarse tiempo y esfuerzo a documentar una nueva aplicación propuesta, sino hasta que exista un mutuo acuerdo con la gerencia del usuario y se haya documentado y entendido por completo el sistema vigente.

12. ¿Se elabora un documento que establece las áreas en que pueden hacerse mejoras?

SI ( ) NO ( )

13. ¿Se documenta el nuevo sistema?

SI ( ) NO ( )

14. ¿Al documentar el nuevo sistema se toma en cuenta:?

( ) Que información será reportada

( ) Que decisiones serán afectadas

( ) Contenido y diseño de los reportes

( ) Formas que se han de generar

15. ¿Se considera que la documentación del nuevo sistema determinará el contenido de los datos que serán necesarios en los archivos del computador (para generar los resultados requeridos)

SI ( ) NO ( )

16. ¿Es revisada la documentación por los usuarios y el personal de sistemas para verificar la claridad de comunicación?

SI ( ) NO ( )

17. ¿Se establecen juntas formales entre el personal clave de la organización usuaria e informática para comentar y entender la misma documentación?

SI ( ) NO ( )

18. ¿Se establecen los elementos de comunicación de las aplicaciones en uso siguientes?

( ) Funciones manuales

( ) Descripciones de los documentos de entrada y salida

( ) Descripciones de los archivos

( ) Diagrama de flujo del sistema existente (tanto de las fases manuales como computarizadas)

( ) Resumen de las funciones efectuadas

( ) Descripción detallada de los datos (Registros) y de los elementos (campos)

( ) Seguridad y respaldos existentes

( ) Glosario de términos

19. Durante la actividad de las especificaciones del usuario deberá prepararse una documentación para describir el contenido y el procesamiento relacionadas con la aplicación propuesta. ¿Consiste ésta en los siguientes aspectos?

( ) Un formato de reporte de salida

( ) Descripción del reporte de salida (sirve de guía para el diseño)

  ( ) Fuentes de información

  ( ) Especificación de impresión del computador

  ( ) Manejo del reporte en el control

  ( ) Distribución

( ) Forma de descripción de los datos de entrada (especifica como será cada registro al presentarse al departamento de sistemas para su conversión y procesamiento)

( ) Especificación de los campos de datos relacionados con cada reporte bajo la nueva aplicación (contenido de un registro por cada documento)

( ) Tabla que indique los pasos de procesamiento a seguir bajo condiciones variables del contenido de datos (para cada dato de salida)

( ) Tablas de decisiones o su equivalente en diagramas que cubra la lógica que va a aplicarse en el procesamiento por computador

( ) Especificación de las limitaciones que vayan a aplicarse al diseño de la nueva aplicación en términos de la calendarización y oportunidades, las políticas y la identificación preliminar de la viabilidad o requerimientos técnicos

( ) Identificación y segregación de todos los controles que vayan a establecerse dentro de la nueva aplicación de acuerdo al punto en que se implantarán

( ) Diagrama de flujo analítico, segregado por funciones, que descubra las porciones manuales de la nueva aplicación propuesta

( ) Manual de funciones para la nueva aplicación (es un compromiso por parte de la gerencia del usuario respecto al trabajo que ha de efectuarse dentro de su organización)

( ) Resumen gerencial (incluye recomendaciones de viabilidad y los beneficios generales de la nueva aplicación propuesta. Al final de la actividad de las especificaciones del usuario, este reporte servirá como sección inicial de la documentación que se

considerará para determinar si se debe continuar o no, y así establecer prioridades)

( ) Propósito resumido, por separado, de los beneficios de la nueva aplicación propuesta. (la organización usuaria deberá relacionarse a sí misma muy estrechamente con este documento)

( ) Evaluación económica específica del impacto de la nueva aplicación propuesta sobre las operaciones dentro del departamento del usuario

nota:	El producto principal de la actividad de especificaciones del usuario consiste en un manual detallado, encuadernado, que incorpore el contenido y documentación indicados, en términos de las necesidades y políticas de la organización usuaria y de lo que esta espera de la aplicación planeada.

ANEXO C5

INSTRUMENTO PARA LA EVALUACIÓN DE LAS ESPECIFICACIONES TÉCNICAS.

1. Para las funciones operativas y las porciones computarizadas. ¿Se desarrollan decisiones a nivel técnico y documentación?

SI ( ) NO ( )

2. Esta documentación técnica (que debe llevar más detalles que las actividades anteriores), ¿Se prepara para proporcionar las instrucciones que deben seguirse durante la actividad de programación?

SI ( ) NO ( )

3. ¿Se toma en cuenta que esta documentación será vital para los cambios de mantenimiento que se hagan después de la conversión e implantación de la aplicación?

SI ( ) NO ( )

4. ¿Se desarrolla un plan y calendario detallados para la preparación de los programas de aplicación? (necesita conocimientos de alto nivel)

SI ( ) NO ( )

5. ¿Se desarrollan el diseño y documentación finales, detallados, para las porciones computarizadas de la nueva aplicación como punto de partida dentro del plan de trabajo? (para dividir al procesamiento en módulos)

SI ( ) NO ( )

6. ¿Se determinan en los archivos que soportarán a la aplicación?

( ) Organización lógica

( ) Organización física

( ) índice secuencial

( ) Acceso al azar

( ) Densidad de almacenamiento de datos (empaque)

( ) Tamaño de los registros

( ) Otros

7. ¿Se considera el equipo físico y medio de almacenamiento que deben asignarse para lograr el uso más eficiente del equipo y de los materiales de apoyo de la aplicación?

SI ( ) NO ( )

8. Si se descubre la necesidad de modificar las especificaciones o procedimientos previamente establecidos con el usuario. ¿Se explican completamente al usuario y se obtiene su conformidad?

SI ( ) NO ( )

9. ¿Se incluye sección de lenguaje de programación?

SI ( ) NO ( )

10. ¿Se incluye sección de programas de operación del sistema operativo?

SI ( ) NO ( )

11. ¿Se desarrollan normas para el manejo de la aplicación por parte del centro de operaciones?

SI ( ) NO ( )

12. En caso de desarrollarse las normas. ¿Cuales de las siguientes se consideran?

( ) Controles del operador

( ) Calendarios de retención de archivos

( ) Acciones que debe seguir el operador en casos de interrupción del programa

( ) Estipulaciones relativas al respaldo del procesamiento

( ) Procedimientos de reinicio

13. ¿Se desarrolla un calendario de programación?

SI ( ) NO ( )

ANEXO C6

INSTRUMENTO PARA LA PLANEACIÓN DE LA IMPLANTACIÓN.

1. ¿Se desarrollan planes detallados para las actividades restantes del proyecto?

SI ( ) NO ( )

2. ¿Se hace uso del conocimiento acumulado y la experiencia obtenida en las actividades precedentes del proyecto?

SI ( ) NO ( )

3. ¿Se obtienen las revisiones y aprobaciones totales y completas del usuario y la gerencia?

SI ( ) NO ( )

4. ¿Se prepara un documento para plan de procedimientos y entrenamiento?

SI ( ) NO ( )

5. El plan de procedimientos y entrenamiento del usuario debe cumplir con una lista de puntos que se muestra a continuación. Señale las que su organización efectúa:

( ) Preparación del usuario

( ) Notificación interna

( ) Notificación externa

( ) Consideraciones de políticas

( ) Procedimientos (plan de contenido, manuales, publicación y expedición)

( ) Descripciones de trabajo

( ) Formas (diseño, impresión interna, Impresión externa)

( ) Entrenamiento y orientación (plan del programa, manual de instrucciones del programa, presentación, otros.)

( ) Equipos y enseres especiales

( ) Equipo de oficina requerido

( ) Espacio y distribución de piso

( ) Personal (calificación y contratación)

A continuación se presenta un ejemplo de lo anterior:

LISTA DE PUNTOS A VERIFICAR PARA LOS PROCEDIMIENTOS Y PLAN DE ENTRENAMIENTO DEL USUARIO

ORGANIZACIÓN:_____
DEPARTAMENTO:_____
SISTEMA:_____
USUARIO RESPONSABLE:_____

PREPARADO POR:_____
REVISADO POR:_____
FECHA:_____

PAG___ DE___
PROYECTO
No.____

DESCRIPCIÓN DE LA ACTIVIDAD	PERSONA RESPONSABLE	ORGANIZACIÓN	FECHA DE INICIACIÓN	FECHA DE TERMINACIÓN	APROBADO POR
1. Preparación del usuario					
2. Notificación interna Aviso al ejecutivo Aviso al empleado					
3. Notificación externa Coordinación con el cliente Coordinación con el proveedor Relaciones públicas Otros					
4. Consideraciones de políticas Corporativas Divisionales					
5. Procedimientos Plan del contenido Manuales Publicación y expedición					
6. Descripciones de trabajo					

7. Formas Diseño Impresión interna Impresión externa					
8. Entrenamiento y orientación Plan del programa Manual de instrucciones del programa Presentación Otros					
9. Equipo y enseres especiales Determinación de requerimientos Departamento de ingeniería Subcontratistas					
10. Equipo de oficina requerido					
11. Espacio y distribución de piso					
12. Abastecimientos					
13. Personal Reclasificación Contratación					
Aprobado por:_____ Grupo de Sistemas			_____ Encargado del proyecto		

6. ¿Se tiene establecido el alcance y contenido de un plan para probar un sistema?

SI ( ) NO ( )

7. En la página siguiente se muestra una lista de puntos a verificar para la prueba del sistema.

La idea es reunir y probar los incrementos de una aplicación terminada hasta que todos los elementos se operen y prueben como una unidad. (califique de 0 a 100 según su criterio la prueba del sistema tal y como se hace - 0 no se hace, 100 efectivo)_____.

8. ¿Se prepara una revisión y aprobación por parte de los usuarios y la gerencia?

SI ( ) NO ( )

9. ¿Existe un plan de conversión del sistema anterior al sistema nuevo?

SI ( ) NO ( )

10. Dos páginas más adelante se muestra una lista de puntos para verificar el plan de conversión. (califique de 0 a 100 según su criterio el plan de conversión tal y como se hace)_____.

LISTA DE PUNTOS A VERIFICAR DE LOS PROCEDIMIENTOS PARA LA PRUEBA DEL SISTEMA

ORGANIZACIÓN:_____
DEPARTAMENTO:_____
SISTEMA:_____
USUARIO RESPONSABLE:_____

PREPARADO POR:_____
REVISADO POR:_____
FECHA:_____

PAG___ DE___
PROYECTO
No.___

MÓDULO	NOMBRE DEL MÓDULO	FECHA DE INICIO PROGRAMADA	FECHA DE INICIO REAL	TERMINACIÓN PROGRAMADA	TERMINACIÓN REAL	ENCARGADO DEL PROYECTO

DESCRIPCIÓN DE LA ACTIVIDAD	PERSONA RESPONSABLE	ORGANIZACIÓN	FECHA DE INICIACIÓN	FECHA DE TERMINACIÓN	APROBADO POR
1. Plan de prueba del computador					
2. Procedimientos de prueba Organización usuaria Operación de procesamiento de datos Sistemas y programación Controles del procesamiento de datos					
3. Formas Datos de entrada de prueba Creación y mantenimiento de archivos					

4. Controles Organización usuaria Controles del procesamiento de datos					
5. Equipo Disponibilidad Servicio de emergencia					
6. Personal Organización usuaria Operación de procesamiento de datos Sistemas y programación Controles del procesamiento de datos					
7. Suministro Disponibilidad					
8. Información Creada y verificada Controlada					
9. Archivos Creados y verificados Controlados					
10. Varios					

Aprobado por: _____ _____ _____ _____

Organización usuaria Grupo de sistemas Proc. de datos Encargado del proyecto

LISTA DE PUNTOS A VERIFICAR PARA EL PLAN DE CONVERSIÓN

ORGANIZACIÓN:_____
DEPARTAMENTO:_____
SISTEMA:_____
USUARIO RESPONSABLE:_____

PREPARADO POR:_____
REVISADO POR:_____
FECHA:_____

PAG___ DE___
PROYECTO
No.___

DESCRIPCIÓN DE LA ACTIVIDAD	PERSONA RESPONSABLE	ORGANIZACIÓN	FECHA DE INICIACIÓN	FECHA DE TERMINACIÓN	APROBADO POR
1. Preparación del usuario					
2. Plan de adquisición de archivos de datos					
3. Plan de personal y equipo					
4. Archivos Depuración de registros Requerimientos de codificación Control Conversión Mantenimiento					
5. Formas Diseño Impresión interna Impresión externa Conversión					

6. Procesamiento en paralelo Procedimientos Requerimientos de verificación Calendario					
7. Secuencia de conversión Secuencia organizacional Calendario					
8. Programas de conversión Definición Especificaciones Programación					
9. Interrelación con otros sistemas Archivos Programación Programas					

Aprobado por: _____ _____ _____ _____

Organización usuaria Grupo de sistemas Proc. de datos Encargado del proyecto

ANEXO C7

INSTRUMENTO PARA EVALUAR LA PROGRAMACIÓN.

1. ¿Los resultados que se obtienen son programas de aplicación que han sido compilados y que han sido probados?

SI ( ) NO ( )

2. ¿Se elaboran instrucciones documentadas para los operadores del computador respecto al procesamiento de la nueva aplicación?

SI ( ) NO ( )

3. ¿La programación se hace en base a módulos de programas?

SI ( ) NO ( )

4. ¿Se preparan datos de prueba para utilizarlos con los programas en desarrollo (simultáneamente al diseño de la lógica detallada y la codificación)?

SI ( ) NO ( )

5. ¿Se considera la elaboración de programas de operación adicionales para correr la nueva aplicación?

SI ( ) NO ( )

6. ¿Se desarrollan mensajes de error e instrucciones de operación que harán referencia a las instrucciones de recuperación respecto a los pasos que han de seguirse para reiniciar el procesamiento (bajo cualquier interrupción)?

SI ( ) NO ( )

7. ¿Se elaboran diagramas de flujo del programa o tablas de lógica detalladas?

SI ( ) NO ( )

8. ¿Se preparan en esta etapa instrucciones operativas (para las pruebas de los programas)?

SI ( ) NO ( )

9. ¿Se realizan revisiones técnicas y operacionales?

SI ( ) NO ( )

10. Las revisiones técnicas incluyen:

( ) Compatibilidad de la lógica del programa

( ) Normas de programación

( ) Procedimientos de recuperación por errores

( ) Aceptabilidad de la técnica de manejo de archivos

( ) Posibilidad de mantener el sistema

11. La revisión operacional incluye:

( ) Aceptación de las características operacionales del sistema

( ) Instrucciones documentadas para correrlo

12. ¿Es el producto final de esta fase de programación un sistema de aplicación completamente programado que el personal de programación considera totalmente operacional?

SI ( ) NO ( )

ANEXO C8

INSTRUMENTO PARA EVALUAR LOS PROCEDIMIENTOS Y ENTRENAMIENTO DEL USUARIO.

1. ¿Son entrenados los usuarios para manejar la conversión, prueba y operación de la nueva aplicación sobre una base continua?

SI ( ) NO ( )

2. ¿Se preparan procedimientos (aun en borrador), para efectos de entrenamiento y referencia continuos?

SI ( ) NO ( )

3. A pesar de poder parecer rutinarias las actividades de procedimientos y entrenamiento del usuario, deben verificarse antes que cualquier aplicación llegue a estar en operación. En la página siguiente se especifica una lista de puntos a verificar:

(califique de 0 a 100 según su criterio la lista de procedimientos y plan de entrenamiento tal y como se hace) _____.

4. El punto 5 y 8 tienen una duración relativamente larga. Evalúe según su criterio de 0 a 100 _____.

5. ¿Se elabora un borrador que concentre el contenido técnico e instruccional de las actividades manuales relacionadas con la aplicación?

SI ( ) NO ( )

6. ¿Se utiliza este borrador como base para el entrenamiento del usuario?

SI ( ) NO ( )

7. ¿Se establece la preparación de los procedimientos finales hasta que el sistema este implantado?

SI ( ) NO ( )

LISTA DE PUNTOS A VERIFICAR PARA LOS PROCEDIMIENTOS Y PLAN DE ENTRENAMIENTO DEL USUARIO

ORGANIZACIÓN:_____
DEPARTAMENTO:_____
SISTEMA:_____
USUARIO RESPONSABLE:_____

PREPARADO POR:_____
REVISADO POR:_____
FECHA:_____

PAG___ DE___
PROYECTO No.___

DESCRIPCIÓN DE LA ACTIVIDAD	PERSONA RESPONSABLE	ORGANIZACIÓN	FECHA DE INICIACIÓN	FECHA DE TERMINACIÓN	APROBADO POR
1. Preparación del usuario					
2. Notificación interna Aviso al ejecutivo Aviso al empleado					
3. Notificación externa Coordinación con el cliente Coordinación con el proveedor Relaciones públicas Otros					
4. Consideraciones de políticas Corporativas Divisionales					
5. Procedimientos Plan del contenido Manuales Publicación y expedición					
6. Descripciones de trabajo					

7. Formas diseño Impresión interna Impresión externa					
8. Entrenamiento y orientación Plan del programa Manual de instrucciones del programa Presentación Otros					
9. Equipo y enseres especiales Determinación de requerimientos Departamento de ingeniería Subcontratistas					
10. Equipo de oficina requerido					
11. Espacio y distribución de piso					
12. Abastecimientos					
13. Personal Reclasificación Contratación					
Aprobado por:_____ Grupo de Sistemas			_____ Encargado del proyecto		

ANEXO C9

INSTRUMENTO PARA EVALUAR LA PRUEBA DEL SISTEMA.

1. ¿Se logra que los usuarios prueben todas las facetas de la aplicación como una unidad?

SI ( ) NO ( )

2. De la siguiente lista. ¿Cuales elementos se incluyen en las pruebas del sistema?

( ) Los programas

( ) La operación del computador

( ) Las actividades del usuario

( ) Las funciones del grupo de control

3. ¿Se considera que las pruebas se efectúen bajo condiciones reales?

SI ( ) NO ( )

4. ¿Las pruebas son dirigidas y desarrolladas por el personal usuario?

SI ( ) NO ( )

5. ¿Los analistas y programadores únicamente participan en la corrección de discrepancias que se descubran?

SI ( ) NO ( )

6. ¿Es el objetivo en la prueba del sistema hacerlo fallar?

SI ( ) NO ( )

7. ¿Se tiene la visión de identificar y corregir tantas deficiencias como sea posible?

SI ( ) NO ( )

8. ¿Es el fin último de esta fase tener la aplicación lista para ser implantada?

SI ( ) NO ( )

9. ¿Se lleva un registro de la actividad de prueba del sistema para todas las tareas efectuadas?

SI ( ) NO ( )

10. ¿Se prepara un reporte de discrepancias durante el proceso de prueba?

SI ( ) NO ( )

11. Pondere según su criterio si se cumple con un reporte de discrepancias, de 0 a 100 comparando con el cuadro de la página siguiente._____.

12. ¿Se lleva acabo una documentación de las aprobaciones para cada prueba efectuada?

SI ( ) NO ( )

REPORTE DE DISCREPANCIAS

NOTA DE CONTROL DE PROBLEMAS/SOLICITUDES

SISTEMA:_____

NUMERO
FECHA DE COMPROMISO_____
TERMINADO?_____

PAG __ DE __

SOLICITUD DE SINTOMA

PRESENTADO POR _____ FECHA _____

PROLEMA/RAZON

DIAGNOSTICADO POR _____ FECHA _____

SOLUCION DISPOSICION

RESUELTO POR _____ FECHA _____

SOLICITUD(ES) DE CAMBIO EMITIDA(S)

No.	PARTIDA QUE DEBE CAMBIARSE	ASIGNADA A	FECHA DE SOLICITUD	FECHA DE TERMINACION

APROBADO POR _____ FECHA _____

ANEXO C10

INSTRUMENTO PARA EVALUAR LA CONVERSIÓN.

1. ¿Los sistemas de conversión existentes son descontinuados?

( ) Repentinamente

( ) Gradualmente

( ) Depende del plan

2. ¿Se logra en esta fase que el sistema esté listo para operar?

SI ( ) NO ( )

3. ¿Se logran los beneficios y el comportamiento de los costos que se predijeron al inicio del proyecto?

SI ( ) NO ( )

4. ¿Se obtiene aprobación (con documentación) de la conversión de los archivos?

SI ( ) NO ( )

5. ¿La aprobación operacional se basa en un número de ciclos operativos previamente establecidos?

SI ( ) NO ( )

7. ¿Las acciones correctivas se programan e implantan como parte del mantenimiento continuo?

SI ( ) NO ( )

ANEXO C11

INSTRUMENTO PARA EVALUAR LA REVISIÓN POSTERIOR A LA IMPLANTACIÓN.

1. ¿Se tiene calendarizada la actividad de revisión posterior a la implantación?

SI ( ) NO ( )

2. ¿El ciclo de actividades para proyectos realiza al menos una revisión formal a la implantación?

SI ( ) NO ( )

3. ¿Están involucradas todas las partes del desarrollo de sistemas en la actividad de revisión?

SI ( ) NO ( )

4. ¿Esta participación está encaminada a obtener lecciones y guías de orientación para mejorar la capacidad de mejorar sistemas?

SI ( ) NO ( )

5. ¿La actividad de revisión está enfocada a una comparación entre los beneficios planeados y los reales del sistema implantado? (hasta que la operación sea normal)

SI ( ) NO ( )

6. ¿En cual de las siguientes categorías cae su actividad de revisión?

( ) El sistema en curso debe revisarse y evaluarse

( ) La estructura y actividades anteriores deberán revisarse y evaluarse, a fin de obtener lecciones que puedan aplicarse a trabajos futuros

7. ¿Se revisan los presupuestos de los departamentos usuarios, que reflejen el impacto de la aplicación en curso?

SI ( ) NO ( )

8. ¿Se revisan datos sobre el costo de operación del departamento de sistemas que se apliquen a la nueva aplicación?

SI ( ) NO ( )

9. ¿La revisión se apoya en la documentación obtenida en la fase de la implantación?

SI ( ) NO ( )

10. ¿Se recopilan los siguientes datos?

( ) Grado de eficiencia del nuevo sistema

( ) Cumplimiento de los calendarios

( ) Tiempo de respuesta en la entrega de los resultados a los usuarios

11. ¿Se comparan los resultados de operación y los beneficios pronosticados por los usuarios durante la actividad de especificaciones del usuario?

SI ( ) NO ( )

12. ¿Se revisan los avisos de discrepancias, los cambios y los registros de errores que se hayan preparado desde que el sistema fue implantado?

SI ( ) NO ( )

13. Al evaluarse la aplicación. ¿Se revisa conjuntamente el trabajo del proyecto (desarrollo de sistemas)?

SI ( ) NO ( )

14. ¿Se hacen comparaciones entre los planes y los resultados en las actividades claves? (planeación de sistemas, especificación del usuario y planeación de la implantación)

SI ( ) NO ( )

15. ¿Se identifican las formas en que puede mejorarse la coordinación para establecer responsabilidades de manera más efectiva?

SI ( ) NO ( )

16. ¿Se evalúa la actuación del personal? (es actividad de los gerentes de línea)

SI ( ) NO ( )

17. ¿Se efectúa evaluación interna técnica del grado de eficiencia de las funciones dentro del departamento de sistemas, por su personal? (otros no tienen la experiencia técnica necesaria para participar en este tipo de estudio especializado)

SI ( ) NO ( )

ANEXO C12

INSTRUMENTO PARA EVALUAR EL MANTENIMIENTO CONTINUO.

1. ¿Se considera que el mantenimiento está limitado a modestas alteraciones (de lo contrario es un proyecto de desarrollo)?

SI ( ) NO ( )

2. ¿Se considera que los proyectos de mantenimiento lleguen a un 20 % como máximo de los esfuerzos de desarrollo?

SI ( ) NO ( )

3. ¿Se refleja el hecho de que cada vez que la estructura operacional se modifica existe un riesgo de que surjan errores y problemas de control?

SI ( ) NO ( ).

4. ¿Los controles que se aplican sobre cada cambio proporcionan la seguridad de que las modificaciones no han resultado en un deterioro de la calidad de las aplicaciones?

SI ( ) NO ( )

5. Un proyecto de desarrollo tiene énfasis en un nivel administrativo, con objetivos primordialmente económicos. En un proyecto de mantenimiento. ¿Se considera que son técnicas de investigación y selección más estrictas y más técnicas para la aprobación y control de los cambios?

SI ( ) NO ( )

6. Los requerimientos de mantenimiento (suponiendo que no son urgentes). ¿Se acumulan? (al manejar en lote todos los requerimientos de cambios, las medidas de control serán mas efectivas si se hiciesen en forma individual)

SI ( ) NO ( )

7. ¿Se establecen normas mínimas de documentación?

SI ( ) NO ( )

8. ¿Se lleva un registro de cambios a los programas establecido para cada programa dentro de cada aplicación, que incluya alguna indicación de que cambios se han hecho, cuando, porque y por quién?

SI ( ) NO ( )

9. ¿Cada vez que se modifica un programa se genera nueva documentación?

SI ( ) NO ( )

10. ¿Esta documentación incluye?

( ) lista completa de los programas fuente y objeto

( ) Especificaciones técnicas para la codificación

( ) Documentación para cualquier regla de decisión que se haya modificado

11. ¿Todos los cambios se acompañan por aprobaciones técnicas y del usuario documentadas?

SI ( ) NO ( )

EVALUACIÓN DEL ANEXO C

Este instrumento consta de 12 cuestionarios y como la mayoría de instrumentos, debe evaluarse en forma secuencial para no perder la objetividad de la auditoría.

Cada pregunta y cuadro tienen un valor que es cuantificable, positivo.

Hay casos en que algunas preguntas no tienen valor medible; estas preguntas solo sirven para información de apoyo al dictamen que se realizará, por lo que no se toman en cuentan como valor (están marcadas con *).

Cada cuestionario tiene un valor numérico según la siguiente tabla:

Compromiso progresivo	300
Pasos en el proceso de desarrollo	600
Planeación de sistemas	1600
Especificaciones del usuario	4400
Especificaciones técnicas	2300
Planeación de la implantación	2100
Programación	1700
Procedimientos y entrenamiento del usuario	700
Prueba del sistema	1500
Conversión	800

Revisión posterior a la implantación	2000
Mantenimiento continuo	1300

El valor de cada cuestionario será comparado con la sumatoria de sus preguntas contestadas. De esto se obtendrá un porcentaje que en ningún momento será un dictamen de la auditoria, sino un valor con el que el auditor y su equipo harán el dictamen

En algunos casos habrán preguntas que no competen al sistema objeto de evaluación, en ese caso se eliminará la pregunta, y su valor (100 por cada opción que tenga la pregunta) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas dan un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellos deberá ser parte de un documento para una evaluación posterior.

ANEXO D

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE ADMINISTRACIÓN DE DATOS.

1. ¿Está definida formalmente la función del administrador de datos?

SI ( ) NO ( )

2. ¿Está formalmente definida la función del administrador de la base de datos?

SI ( ) NO ( )

3. ¿Existen controles sobre la definición de la base de datos? (busca correspondencia entre la base de datos y su definición)

SI ( ) NO ( )

4. ¿Existe control sobre la recuperación de los datos? (establece un mecanismo para recuperar la información en caso de fallas, pérdida o daño de la información)

SI ( ) NO ( )

5. ¿Existe control de acceso? (previene el riesgo del ingreso no autorizado a la utilización y/o modificación de la información contenida en la base de datos)

SI ( ) NO ( )

6. ¿Existen controles de concurrencia? (evitan los problemas de integridad que pueden ocurrir al permitir el acceso a la misma información por dos procesos al mismo tiempo. Muchos paquetes administradores de bases de datos proveen solución parcial para este problema, por lo que es necesaria alguna intervención adicional)

SI ( ) NO ( )

7. ¿Existe definido un control de calidad? (asegura la exactitud y consistencia de la información incorporada a la base de datos)

SI ( ) NO ( )

8. ¿Existen controles sobre la actualización? (restringen la adición y/o actualización de la base de datos en forma exclusiva a los usuarios autorizados)

SI ( ) NO ( )

9. En caso de que los controles no sean automatizados, es decir que no son provistos por la base de datos, ¿Se establecen políticas?

SI ( ) NO ( )

10. ¿Se determina la efectividad del cumplimiento del DA/DBA?

SI ( ) NO ( )

11. ¿Existe un control para evitar riesgos de fraude o pérdida de información de la base de datos en forma accidental o por atentados a la información perpetrados por el DA/DBA, haciendo un mal uso de sus capacidades y conocimientos?

SI ( ) NO ( )

12. Para el DA/DBA existe:

( ) Separación de responsabilidades

( ) Rotación de personal

( ) Capacitación en el desarrollo de sus funciones

( ) Registro de sus actividades en la base de datos en bitácoras (log) que generalmente son provistos por el administrador de la base de datos.

EVALUACIÓN DEL ANEXO D

El cuestionario de este instrumento se evaluará de la siguiente manera: Todas las preguntas tienen un valor que es cuantificable, el cuestionario en sí, tiene un valor numérico de 1500, el cual será comparado con la sumatoria de todas sus preguntas contestadas. Esto dará como resultado un porcentaje que en ningún momento será el resultado de la auditoria, sino el valor con el que el auditor y su equipo harán el dictamen.

En algunos casos habrán preguntas que no competan a este subsistema, en ese caso se eliminará la pregunta, y su valor (100 por cada opción de la pregunta) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas dan un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellos deberá ser parte de un documento para una evaluación posterior.

ANEXO E

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE ADMINISTRACIÓN DE LA SEGURIDAD.

ANEXO E1

INSTRUMENTO PARA EVALUAR LA SEGURIDAD FÍSICA.

1.- El nivel de temperatura adecuado, cuando el equipo se encuentra en operación, es entre 10 y 40 grados centigrados.

2.- El medio ambiente donde está ubicado el equipo debe estar limpio y libre de polvo, humo y motas de tapetes.

El computador no debe estar colocado a nivel del suelo ya que es más factible que los lectores de discos (drive) se llenen de polvo o de motas de tapete.

3.- La distancia mínima requerida entre un equipo y otros similares, aparatos eléctricos, radio transmisores, teléfonos o ascensores deben ser de 1.5 Mts., para evitar el efecto de los campos magnéticos generados por estos equipos.

4.- El equipo debe estar colocado sobre una superficie resistente, y deben existir al menos diez cms. libres al rededor del equipo.

5.- Observar que los microcomputadores ubicados en áreas abiertas estén adecuadamente protegidos contra daños accidentales o pérdida, tanto de los equipos como de sus partes; usando muebles diseñados especialmente para ellos; ubicandolos en áreas en dónde la circulación de personas no sea muy continua; asegurando sus partes para evitar robos de estas, y, si los equipos se encuentran ubicados en áreas cerradas, verificar que se cierre el área en horas no hábiles.

6.- Observar que las conexiones eléctricas estén protegidas, aseguradas contra la pared, que los cables se encuentren dentro de ductos y no dispersos en el suelo, de manera que se eviten desconexiones accidentales de los equipos; y, verificar que los tomacorrientes no estén sin sus correspondientes tapas que minimizan los riesgos de corto.

7.- Dependiendo de la concentración de los equipos en una misma área, observar si existen detectores de humo, y suficientes extinguidores de gas *halón* debidamente cargados, con el propósito de que cualquier incendio sea detectado y sofocado oportunamente.

8.- Observar que las personas que operan los equipos no coloquen sobre las rendijas de ventilación de los

microcomputadores, papeles, libros, documentos o cualquier otro elemento que obstruya la ventilación de los mismos.

9.- Verificar que, el área donde están ubicados los microcomputadores, no se fume ni se consuman alimentos ni bebidas, pues las partículas que estos causas pueden producir daños a los equipos.

10.- Verificar que los equipos se protejan del polvo mediante forros.

11.- Verificar que se desconecten cuando no estén en uso.

12.- Verificar que el área física donde se encuentran ubicados los equipos, esté conformada principalmente por elementos anti-inflamables.

13.- Verificar si cada área donde existen micros hay un funcionario encargado de administrarlos, velar por su seguridad y controlar sus recursos.

Entre sus funciones estará:

* Verificar y controlar el mantenimiento de los micros.

* Controlar que los usuarios tengan acceso a los recursos que necesitan para su trabajo.

* Controlar que existan los recursos necesarios.

* Controlar que únicamente las personas autorizadas den mantenimiento a los equipos.

* Controlar los paquetes y manuales de los equipos.

* Controlar que solo el personal autorizado maneje los equipos.

* Definir y controlar los horarios de utilización de los micros, para que todos los usuarios autorizados puedan usarlos.

* Comunicarse con el centro de información para actualizar versiones de paquetes.

* Controlar los procedimientos de limpieza regular de los micros.

14.- Verificar si existe un contrato de mantenimiento preventivo y correctivo para mantener en condiciones de buen funcionamiento los micros.

15.- Verificar si se controla el cumplimiento de dichos contratos y las cláusulas de garantía de los equipos.

16.- Verificar si se tiene un registro de los problemas en los equipos, mantenimientos efectuados, soluciones, cambios de elementos, etc.

17.- Verificar si existen procedimientos alternos, tales como soporte con equipos de otros departamentos de la empresa, para realizar las operaciones criticas, en caso de falla del equipo.

ANEXO E2

INSTRUMENTO PARA EVALUAR LA SEGURIDAD A LOS ARCHIVOS Y PROGRAMAS.

1. Verificar que los funcionarios usuarios de las micros hayan recibido un entrenamiento adecuado en el manejo de ellas, sistema operativo y uso de los diferentes paquetes (procesadores de palabras, hojas electrónicas, bases de datos, etc.) con el propósito de reducir los riesgos de pérdidas de información accidental por el mal manejo de los elementos, comandos, etc.

2. Verificar que en el área de microcomputadores existen manuales actualizados del sistema operativo y de los paquetes y programas de aplicación.

3. Verificar que los diskettes estén marcados para facilitar su identificación, y que los rótulos sean marcados antes de colocarlos en el diskette.

4. Observar que en el manejo de los diskettes se tengan los siguientes cuidados:

* Se guarden en los sobres protectores.
* Se archiven en posición vertical.
* Que el microcomputador ni se encienda ni se apague con los diskettes dentro de los drives.
* Que los diskettes no se coloquen cerca de los teléfonos.
* Que no se toque la superficie del diskette.
* Que los diskettes no se doblen.
* Que no se sujeten con clips.
* Que se almacenen en lugares frescos donde no reciba la luz directa del sol.

5. Verificar que existen copias de todos los archivos. De aquellos que contengan información crítica, cuya recuperación en caso de pérdida es muy costosa o poco probable, examinar si existe otra copia almacenada en un lugar diferente al área de los micros, y que permita su recuperación en caso de requerirse.

6. Verificar que en los discos duros no residen archivos ni programas de usuarios. El disco debe usarse para el sistema operacional, compiladores, paquetes y en general programas de uso común para todos los usuarios únicamente. Los programas deben grabarse en versión objeto o compilados, no en lenguaje fuente. (recomendación de IBM).

El apoyo necesario para evaluar está fundado en los criterios anteriormente descritos, la metodología para evaluar se basa en formularios y cuestionarios que poseen cierta ponderación y que al final se obtendrá una media.

Por lo tanto se evaluará de la siguiente manera:

A. Seguridad física que afecta a la instalación.

El objetivo de este subsistema es evaluar la seguridad física del equipo en lo que concierne a su adecuada instalación y funcionamiento, de tal forma que permitan un funcionamiento continuo.

En primera instancia realice una observación visual en base al siguiente formulario:

EMPRESA:	GERENTE:	
CÓDIGO:PR04-FM01	OBJETIVO: Evaluar la Seguridad Física.	
EVALUADO POR:	FECHA:	HORA:
INSTRUCCIONES: Coloque las observaciones pertinentes con respecto a cada elemento del equipo. Al final de las observaciones estime una ponderación del (0 - 100).		

EQUIPO	Aire acondicionado
GRADO DE LIMPIEZA: A. MUY LIMPIO B. POCO LIMPIO C. MUY SUCIO	
NIVEL DE POLVO	
OBSERVACIONES	
PONDERACIÓN (0 - 100)	

EQUIPO	Extintores de incendio
LIBRE ACCESO AL EQUIPO	
UBICACIÓN ESTRATÉGICA	
SEÑALIZACIÓN ADECUADA	
CONOCIMIENTOS DEL PERSONAL EN RELACIÓN AL MANEJO DEL EQUIPO	
FECHA DE CARGA DEL MATERIAL EXTINGUIDOR	
PONDERACIÓN (0 - 100)	

CARACTERÍSTICAS FÍSICAS	Mueblería del equipo del computador
MATERIAL	
DISTANCIA ENTRE EQUIPOS	
EXISTENCIA DE COBERTORES	
UBICACIÓN DEL CENTRO	
PONDERACIÓN (0 - 100)	

CARACTERÍSTICAS GENERALES	Sistema eléctrico
PROTECCIÓN DE CONEXIONES	
UNIDAS A LA PARED	
EXISTENCIA DE DUCTOS	
TOMACORRIENTES (SATURADOS)	
PONDERACIÓN	

Para lograr una evaluación completa es necesario responder al cuestionario siguiente: (Por favor estime la ponderación en base a los criterios y los límites que aparecen al lado de la pregunta)

1.- ¿Existe una persona responsable de la seguridad? (0-25)

2.- ¿Existe un plan de seguridad? (0-20)

3.- ¿El edificio donde se encuentra la computadora está situado a salvo de :

a) inundación ?

b) terremoto ?

c) fuego ?

d) sabotaje ?

e) sonido ? (0-20)

4.- Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que fue construido.

5.- ¿Cuantas salidas de seguridad existen?(0-10)

6.- ¿Existe control en el acceso a este cuarto

a) Por identificación personal?

b) Por tarjeta magnética?

c) Por claves verbales?

d) Otras? (0-10)

7.- ¿Se registra el acceso al cuarto de personas ajenas a la dirección de informática? (0-5)

8.- ¿Existe alarma para

a) Detectar fuego (calor o humo)en forma automática?

b) Avisar en forma manual la presencia del fuego?

c) Detectar una fuga de agua?

d) Detectar magnetos?

e) No existe (0-5)

9.- ¿Existen puertas y vías de acceso en caso de emergencia? (0-5)

El segundo cuestionario evalúa aspectos administrativos de aspectos lógicos y físicos:

1.- ¿Existe un funcionario que administre la función de este rubro? (0-15)

2.- ¿Existe un contrato de mantenimiento preventivo y correctivo? (0-10)

3.- ¿Se le da cumplimiento al contrato? (0-10)

4.- ¿Existen archivos de problemas, soluciones, correcciones, etc? (0-5)

5.- ¿Existen procedimientos alternos en caso de falla del equipo? (0-10)

6.- En relación al entrenamiento del personal que maneja el software:¿es satisfactorio? (0-10)

7.- ¿Existen manuales del software? Revisar que sean explícitos en el manejo de la seguridad de ellos. (0_5)

8.- ¿Todos los medios de grabación están rotulados? (0-5)

9.- ¿Se desarrolla el manejo de los diskettes acorde a lo descrito anteriormente?(0-5)

10.- ¿Existen copias de respaldo de la información más importante? (0-15)

11.- ¿Existen archivos no autorizados de los usuarios en los discos duros? (0-10)

ANEXO E3

INSTRUMENTO PARA EXAMINAR EL PLAN DE CONTINGENCIA.

El instrumento para evaluar los planes es una matriz que contiene en las ordenadas la clasificación de los desastres existentes y en las abscisas contiene todos los elementos necesarios para su eficiente funcionamiento.

El gráfico interrelaciona los desastres y los elementos mínimos del plan por medio de una intersección que se logra mediante la unión de los puntos de las abscisas con los de las ordenadas. Así pues la información de la parte superior es:

a) Completa destrucción del centro de cómputo (E1).
b) Destrucción parcial del centro de cómputo (E2).
c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire acondicionado, etc.) (E3).
d) Destrucción parcial o total de los equipos centralizados (E4).
e) Pérdida total o parcial de información, manuales o documentación (E5).
f) Pérdida del personal clave (E6).
g) Huelga o problemas laborales (E7).

El plan en caso de desastre debe incluir:

1.- La documentación de programación y de operación (P1).

2.- El equipo completo (P2).

3.- Datos y archivos (P3).

4.- Papelería y equipo accesorio (P4).

5.- Sistemas (sistemas operativos, bases de datos, programas de utilería, programas) (P5).

El gráfico está diseñado de la manera siguiente:

En las ordenas de la matriz contiene los posibles desastres contemplados para un centro de procesamiento de datos. En las abscisas contienen todos los elementos que un plan de contingencia debe poseer. En el interior de cada cuadro se encuentran 4 letras (A, B, C, D) que deben ser marcadas y que representan la evaluación de la interrelación. En la parte inferior de la hoja aparece el valor y significado de cada letra.

MATRIZ PARA EVALUAR

	P1	P2	P3	P4	P5
E1	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D
E2	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D
E3	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D
E4	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D
E5	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D
E6	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D
E7	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D	A-B-C-D

SIGNIFICADO	LETRA	VALOR
PROFUNDO Y COMPLETO	A	100 - 80
SATISFACTORIO	B	79 - 50
INCOMPLETO	C	49 - 30
INEXISTENTE	D	29 - 0

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no puede ser utilizado.

La evaluación del procedimiento en caso de que el plan sea requerido debido a una emergencia se basa en la observación de las siguientes fases:

i. Asegurar que todos los miembros sean notificados.

ii. Informar al director de informática.

iii. Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que parte del plan debe ser activada.

iv. Determinar el estado de todos los sistemas en proceso.

v. Notificar a los proveedores del equipo cuál fue el daño.

vi. Establecer la estrategia para llevar a cabo las operaciones de emergencia tomando en cuenta:

a) Elaboración de una lista con los métodos disponibles par realizar la recuperación.

b) Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustitución de procesos en línea por procesos en lote).

c) Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.

ANEXO F

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE ADMINISTRACIÓN DE OPERACIONES.

1. ¿Existen funciones claramente descritas que los operadores del computador deban realizar?

SI ( ) NO ( )

2. ¿Existen procedimientos que describan la forma en que el equipo; programas y datos deban ser manipulados?

SI ( ) NO ( )

3. ¿Existen procedimientos que describan la forma en que el equipo debe ser mantenido?

SI ( ) NO ( )

4. ¿Existen procedimientos que establecen la forma en que debe realizarse la operación de la red de comunicaciones?

SI ( ) NO ( )

5. ¿La operación de la red de comunicaciones está bajo la tutela de operadores experimentados?

SI ( ) NO ( )

6. ¿Existen funciones sobre la preparación de los lotes de datos que serán digitados, así como la digitación y verificación de los datos? (especialmente para los sistemas que funcionan con actualizaciones por lotes)

SI ( ) NO ( )

7. ¿Existe alguna área que controle el flujo de información del procesamiento de datos?

SI ( ) NO ( )

nota:	Al crear una sección para llevar a cabo este control, se vuelve más difícil que los operadores del computados o el personal de preparación de datos puedan modificar la información, ya sea por error involuntario o fraude.

8. ¿Se verifica que los archivos se utilizan para propósitos autorizados?

SI ( ) NO ( )

9. ¿Se mantienen en perfecto estado de funcionamiento los medios de almacenamiento de archivos?

SI ( ) NO ( )

10. ¿Existen estrategias para administrar copias de respaldo y retención de archivos?

SI ( ) NO ( )

11. ¿Existen manuales y documentos para?

( ) Documentación de las aplicaciones

( ) Documentación de los programas

( ) Manuales de operación de las aplicaciones

( ) Manuales del usuario

( ) Manuales de estándares

( ) Manuales de referencia de los programas de soporte al sistema

( ) Manuales de referencia del equipo

12. ¿Se asegura que la documentación esté almacenada correctamente?

SI ( ) NO ( )

13. ¿Se verifica que el préstamo de los documentos sea a las personas autorizadas para ello?

SI ( ) NO ( )

14. ¿Se mantienen suficientes copias de la documentación?

SI ( ) NO ( )

15. ¿Se tiene un registro de las personas que han tenido acceso a la información? (una bitácora instalada para tal propósito)

SI ( ) NO ( )

16. ¿Se solicita la autorización correspondiente al acceso a dicha documentación?

SI ( ) NO ( )

17. ¿Se monitorea el rendimiento de los equipos y programas? (el objetivo es determinar si las aplicaciones se están procesando eficientemente)

SI ( ) NO ( )

18. ¿Se evalúa el cumplimiento de las metas de los usuarios?

SI ( ) NO ( )

19. ¿Se evalúa el costo de los servicios a los usuarios?

SI ( ) NO ( )

EVALUACIÓN DEL ANEXO F

Para el cuestionario de este instrumento se evaluará de la siguiente manera: Todas las preguntas tienen un valor que es cuantificable Positivo.

El cuestionario en sí, tiene un valor numérico de 1500, el cual será comparado con la sumatoria de todas sus preguntas contestadas. Esto dará como resultado un porcentaje que en ningún momento será el resultado de la auditoría, sino el valor con el que el auditor y su equipo harán el dictamen.

En algunos casos habrán preguntas que no competan a este subsistema, en ese caso se eliminará la pregunta, y su valor máximo positivo (100 por cada opción de la pregunta) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas dan un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellas deberá ser parte de un documento para una evaluación posterior.

ANEXO G

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE SOPORTE TÉCNICO.

1. ¿Se desarrollan programas y procesos utilitarios que soporten al sistema?

SI ( ) NO ( )

2. ¿Se da mantenimiento a esos programas y procesos?

SI ( ) NO ( )

3. Existe un responsable de los posibles problemas que se encuentren en relación a:

( ) Sistema operativo

( ) Funcionamiento de la red de comunicaciones

( ) Herramientas de desarrollo de sistemas

( ) Paquete administrador de la base de datos

( ) Otros

4. ¿Existe una bitácora de las personas que trabajan en este subsistema? (por el amplio acceso que estas tienen sobre las instalaciones)

SI ( ) NO ( )

5. ¿Se restringen las acciones que estas personas a las responsabilidades especificas que están desarrollando en un momento determinado?

SI ( ) NO ( )

nota:	En instalaciones pequeñas, es probable que no se encuentre personal destacado en forma exclusiva para el área de soporte al técnico, y que estas funciones sean desarrolladas por los analistas/programadores de sistemas, e incluso, por los operadores del computador.

EVALUACIÓN DEL ANEXO G

Para el cuestionario de este instrumento se evaluará de la siguiente manera: Todas las preguntas tienen un valor que es cuantificable Positivo. El cuestionario en sí, tiene un valor numérico de 900, el cual será comparado con la sumatoria de todas sus preguntas contestadas. Esto dará como resultado un porcentaje que en ningún momento será el resultado de la auditoria, sino el valor con el que el auditor y su equipo harán el dictamen.

En algunos casos habrán preguntas que no competan a este subsistema, en ese caso se eliminará la pregunta, y su valor máximo positivo (100 por cada opción de la pregunta) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas dan un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellos deberá ser parte de un documento para una evaluación posterior.

ANEXO H

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE ACCESOS.

METODOLOGÍA PARA AUDITAR EL SISTEMA DE ACCESO
1) Determinar si existen controles para detectar accesos no autorizados.
2) Revisar el plan maestro de seguridad para determinar si los sistemas de control son adecuados y completos.
3) Examinar los resultados de las pruebas hechas a los sistemas de control de la seguridad de el acceso al sistema, y examinar la posición gerencial en torno a estos resultados.
4) Visitar las instalaciones de las computadoras, verificando allí las operaciones de acceso al sistema y la ubicación física de los elementos de hardware, así como inspeccionar si la edificación es adecuada.
5) Visitar la biblioteca de archivos para determinar si los procedimientos que allí se usan, en verdad restringen el acceso a los datos, programas y a la documentación, ya que esta es otra forma de accesar indirectamente el sistema informático.

6) Visitar las instalaciones de las terminales de la computadora y verificar si el acceso al sistema informático está realmente restringido.

7) Revisar el esquema de autorizaciones para determinar si las autorizaciones que ganan acceso al sistema son consistentes con la segregación de tareas, y si se proporciona confidencialidad a los datos mas sensibles.

8) Revisar los métodos de identificación de los usuarios autorizados, para determinar si exclusivamente usuarios autorizados están en capacidad de usar el sistema para propósitos autorizados.

9) Rastrear algunas claves de acceso, que tomen parte de la tabla de autorización y determinar si la implementación de la tabla está correcta (hacer muestreo)

10) Revisar los métodos a través de los cuales se hace efectivo el acceso en la comunicación de los datos, y diagnosticar si las intromisiones son sólo una posibilidad remota. Revisar las conclusiones de ellos acerca de lo adecuado que con esos controles.

11) Revisar los informes de la auditoría interna acerca de la seguridad que ofrece el sistema de accesos al sistema informático. Revisar las conclusiones de ellos acerca de lo adecuado que son esos controles

12) Revisar el diagnóstico que la compañía aseguradora, ha hecho en torno al sistema de seguridad en el acceso de la información del sistema informático.

13) Revisar las memorias de auditorías anteriores y las medidas que la organización ha tomado.

14) Evaluar la administración de las llaves del sistema informático.

15) Verificar que sus usuarios del sistema mantienen la confidencialidad de las llaves.

16) Verificar que las llaves de usuarios se encuentran a salvo dentro de la base de datos. Esto se puede realizar a través de algún cifrado o encriptamiento de las llaves.

17) Debe verificar la capacidad de la base de datos, en cuanto a la capacidad de recuperación ante fallas.

18) Evalúe si se realizan bitácoras de accesos y pistas de auditoría, para poder determinar posibles debilidades en los controles, el consumo de recursos asociado al mecanismo de acceso.

EVALUACIÓN DE RESULTADOS

La evaluación de este subsistema estará sujeta en el juicio crítico de el grupo de auditoría de sistemas y respaldado por sus respectivos papeles de trabajo.

La metodología de evaluación es la siguiente:

a) Someta a evaluación objetiva todos y cada uno de los apartados de los dieciocho numerales desarrollados en este anexo H.

b) Califique con una nota de 0 (cero) a 100 (cien) puntos cada uno de los dieciocho aspectos.

c) Sume todos los puntos ganados por cada numeral.

d) Si se omitiera alguna de los dieciocho aspectos la metodología, entonces califíquela con 0 puntos. Justifique su calificación con los papeles de trabajo.

e) Realice un promedio de todos los puntos.

f) Realice sus recomendaciones.

RESULTADOS:

0	-	33.33	PUNTOS:	NECESITA MEJORAR.
33.33-		66.66	PUNTOS:	BUENO, PERO DEBE MEJORAR.
66.66-		100	PUNTOS:	MUY BUENO, PERO PUEDE MEJORAR.

ANEXO I

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE ENTRADA.

-PARA LA DIRECCIÓN-

1. ¿Existe responsabilidad de los datos (por ejemplo compartida por alguna función de la organización y la de procesamiento de datos)? SI ( ) NO ( )

¿Qué funciones?_____

2. ¿Se ha considerado algún procedimiento en caso de encontrarse en el caso de duplicidad de datos?

SI ( ) NO ( )

3.¿Se determinan los usuarios o propietarios posibles?

SI ( ) NO ( )

4. ¿Se determina al responsable de su actualización y consistencia? SI ( ) NO ( )

5. En el caso que los usuarios son los que se encargan de la captura y modificación de la información ¿Se ha determinado que usuario es responsable de cada uno de los datos que ingresan?

SI ( ) NO ( )

6.¿Existe un responsable del subsistema de entrada de cada uno de los datos ingresados al sistema?

SI ( ) NO ( )

7. ¿La generación de alguna transacción es generada por el personal del sistema informático?

SI ( ) NO ( )

8. ¿Se especifica por escrito la preparación de los documentos fuente? SI ( ) NO ( )

9. De un documento fuente para la entrada de datos ¿Se registra la siguiente información?

* Origen del documento ( )
* Autorización ( )
* Preparación de datos (responsable) ( )
* Responsable de retener documento ( )
* Responsable de manipular errores ( )

10. ¿Existe una numeración consecutiva de los documentos fuente?

SI ( ) NO ( )

EVALUACIÓN PARA LOS DATOS DE ENTRADA DIRECTA (EN LÍNEA)

1. ¿Que porcentaje de datos se hacen en forma directa (es decir que los datos se registran de inmediato en el instante en que ocurran)? _____ %

2. ¿Se registran las transacciones efectuadas en las entradas directas?

SI ( ) NO ( )

¿Cómo?

* En forma automática ( )
* Algún tipo de comprobante ( )
* Otro ( )

3. ¿Son verificadas al momento de su captura?

SI ( ) NO ( )

4. ¿Se tiene un registro de los posibles errores que pueden existir?

SI ( ) NO ( )

5. ¿Se tiene un registro de los errores encontrados?

SI ( ) NO ( )

6. De tenerse este tipo de registros, ¿En que forma se registran?

* Por período de tiempo ( )
* Por tipo de error ( )
* Por función de la organización ( )
* Por persona responsable ( )
* Otro

EVALUACIÓN A LA CODIFICACIÓN

1. En la codificación de los datos, ¿Se identifica en forma única una entidad o evento?

SI ( ) NO ( )

¿Cómo? _____ _____

EVALUACIÓN DE LOS DOCUMENTOS FUENTE

1. ¿Se revisan los datos contenidos en los formularios que se usarán como documentos fuente?

SI ( ) NO ( )

2. De esos formularios, ¿Se crean lotes, identifican y forman totales de control?

SI ( ) NO ( )

CONTROL SOBRE EL INGRESO Y VALIDACIÓN

1. ¿Existe alguna manera de determinar si todos los datos fueron incorporados al sistema?

SI ( ) NO ( )

¿Cómo? _____

2. ¿Existe algún procedimiento para corregir el ingreso de datos si se llegan a encontrar errores?

SI ( ) NO ( )

3. ¿Qué aspectos se consideran en la validación de los datos?

¿se chequean:

* Caracteres en forma individual ( )?
* Campos individualmente ( )?
* Registros o transacciones completas ( )?
* Controles totales de registros ( )?

CONTROL DE RECUPERACIÓN EN CASO DE FALLAS

1. ¿Se han considerado copias de las transacciones de entrada en caso de fallas?

SI ( ) NO ( )

2. ¿Es posible recuperar el estado de la base de datos al momento en que ocurrió la falla?

SI ( ) NO ( )

3. ¿Existe una copia de los formularios fuente en los que se originaron las transacciones de entrada?

SI ( ) NO ( )

PISTAS DE AUDITORIA

1.¿Se registra la cronología de eventos desde la captura de información (datos e instrucciones), validación, corrección (si fuese necesario) e ingreso al sistema?

SI ( ) NO ( )

Explique:_____ _____

2. De responder afirmativamente a la pregunta anterior. ¿Se obtiene la siguiente información?

* Origen ( )
* Elaboración ( )
* Autorización ( )
* Digitación (encargado) ( )
* Fechas de los diferentes eventos en el proceso de entrada ( )
* Tiempo de digitación ( )

* Número de errores ( )
* Tipo de errores ( )
* Tiempo requerido para corregir los errores ( )
* Recursos consumidos ( )

3. ¿Existen controles para los siguientes aspectos del sistema de entrada?

* Controles manuales ( )
* Controles incorporados en el diccionario y/o la base de datos ( )
* Controles insertados en programas de ingreso ( )
* Validación de datos ( )
* Otro ( )

Especifique:_____ _____

CONTROL DE LOS DATOS Y MANEJO DE CIFRAS DE CONTROL

1. ¿Existen normas que definan el contenido de los instructivos de entrada de datos?

SI ( ) NO ( )

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

* Número de folio ( )
* Fecha y hora de recepción ( )
* Nombre del documento ( )
* Volumen aproximado de registros ( )
* Número aproximado de registros ( )
* Clave del capturista ( )
* Fecha estimada de entrega ( )
* Nombre, Dpto., usuario ( )
* Nombre responsable ( )
* Fecha y hora de entrega de documentos y registros captados ( )

3. Indique cuales controles internos existen en el sistema de entrada de datos:

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

4. ¿Existe un programa de trabajo de entrada de datos?

a) ¿Se elabora este programa de trabajo para cada turno?

* Diariamente ( )
* Semanalmente ( )
* Mensualmente ( )

b) La elaboración del programa de trabajo se hace:

* Internamente ( )
* Se les señalan a los usuarios las prioridades ( )
* Se les señala a los usuarios la posible fecha de entrega ( )

c) ¿El programa de trabajo es congruente con el calendario de producción?

SI ( ) NO ( )

d) Indique el contenido del programa de trabajo de entrada

* Nombre del usuario ( )
* Clave de trabajo ( )
* Fecha programada ( )
* Recepción ( )
* Hora programada de recepción ( )

* Volumen estimado de registros por trabajo ( )
* Fecha programada de entrega ( )
* Hora programada de entrega ( )

e) ¿Qué acciones se toman si el trabajo programado no se recibe a tiempo?

_____

_____

5. Cuando la capacidad de trabajo supera la capacidad instalada se requiere:

* Tiempo extra ( )
* Se subcontrata ( )

6. ¿Qué documentos de entrada se tienen?

SISTEMAS	DOCUMENTOS	DPTO. QUE PROPORCIONA EL DOCUMENTO	PERIODICIDAD	OBSERVACIONES

Pondere según su criterio de 0 a 100 _____.

7.¿Se revisan las cifras de control antes de enviarlas al sistema de entrada?

SI ( ) NO ( )

8. ¿Para aquellos procesos que no traigan cifras de control se han establecido criterios a fin de asegurar que la información es completa y válida?

SI ( ) NO ( )

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

SI ( ) NO ( )

10. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se guarda?_____

Pondere según su criterio de 0 a 100 _____.

11. ¿Existe un procedimiento de anomalías en la información debido a mala codificación?

SI ( ) NO ( )

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

SI ( ) NO ( )

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

SI ( ) NO ( )

14. ¿Se controlan adecuadamente los documentos confidenciales?

SI ( ) NO ( )

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

SI ( ) NO ( )

16. ¿Existe un registro de los documentos que entran a captura? SI ( ) NO ( )

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

SI ( ) NO ( )

18. ¿Quién revisa este control? _____

Pondere según su criterio de 0 a 100 _____.

EVALUACIÓN DEL ANEXO I

Este instrumento consta de 8 cuestionarios y su forma de evaluación puede hacerse de dos maneras diferentes.

La manera de evaluarlo dependerá del auditor y su equipo de trabajo, pues la mejor manera lo determinará la particularidad del sistema y las condiciones propias de la auditoría.

Las dos maneras son:

a) Hacer una evaluación individual de cada cuestionario independientemente; y

b) Hacer una evaluación de todo el instrumento en general.

(Aunque una combinación de ambos, sea una buena opción a tomar)

Cada pregunta y cuadro tienen un valor que es cuantificable: positivo (100) y en un caso particular (Preg. 4e de control de datos... y Preg. 1 de entrada directa) serán solamente información de apoyo al dictamen que se realizará.

Cada cuestionario tiene un valor numérico según la siguiente tabla:

Dirección del sistema	1400
Evaluación de datos de entrada directa	1000
Evaluación de la codificación	100
Evaluación de los documentos fuente	200
Evaluación al ingreso y validación	600
Control de recuperación de datos	300
Pistas de auditoria	1600
Control de los datos y cifras de control	5500

Si se decide evaluar todo el instrumento su valor es de 10700.

El valor de cada cuestionario (o el instrumento total) será comparado con la sumatoria de todas sus preguntas contestadas. Esto dará como resultado un porcentaje que en ningún momento será un dictamen de la auditoría, sino un valor con el que el auditor y su equipo harán el dictamen.

En algunos casos habrán preguntas que no competan a este subsistema, en ese caso se eliminará la pregunta, y su valor (100 por cada opción) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas dan un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellas deberá ser parte de un documento para una evaluación posterior.

ANEXO J

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE PROCESO.

ANEXO J1

INSTRUMENTO PARA EVALUAR EL CONTROL DE OPERACIONES.

1.¿Existen procedimientos formales para la operación del sistema?

SI ( ) NO ( )

2. Esos procedimientos describen detalladamente tanto la organización del centro de procesamiento de datos como la operación del sistema?

SI ( ) NO ( )

3. ¿Están actualizados los procedimientos?

SI ( ) NO ( )

4. Indique la periodicidad de la actualización de los procedimientos:

en caso de falla del equipo ( )

Puntos de reinicio, procedimientos de recuperación para proceso de gran duración o criterios ( )

Identificación de todos los dispositivos de la máquina a ser usados ( )

Especificaciones de resultados (cifras de control, registros de salida por archivo, etc.) ( )

7. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?

SI ( ) NO ( )

8. ¿Son suficientemente claras para los operadores estas órdenes?

SI ( ) NO ( )

9.¿Existe una estandarización de las ordenes de proceso?

SI ( ) NO ( )

10.¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que están trabajando están autorizados y tengan una razón de ser procesados).

SI ( ) NO ( )

11. ¿Como programan los operadores los trabajos dentro del centro de procesamiento?

Primero que entra, primero que sale ( )

Se respetan las prioridades ( )

Otra (especifique) ( )

12. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?

SI ( ) NO ( )

13. ¿Quién revisa este reporte en su caso?_____

Pondere según su criterio de 0 a 100 _____.

14. ¿Controlan los operadores las versiones correctas y se identifican las que son de prueba?

SI ( ) NO ( )

15. Analice la eficiencia con que se ejecutan los trabajos en el centro de procesamiento, tomando en cuenta equipo y operador, a través de inspección visual. y describa sus observaciones:

_____ _____

Pondere según su criterio de 0 a 100 _____.

16. ¿Existen procedimientos escritos para la recuperación del sistema en caso de fallas?

SI ( ) NO ( )

17. ¿Como se actúa en caso de errores?

Pondere según su criterio de 0 a 100 _____.

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

Pondere según su criterio de 0 a 100 _____.

19. ¿Se tienen procedimientos especificos que indique al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

SI ( ) NO ( )

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

SI ( ) NO ( )

21.¿ Se prohíbe a analistas y programadores la operación de la máquina?

SI ( ) NO ( )

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

SI ( ) NO ( )

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

SI ( ) NO ( )

¿Cuáles son?_____

24. Las intervenciones de los operadores:

Son muy numerosas	SI ( )	NO ( )
Se limitan los mensajes esenciales	SI ( )	NO ( )
Otras (especifique)	( )	

25. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?

SI ( ) NO ( )

26.¿ Como se controlan los trabajos en el centro de procesamiento de datos?

_____

Pondere según su criterio de 0 a 100 _____.

27. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de los datos?

SI ( ) NO ( )

28. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?

SI ( )

Por máquina ( )

Escrita manualmente ( )

NO ( )

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

SI ( ) NO ( )

30. ¿Existen procedimientos para evitar las corridas de programas no autorizados?

SI ( ) NO ( )

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

SI ( ) NO ( )

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

Pondere según su criterio de 0 a 100 _____.

33. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuentes, etc., fuera del centro de procesamiento de datos?

SI ( ) NO ( )

34. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?

SI ( ) NO ( )

Cómo? _____

35. Los privilegios del operador se restringen a aquellos que le son asignados a la clasificación de la seguridad de operador.

SI ( ) NO ( )

36. Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?

SI ( ) NO ( )

37. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?

SI ( ) NO ( )

38. ¿Durante cuanto tiempo?

Pondere según su criterio de 0 a 100 _____.

39. ¿Se toman que precauciones durante el periodo de implantación?

SI ( ) NO ( )

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

Pondere según su criterio de 0 a 100 _____.

41. ¿Se catalogan los programas liberados para producción rutinaria?

SI ( ) NO ( )

42. ¿Existe un lugar para almacenar las bitácoras del sistema del equipo de cómputo?

SI ( ) NO ( )

43. Indique como está organizado este archivo de bitácora.

Por fecha ( )

Por fecha y hora ( )

Por turno de operación ( )

Otros ( )

44. ¿Cual es la utilización sistemática de las bitácoras?

Pondere según su criterio de 0 a 100 _____.

45. Se lleva un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso del equipo.

SI ( ) NO ( )

46. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?

SI ( ) NO ( )

47. ¿Se tienen seguros sobre todos los equipos?

SI ( ) NO ( )

Con que compañía?

(Solicitar pólizas de seguros y verificar tipo de seguro y montos.)

48. INSTRUCTIVOS DE OPERACIÓN

Se debe verificar que el instructivo de operación contenga los siguientes datos:

Diagrama particular de entrada/salida	( )
Mensajes y su explicación	( )
Parámetros y su explicación	( )
Diseño de impresión de resultados	( )
Cifras de control	( )
Fórmulas de verificación	( )
Observaciones	( )
Instrucciones de casos de error	( )
Calendario de proceso y entrega de resultados	( )

ANEXO J2

INSTRUMENTO PARA EVALUAR EL CONTROL DE ASIGNACIÓN DE TRABAJO.

1- ¿Operan los equipos en base a programas de trabajo?

SI ( ) NO ( )

2- Indique los períodos que abarcan los programas de trabajo:

Pondere según su criterio de 0 a 100 _____.

3- Indique el puesto o departamento responsable de la elaboración de los programas de trabajo:_____

Pondere según su criterio de 0 a 100 _____.

4- ¿Se cambian frecuentemente los programas de trabajo?

SI ( ) NO ( )

5- ¿Cual es la causa principal?_____

Pondere según su criterio de 0 a 100 _____.

6- ¿Se comunica oportunamente a los usuarios las modificaciones a los programas de trabajo?

SI ( ) NO ( )

¿Como se comunican?_____

Pondere según su criterio de 0 a 100 _____.

7- Dentro del programa de trabajo para el equipo, Se tienen previstas:

- Demandas inesperadas? ( )
- Fallas del equipo? ( )
- Soporte de los usuarios? ( )
- Mantenimiento preventivo? ( )
- Otras (especifique)

8- ¿Con que frecuencia se asigna la computadora, en su totalidad, para una sola aplicación (la de mayor utilización).

_____ %

9- Especifique los elementos que sirven como base para programar las cargas del equipo

_____

_____

_____

Pondere según su criterio de 0 a 100 _____.

nota: debe procurarse que la distribución física del equipo sea funcional, que la programación de las cargas del equipo satisfaga en forma eficaz al usuario; se tendrá cuidado con los controles que se tengan para la utilización del equipo y el mantenimiento satisfaga las necesidades del equipo.

ANEXO J3

INSTRUMENTO PARA EVALUAR EL CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO.

1. Los locales asignados a la cintoteca y discoteca tienen:

Aire acondicionado ( )

Protección contra fuego ( )

(señalar el tipo de protección)

Cerradura especial ( )

Otra ( )

Observaciones:_____

ANÁLISIS DE ARCHIVOS

FUNCIÓN:

NOMBRE DEL ARCHIVO: _____

TIPO DE ARCHIVO: _____

DESCRIPCION: _____

_____

LOCALIZACIÓN: _____

VOLUMEN DE ARCHIVOS: _____

VOLUMEN DE ACTUALIZACIÓN: _____ FRECUENCIA: _____

EN VIGOR DESDE: _____

CLASIFICADO POR: _____

DOCUMENTOS O INFORMES A QUE DA ORIGEN: _____

_____

OTROS: _____

_____

USUARIO	USO	FRECUENCIA

CONTENIDO DEL ARCHIVO

FECHA	RECOPILÓ	REVISÓ	
			PÁGINA ___ DE ___

2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego?

SI ( ) NO ( )

(Señalar que tipo)

3. ¿Que información mínima contiene el inventario de la cintoteca y la discoteca?

Número de serie o de carrete ( )

Nombre o clave del usuario ( )

Nombre del archivo lógico ( )

Nombre del sistema que lo genera ( )

Fecha de la generación del archivo ( )

Fecha de expiración del archivo ( )

Número de volumen ( )

Otros ( )

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI ( ) NO ( )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, ¿se resuelven y explican satisfactoriamente las discrepancias?

SI ( ) NO ( )

6. ¿Que tan frecuentes son estas discrepancias?_____ _____

al mes.

Pondere según su criterio de 0 a 100 _____.

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta o disco, el cual fue inadvertidamente destruido?

SI ( ) NO ( )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

SI ( ) NO ( )

¿Cómo?_____ _____

9. ¿Existe un control estricto de las copias de estos archivos?

SI ( ) NO ( )

10. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ( )

Bóveda ( )

Otro ( )

(especifique)_____

11. Este almacén está situado:

*En el mismo edificio de la dirección de informática ( )

*En otro lugar ( )

¿Cuál?_____

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

SI ( ) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

14.¿Se registran como parte del nuevo inventario las nuevas cintas que recibe la biblioteca?

SI ( ) NO ( )

15. ¿Se tiene un responsable por turno, de la cintoteca y discoteca?

SI ( ) NO ( )

16. ¿Se realiza algún tipo de auditoria periódica a los medios de almacenamiento?

SI ( ) NO ( )

¿Con qué periodicidad?_____

17. ¿Se toman medidas en el caso del extravío de algún dispositivo de almacenamiento?

SI ( ) NO ( )

¿Cuales?_____

Pondere según su criterio de 0 a 100 _____.

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

SI ( ) NO ( )

19. ¿Se tiene personal autorizado para firmar la salida de archivos confidenciales?

SI ( ) NO ( )

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?

SI ( ) NO ( )

21. ¿Se lleva un control sobre los archivos prestados?

SI ( ) NO ( )

22. En caso de préstamo, ¿Con qué información se documentan?

*Nombre de la institución que hace el préstamo ( )

*Fecha de recepción ( )

*Fecha en que se debe devolver ( )

*Archivos que contiene ( )

*Formatos ( )

*Cifras de control ( )

*Código de grabación ( )

*Nombre del responsable que lo prestó ( )

*Otros_____

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros: _____

_____

_____

Pondere según su criterio de 0 a 100 _____.

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO ( )

25. ¿El cintotecario controla la cinta maestra anterior previniendo su uso incorrecto o su eliminación prematura?

SI ( ) NO ( )

26. ¿La operación de reemplazo es controlada por el cintotecario? SI ( ) NO ( )

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?

SI ( ) NO ( )

28. En los procesos que manejan archivos en línea, ¿existen procedimientos para recuperar archivos?

SI ( ) NO ( )

29. ¿Estos procedimientos los conocen los operadores?

SI ( ) NO ( )

30. ¿Con qué periodicidad se revisan estos procedimientos?

MENSUAL	( )	ANUAL	( )
SEMESTRAL	( )	OTRA	( )

31. ¿Existe un responsable en caso de falla?

SI ( ) NO ( )

32. Explique qué políticas se siguen para la obtención de archivos de respaldo: _____

_____

Pondere según su criterio de 0 a 100 _____.

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?

SI ( ) NO ( )

34. ¿Lo conoce y lo sigue el cintotecario?

SI ( ) NO ( )

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

SI ( ) NO ( )

¿Con qué frecuencia? _____

Pondere según su criterio de 0 a 100 _____.

ANEXO J4

INSTRUMENTO PARA EVALUAR EL CONTROL DE MANTENIMIENTO.

*1. Evaluar el tipo de mantenimiento mas conveniente.

---

2. Pedir el contrato de mantenimiento y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.
Pondere según su criterio de 0 a 100 _____.

3. Verificar el tipo de contrato que se tiene.

Pondere según su criterio de 0 a 100 _____.

4. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?

SI ( ) NO ( )

5. ¿Se lleva a cabo tal programa?

SI ( ) NO ( )

6. ¿Existen tiempos de respuesta y descompostura estipulados en los contratos?

SI ( ) NO ( )

7. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿que acciones correctivas se toman para ajustarlo a lo convenido? _____

_____

Pondere según su criterio de 0 a 100 _____.

8. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.

Pondere según su criterio de 0 a 100 _____.

9. ¿Existe algún tipo de mantenimiento preventivo que pueda dar el operador autorizado por el proveedor?

SI ( ) NO ( )

¿Cual? _____

Pondere según su criterio de 0 a 100 _____.

10. ¿Cómo se notifican las fallas?

_____

Pondere según su criterio de 0 a 100 _____.

11. ¿Cómo se les da seguimiento?

_____

Pondere según su criterio de 0 a 100 _____.

ANEXO J5

INSTRUMENTO PARA EVALUAR EL CONTROL DE FALLAS.

1. ¿Se mantienen registros actualizados de las fallas de los dispositivos del sistema de cómputo y servicios auxiliares (aire acondicionado, sistema de energía ininterrumpido, etc.)?

SI ( ) NO ( )

(solicitar los registros de los últimos seis meses)

2. ¿Es posible identificar por medio de estos registros, los problemas más recurrentes o fallas mayores que afectan en forma determinante el funcionamiento del equipo?

SI ( ) NO ( )

¿Cómo se identifican? _____

3. Tiempo de respuesta promedio que ha tenido con el contrato de mantenimiento (tiempo de respuesta es el período entre la notificación o aviso de la existencia de un problema o la llegada del personal técnico que realizó las reparaciones del equipo). _____ _____

Pondere según su criterio de 0 a 100 _____.

4. ¿Cuales son las actividades de los ingenieros que mantienen sus equipos? _____ _____

Pondere según su criterio de 0 a 100 _____.

5, ¿Cual considera que es la competencia técnica de los ingenieros de servicio que dan mantenimiento a sus equipos?

¿Porqué? _____ _____

Pondere según su criterio de 0 a 100 _____.

6. ¿Cuál es el tiempo promedio que toma investigar y resolver el problema? _____

Pondere según su criterio de 0 a 100 _____.

7. ¿Cuál es la disponibilidad de refacciones necesarias para dar mantenimiento a sus equipos? _____ ____

Pondere según su criterio de 0 a 100 _____.

8. ¿Cuál es la efectividad del proveedor para resolver sus problemas de mantenimiento? _____

Pondere según su criterio de 0 a 100 _____.

9. ¿Existen medidas de mantenimiento preventivo al dar mantenimiento preventivo a su equipo?

SI ( ) NO ( )

10. ¿Cuál es en general la calidad de los servicios ofrecidos bajo su "CONTRATO DE MANTENIMIENTO"?

Pondere según su criterio de 0 a 100 _____.

11. Cuál es el tiempo entre fallas ?_____.

Pondere según su criterio de 0 a 100

ANEXO J6

INSTRUMENTO PARA EVALUAR EL MANTENIMIENTO.

1. Indique los registros que se llevan de la utilización del equipo (especificando la periodicidad).

* Tiempo de uso del procesador central ( )
* Tiempo de compilación y prueba de programas ( )
* Tiempo dedicado a la producción ( )
* Tiempo dedicado a mantenimiento correctivo del sistema operativo ( )
* Tiempo dedicado a mantenimiento preventivo ( )
* Tiempo de operación del equipo ( )
* Tiempo de falla de los dispositivos ( )
* Tiempo de uso de cada unidad de cinta ( )
* Tiempo ocioso ( )
* Tiempo de uso de terminales (promedio por terminal) ( )
* Tiempo de uso de impresora ( )
* Tiempo de reproceso ( )
* Tiempo de la computadora utilizado en demostraciones ( )

* Tiempo de falla por servicios auxiliares ( )
* Número de programas corridos por compilador ( )
* Número de programas objeto ejecutados ( )

2. Anote los siguientes datos:

* Tiempo promedio de operaciones por día ___ Hrs
* Número promedio de compilaciones por día
* Número promedio de programas corridos por día
* Tiempo promedio de respuesta para compilaciones,__ Hrs
* Tiempo promedio de respuesta para programas de producción con cintas ____ Hrs.
* Tiempo promedio de respuesta para programas de producción
* Número promedio al día que se consideran como horas de producción
* Número promedio de trabajos en cola de espera de ejecución en horas pico
* Número promedio de trabajos en cola de espera de impresión en horas pico
* Número promedio de trabajos de ejecución en horas pico

Pondere según su criterio de 0 a 500 _____.

*3. Anote los porcentajes de tiempo por turno de operación que se dedica a:

turno	1er.	2o.	3er.
Compilación			
Prueba			
Producción			

*4. Evalúe la relación de uso de impresoras con respecto a la mezcla de trabajo. Estudie la frecuencia de cambio de papel y determine si se debe:

a) Incrementar el número de impresora ( )

b) Restaurar las cargas de trabajo ( )

c) Utilizar salida a microfilm ( )

d) Utilizar impresora de mayor velocidad ( )

e) Utilizar impresora láser ( )

f) ¿Es excesivo el volumen de impresión?

SI ( ) NO ( )

En caso de contestar sí, señale las causas:

* Reportes muy largos ( )

* Reportes no utilizados ( )

* Procesos en lote que deben estar en línea ( )

* Otros (especificar cuáles)_____

*g) Especificar si existen procesos que deben cambiarse de batch a línea y viceversa

*5. Evalúe la utilización del sistema de cómputo a través de las siguientes relaciones:

* Si el tiempo ocioso excede el 35 % del tiempo disponible
El equipo instalado está sobrado de capacidad para la carga de trabajo actual

* Si el tiempo de prueba de programas es mayor al 30 % del tiempo de uso del procesador central
Se puede concluir que los procedimientos de depuración de programas son pobres (excepto en instalaciones nuevas)

* Si el tiempo de mantenimiento al sistema operativo sobrepasa el 15 % del tiempo total disponible del sistema
Se deberá exigir al proveedor la calidad de soporte al sistema operativo

* Si el tiempo de falla del sistema de cómputo es mayor al 5 % del tiempo disponible
El servicio de mantenimiento correctivo que proporciona el proveedor es muy pobre y deberán revisarse las cláusulas del contrato relativas a este renglón

nota:
Estos son solamente ejemplos de factores que pueden obtenerse, los cuales pueden ser ampliados, y los porcentajes dependerán del tipo de equipo y la experiencia que se tenga.

6. A continuación se revisan las acciones que realiza la dirección de informática para evaluar, mantener y auditar los sistemas implantados:

* Número total de trabajos procesados ( )
* Número de programas corridos por usuarios y departamentos de la dirección de informática ( )
* Detalle de programas con terminación anormal especificando la causa (por departamento y usuario) ( )
* Tiempo de uso de los diversos equipos de captura por equipo y usuario ( )
* Número de líneas impresas en cada impresora ( )
* Otros

*7. Indique que tipo de evaluación se realiza a los sistemas implantados:

Ninguna	( )	De objetivos	( )
Económica	( )	De oportunidad	( )
De beneficios	( )	De operación	( )
Otros (especificar)	( )	_____	

8. Indique que instructivos se elaboran:

De codificación	( )	De captación	( )
Del usuario	( )	De operación	( )
Otros (especificar)	( )		

9. ¿Que porcentaje del personal de programación se dedica a dar mantenimiento a los sistemas existentes? _____

Pondere según su criterio de 0 a 100 _____.

11. ¿En que porcentaje se cumplen los calendarios de producción? _____

Pondere según su criterio de 0 a 100 _____.

12. Indique las estadisticas de elaboración de programas que se llevan a cabo en la unidad de informática:

Por programador	( )	Por sistema	( )
Por programa	( )	Por toda el área	( )
Otras (especificar)	( )	_____	

EVALUACIÓN DEL ANEXO J

Este instrumento consta de 6 cuestionarios y su forma de evaluación es de la siguiente manera: Todas las preguntas tienen un valor cuantificable positivo (100), dependiendo de la pregunta; pero, en algunos casos la pregunta será solamente de información y no tendrá valor cuantificable (Ej. Preg. 1 de control de mantenimiento) pues solamente servirá de apoyo al dictamen que se realizará (están marcadas con *).

Cada cuestionario tiene un valor numérico según la siguiente tabla:

Control de operaciones	5450
Control de asignación de trabajo	1200
Control de medios de almacenamiento masivo	5600
Control de mantenimiento	1100
Control de fallas	1200
Evaluación del mantenimiento	3250

El valor de cada cuestionario será comparado con la sumatoria de sus preguntas contestadas. De esto se obtendrá un porcentaje que en ningún momento será un dictamen de la auditoría, sino un valor con el que el auditor y su equipo harán el dictamen

En algunos casos habrán preguntas que no competan al sistema objeto de evaluación, en ese caso se eliminará la pregunta, y su valor (100 por cada opción que tenga) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas obtienen un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellos deberá ser parte de un documento para una evaluación posterior.

ANEXO K

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE PROCESO.

-CONTROL DE PRESENTACIÓN-

1. ¿Se tiene claro a quienes van dirigidos los informes generados por cada uno de los programas?

DESTINO DE LOS INFORMES POR CADA UNO DE LOS PROGRAMAS=					
PROGRAMA	NOMBRE DEL INFORME	PERSONA QUE RECIBE EL INFORME	UNIDAD A QUE PERTENECE	FRECUENCIA ESTIMADA	OBSERVACIONES

Pondere según su criterio de 0 a 100 _____.

=UN SOLO PROGRAMA PUEDE GENERAR VARIOS INFORMES

2. Evaluación a cada uno de los programas involucrados en la presentación de informes o resultados[4]

2.1 El informe o resultado presenta el contenido adecuado para:
( ) La persona que recibe el informe
( ) La unidad que recibe el informe
comentarios:_____
_____
_____

2.2 El informe o resultado presenta el formato adecuado para
( ) La persona que recibe el informe
( ) La unidad que recibe el informe
comentarios:_____
_____
_____

2.3 El informe o resultado se presenta con la frecuencia adecuada para
( ) La persona que recibe el informe
( ) La unidad que recibe el informe
comentarios:_____
_____
_____

3. ¿Existe una descripción formal de cada uno de los informes que se generan?

SI ( ) NO ( )

4. ¿Se hace análisis de los informes?

SI ( ) NO ( )

Ver cuadros referidos a la pregunta 3 y 4 al final de este instrumento.

[4] **POR CADA INFORME DE LA PREGUNTA ANTERIOR**

-CONTROLES A LOS INFORMES-

1. Cuando los informes quedan almacenados en archivos. ¿Se tienen copias de estos en otros locales?

SI ( ) NO ( )

2. ¿En que lugar se encuentran esos locales?

_____

_____

Pondere según su criterio de 0 a 100 _____.

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

MUCHA ( ) POCA ( ) NINGUNA ( )

4. ¿Qué confidencialidad se tiene en esos locales?

MUCHA ( ) POCA ( ) NINGUNA ( )

5. ¿Existe una persona encargada de la entrega de los documentos de salida?

SI ( ) NO ( )

explique:_____

_____

6. ¿En que forma se entregan?

_____

_____

ADECUADO ( ) ACEPTABLE ( ) INADECUADO ( )

7. ¿Se tiene un responsable usuario de la información de cada sistema?

SI ( ) NO ( ).

8. ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

_____

_____

ADECUADO ( ) ACEPTABLE ( ) INADECUADO ( )

9. ¿Se destruye la información no utilizada, o bien que se hace con ella?

DESTRUYE ( ) VENDE ( ) TIRA ( )

OTRO: _____

-CONTROLES A LA INFERENCIA-

1. ¿Se han previsto controles a la inferencia de la información no autorizada a determinados usuarios?

SI ( ) NO ( )

2. ¿Se han previsto controles a la inferencia tratando de obtener información no autorizada de la base de datos, a través del conocimiento de alguna característica de la información?

SI ( ) NO ( )

3. ¿Existen restricciones aplicadas a las consultas sobre la información?

SI ( ) NO ( )

4. ¿Existen restricciones aplicadas a la perturbación de los resultados obtenidos en fórmulas estadísticas?

SI ( ) NO ( )

NO HAY FORMULA CIENTO POR CIENTO EFECTIVA PARA EVITAR EL USO DE PROCESOS DE INFERENCIA, SIN EMBARGO, EL NIVEL DE RIESGOS PUEDE REDUCIRSE UTILIZANDO ESTOS CONTROLES

-CONTROLES DE PRODUCCIÓN Y DISTRIBUCIÓN-

1. ¿Existen procedimientos en caso de pérdida de información de un informe?

SI ( )

* del total de informes ( )

* de la mitad de los informes ( )

* de algún informe ( )

NO ( )

2. ¿Existen procedimientos en caso de modificación de un informe?

SI ( ) NO ( )

-CONTROLES DE RECUPERACIÓN-

1. ¿Se han previsto planes de contingencia si se llega a destruir algún informe, por cualquier razón?

SI ( ) NO ( )

2. ¿Se producen técnicas "SPOOLING" de la información que se produce?

SI ( ) NO ( )

3. ¿Existe un registro de información de los eventos que ocurren entre la producción de resultados y la entrega a los usuarios?

SI ( ) NO ( )

4. ¿Qué información se guarda en este registro?

* Resultados entregados a los usuarios ( )
* Personas que recibirán los resultados ( )
* Fecha en que se produjo el informe ( )
* Fecha en que se produjo la distribución ( )

5. ¿Se registran las siguientes informaciones de los recursos que consume un informe?

SI ( )

* Tiempo de utilización ( )
* Equipo ( )
* Humano ( )
* Otro ( )

NO ( )

6. ¿Existe un registro sobre la distribución de la información?

SI ( )

* ¿Se encuentra al día? SI ( ) NO ( )
* ¿Existe confidencialidad? SI ( ) NO ( )
* ¿Existe oportunidad? SI ( ) NO ( )
* ¿Son aprobados por alguna autoridad? SI ( ) NO ( )

NO ( )

7. ¿Son controlados los datos grabados en los archivos magnéticos con respecto a su concordancia con los informes impresos?
(procedimientos, controles para determinar la concordancia,etc.)

SI ( ) NO ( )

8. ¿Se da el caso de tener salidas en medios de almacenamiento para imprimir en otro equipo periférico?

SI ( )

* ¿Existen procedimientos al efectuar la impresión? SI ( ) NO ( )

NO ( )

9. ¿Se da el caso en que los datos son remitidos a sectores externos al sistema para preparar informes?

SI ( )

* ¿Porqué se procede de esta manera?

_____

_____

Pondere según su criterio de 0 a 100 _____.

* ¿Existe comunicación adecuada entre los puntos de emisión y recepción?

SI ( ) NO ( )

NO ( )

DESCRIPCION DE INFORMES

FECHA:

SISTEMA:

NOMBRE DEL INFORME:

PROPOSITO	CLAVE:_____
QUIEN LO FORMULA	PERIODICIDAD:_____
VOLUMEN EN HOJAS	EN VIGOR
FECHA EN QUE DEBE PRESENTARSE	DSDE:_____
OPORTUNIDAD __ COFIABILIDAD __ COMPLETO __	No. DE COPIAS:_____

COPIAS	U S U A R I O	U S O
ORIGINAL		
1a		
2a		
3a		
4a		

	DESCRIPCION DEL PROCEDIMIENTO

ANALIZO:

PAG __ DE __

ANALISIS DE INFORMES

FUNCION:

NOMBRE DEL INFORME: _____

PROPÓSITO DEL INFORME: _____

QUIÉN LO FORMULA: _____

QUÉ LO ORIGINA: _____

VOLUMEN DE HOJAS O REGISTROS: _____

FORMA DE HACERLO: _____

PRINCIPAL USUARIO: _____

FECHA TEORICA DE PRESENTACION: _____ PERIODICIDAD: _____

FECHA DE PRESENTACIÓN: _____ PERIODICIDAD: _____

NIVEL DE INFORMACIÓN: _____

EN VIGOR DESDE: _____

MODIFICACIONES: _____

_____

OTROS DATOS: _____

DATOS QUE CONTIENE	ORIGEN DE LOS DATOS

FECHA	RECOPILÓ	REVISÓ	INDICE
			PAG __ DE __

EVALUACIÓN DEL ANEXO K

Para el cuestionario de este instrumento se evaluará de la siguiente manera: Todas las preguntas y los cuadros tienen un valor que es cuantificable. **El cuestionario, tiene un valor numérico de 3900 más 600 por cada informe de la pregunta 1 del control de presentación**, el cual será comparado con la sumatoria de todas sus preguntas contestadas. Esto dará como resultado un porcentaje que en ningún momento será el resultado de la auditoria, sino un valor con el que el auditor y su equipo harán el dictamen.

En algunos casos habrán preguntas que no competan a este subsistema, en ese caso se eliminará la pregunta y su valor (100 por cada opción de la pregunta) se descontará del total del cuestionario.

Las preguntas que según su caso, al ser contestadas obtengan un valor de cero tendrán que ser parte del dictamen de la auditoria y además todo juicio emitido acerca de ellos deberá ser parte de un documento para una evaluación posterior.

ANEXO L

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE BASES DE DATOS.

La evaluación de este subsistema estará sujeta en el juicio crítico de el grupo de auditoria de sistemas y respaldado por sus respectivos papeles de trabajo.

La metodología de evaluación es la siguiente:

a) Someta a evaluación objetiva todos y cada uno de los cuatro apartados desarrollados en la sección 7.5.

b) Califique con una nota de 0 (cero) a 100 (cien) puntos cada uno de los subtemas de cada apartado.

c) Sume todos los puntos ganados por cada numeral.

d) Si se omitiera alguna de las consideraciones del numeral 7.5.1 de la sección 7.5, entonces califíquela con -25 puntos. En cualesquiera de los casos del numeral 7.5.2 califíquelas con -50 puntos. Los del numeral 7.5.3, con cero y los de la sección 7.5.4, en caso de omitirse alguno de ellos, ya que se refieren a los controles indispensables, califíquense con -75.

e) Realice un promedio de todos los puntos.

f) Cada calificación debe ir respaldada por los respectivos

papeles de trabajo.

g) Haga las recomendaciones que considere adecuadas.

Nota importante acerca de la re-evaluación de este instrumento:

1) En cuanto a los criterios de funcionamiento, específicamente en lo que respecta a los tiempos de accesos y velocidad de procesamiento, debe considerar que existen varios tipos de organización de sistemas de bases de datos: relacionales, jerárquicos y en red. Si se realizan pruebas de clasificación, recuerde que el modelo de red o jerárquico no requiere intrinsecamente de ninguna clasificación

2) Con respecto a las características deseables, tome en cuenta que si se trabaja en micros, sin interrelación entre ellos, la pregunta sobre capacidad de multiusuarios quedará sin efecto.

3) En cuanto a controles indispensables, si no se tiene red en la empresa donde se audita, lo referente a concurrencia, quedará sin efecto.

RESULTADOS:

menos de cero-	33.33	PUNTOS:	NECESITA MEJORAR.
33.33-	66.66	PUNTOS:	BUENO, PERO DEBE MEJORAR.
66.66-	100	PUNTOS:	MUY BUENO, PERO PUEDE MEJORAR.

ANEXO M

INSTRUMENTO PARA LA AUDITORÍA AL SUBSISTEMA DE COMUNICACIONES.

Llene la matriz de controles de acuerdo a la guía que se encuentra en la sección 7.6. Ver la matriz en la siguiente página.

La matriz terminada con los controles mostrará la relación que tiene cada control *in situ* con respecto a la amenaza que se supone que dicho control mitiga y el componente al que salvaguarda o controla.

Ahora es necesario evaluar la idoneidad de los controles. Esto se logra revisando cada subconjunto de controles según se relaciona con dada área de amenaza y de componente de la matriz. Por ejemplo, se evalúa el subconjunto de controles que constituye una columna abajo de una amenaza. El objetivo de este paso es responder la pregunta específica "se tienen los controles específicos y son adecuados con respecto a cada amenaza específica?".

AMENAZAS

COMPONENTES

UBIQUE LAS AMENAZAS Y COMPONENTES QUE SE ENCUENTRAN PRESENTES EN EL SISTEMA DE COMUNICACIONES QUE SE ESTA AUDITANDO

Este tipo de revisión también puede efectuarse para otros diferentes subconjuntos de controles. Por ejemplo, es posible evaluar subconjuntos individuales de controles según se relacionen con amenazas (columnas), componentes (filas), cuadro individuales y cuadros vacios. El método matricial constituye una herramienta perfecta para efectuar un microanálisis de controles en una red de comunicación de datos.

La matriz muestra claramente la relación entre diferentes subconjunto de controles y áreas de amenazas especificas, componentes, cuadros individuales y cuadros vacios.

Algunas casillas individuales pueden ser de especial interés para una red o compañía, y por lo tanto tales casillas se deben revisar con cuidado.

Las casillas vacías significan falta de control, lo que puede ser un serio problema.

La evaluación de este subsistema estará sujeta en el juicio critico de el grupo de auditoria de sistemas y respaldado por sus respectivos papeles de trabajo.

La metodología de evaluación es la siguiente:

a) Someta a evaluación objetiva todas y cada una de las filas y columnas de la matriz.

b) Califique con una nota de 0 (cero) a 100 (cien) la efectividad que a su juicio merezca cada intersección de

fila y columna.

c) Sume todos los puntos ganados por todas las casillas.

d) Realice un promedio de todos los puntos.

e) Cada calificación debe ir respaldada por los respectivos papeles de trabajo.

f) Haga las recomendaciones que considere adecuadas.

Reevaluación de este instrumento:

Por la naturaleza de la metodología empleada en la evaluación de los controles al sistema de comunicaciones, los componentes y amenazas serán las que realmente se encuentran en el lugar. No cabe entonces un adecuamiento de acuerdo al tipo de sistema evaluado.

RESULTADOS:

0	-	33.33	PUNTOS:	NECESITA MEJORAR.
33.33-		66.66	PUNTOS:	BUENO, PERO DEBE MEJORAR.
66.66-		100	PUNTOS:	MUY BUENO, PERO PUEDE MEJORAR.

ANEXO N

COMO USAR EL SOFTWARE DE APOYO

Este apartado trata la forma de utilizar el software que se ha diseñado para apoyar al auditor. Sin embargo es adecuado que primero conozca algunas generalidades en las que se encuentra involucrado para que pueda hacerse un mejor uso de el.

La metodología para Auditar Sistemas Informáticos implica una gran cantidad de pasos, en el que están involucrados una serie de instrumentos bastante específicos y descriptivos que evalúan cada una de las partes dentro del Sistema Informático y su entorno. Esto significa que para aplicarla eficientemente debe conocerse muy bien el sistema que habrá de auditarse y además la metodología diseñada.

El software trabaja en el ambiente de FoxPro 2.0 o FoxProLan 1.02 o versiones mayores. Cuenta con 20 programas que trabajan en conjunto para elaborar pantallas, generar informes y presentar resultados, además presenta a facilidad de reproducir todo el resultado de una auditoría anterior, pues queda registrada en una base de datos especial.

Para poder utilizarla, todo el software debe instalarse en el disco duro creando un directorio llamado sistema (c:\sistema). Debe incluirse el directorio del manejador de base de datos en el PATH (ruta de búsqueda de DOS. Ej. PATH ...;C:\FOX).

Para llamar al programa que ejecuta la auditoría,[5] tiene que estar en la ventana de comandos de Fox y digitar **DO C:\SISTEMA\GENERAL.** A continuación se mostrará una pantalla de la presentación de la Auditoria de Sistemas. Podrá presionar cualquier tecla para pasar a la siguiente pantalla o al cabo de 5 segundos automáticamente cambiará.

La presentación será:

---

[5] Los programas fuente se anexan en un diskette al final de todo el documento

AUDITORIA DE SISTEMAS INFORMATICOS

Universidad de El Salvador, Facultad de ingenieria y arquitectura

AUDITORIA DE SISTEMAS INFORMATICOS

E M P R E S A

RASA

G E R E N T E

JHONY MATA

EVALUADO POR : CESAR CHEVEZ

FECHA : 11/04/94

HORA : 15:14:52

En esta pantalla se digita: El nombre de la empresa que será objeto de áudito, nombre del responsable de la empresa y nombre del auditor encargado. En ese momento queda registrada la fecha y hora de la evaluación (la pantalla muestra nombres ficticios como ejemplo).

Una vez registrada esta información, aparece una pantalla con la presentación de las dos áreas macros a evaluar:

AUDITORIA DE SISTEMAS INFORMATICOS

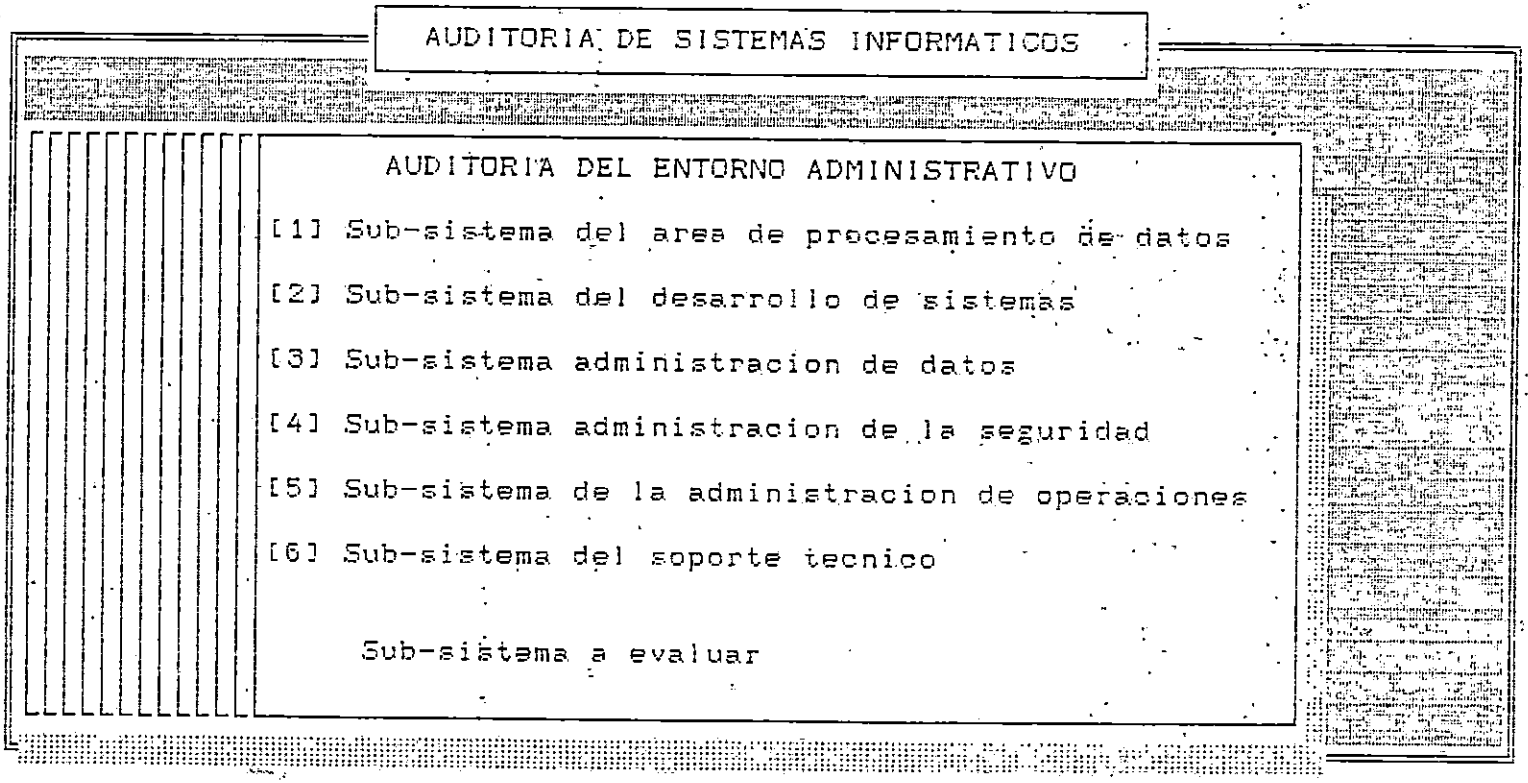
AUDITORIA DEL ENTORNO ADMINISTRATIVO DEL S.I. (1)

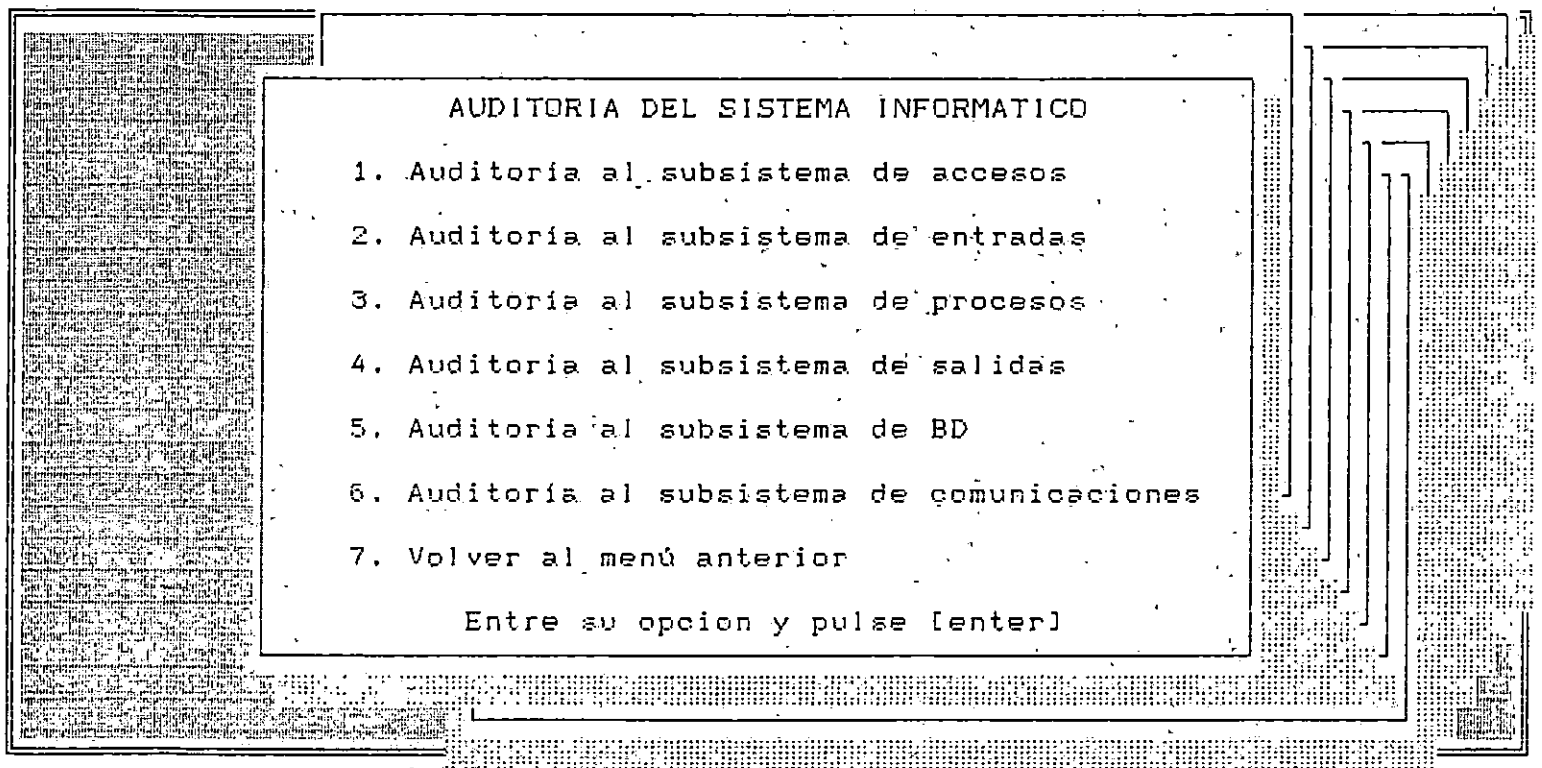
AUDITORIA DEL SISTEMA INFORMATICO (2)

Escoja la opcion

Se sugiere comenzar con la Administración del Sistema (Ver diseño de la metodología en documento), pero, puede comenzar con el que a su criterio considere conveniente.

Si presiona 1 (Entorno Administrativo del Sistema) o bien 2 (Sistema Informático) las pantallas que se mostrarán respectivamente son:


AUDITORIA DE SISTEMAS INFORMATICOS
AUDITORIA DEL ENTORNO ADMINISTRATIVO
[1] Sub-sistema del area de procesamiento de datos
[2] Sub-sistema del desarrollo de sistemas
[3] Sub-sistema administracion de datos
[4] Sub-sistema administracion de la seguridad
[5] Sub-sistema de la administracion de operaciones
[6] Sub-sistema del soporte tecnico
Sub-sistema a evaluar


AUDITORIA DEL SISTEMA INFORMATICO
1. Auditoria al subsistema de accesos
2. Auditoria al subsistema de entradas
3. Auditoria al subsistema de procesos
4. Auditoria al subsistema de salidas
5. Auditoria al subsistema de BD
6. Auditoria al subsistema de comunicaciones
7. Volver al menú anterior
Entre su opcion y pulse [enter]

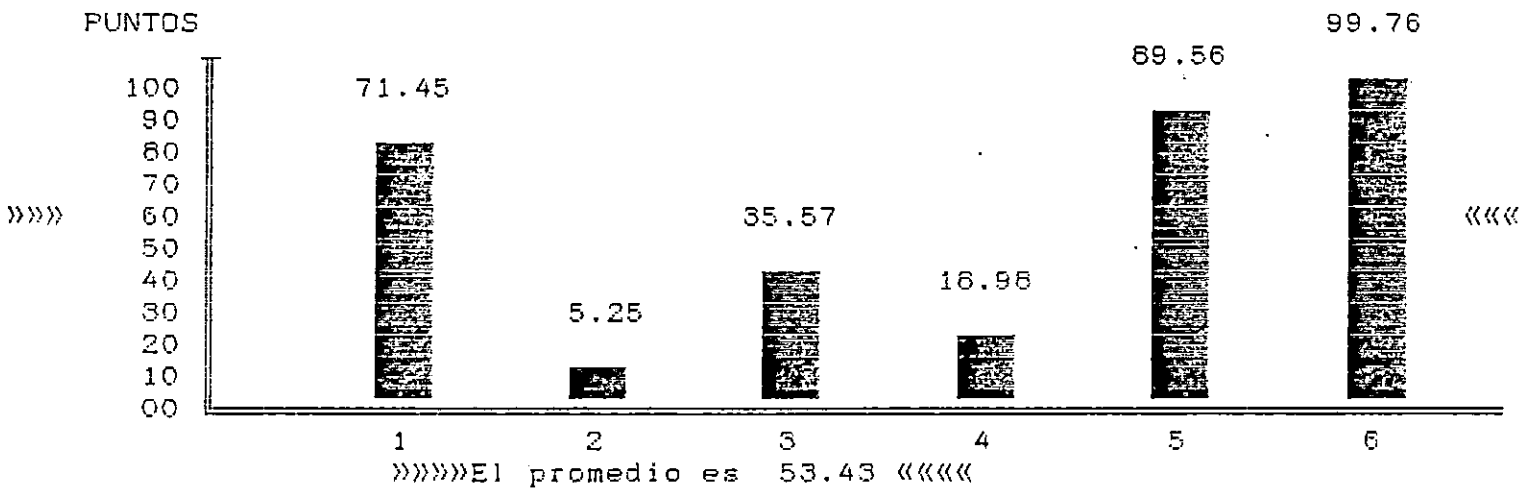
Cada una de estas muestra un menú con opciones para evaluar los subsistemas en que se dividen estas Areas. Si se accesa a una de estas opciones de inmediato tendrá a su disposición el instrumento que lo evalúa.

Cuando un instrumento finaliza (cualquiera que sea este) aparecerá un mensaje con la siguiente pregunta "¿Desea finalizar s/n?", Si presiona **N** o **n** volverá al menú que llamó al instrumento para poder seguir la evaluación de otro subsistema. Cualquier otra tecla que presione lo enviará a una presentación de resultados, en forma de gráfico de barras tanto del Entorno Administrativo como del Sistema.

A continuación se muestra un ejemplo de ello:

RESULTADOS DE LA AUDITORIA
SUBSISTEMAS DEL ENTORNO ADMINISTRATIVO

1-ADMON DEL AREA DE P.E.D. 3-ADMON DATOS 5-ADMON DE OPERAC
2-DESARROLLO DE SISTEMAS 4-ADMON DE SEGURIDAD 6-SOPORTE TECNICO

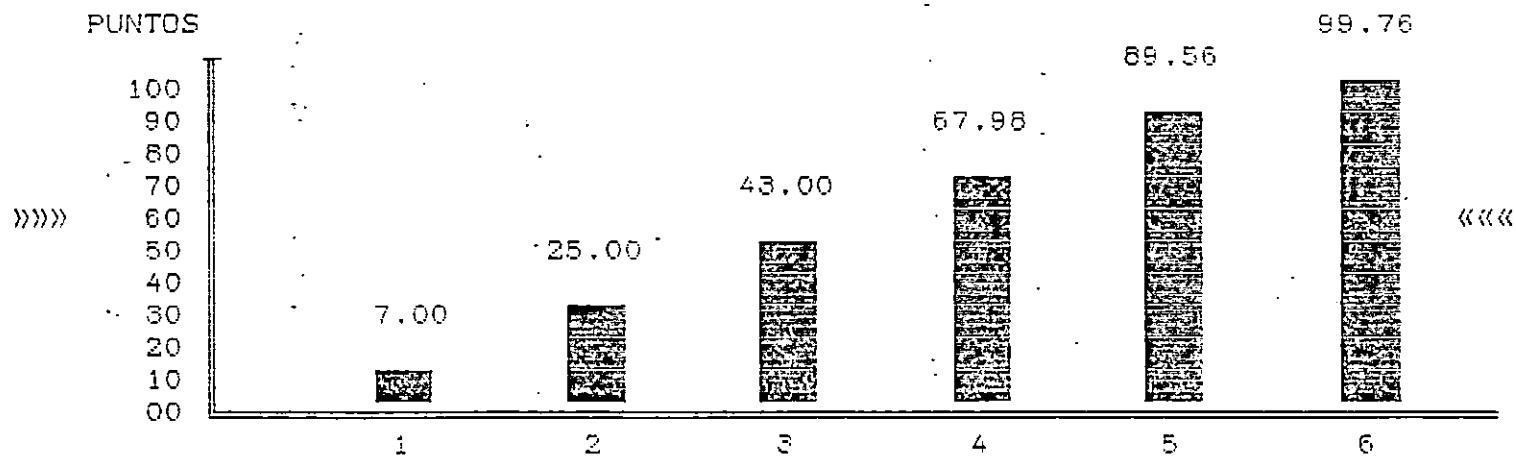


»»»»»El promedio es 53.43 «««««

pulse [ENTER] para continuar

RESULTADOS DE LA AUDITORIA
SUBSISTEMAS DEL SISTEMA INFORMATICO

1-ACCSESOS	3-PROCESOS	5-BASES DE DATOS
2-ENTRADAS	4-SALIDAS	6-COMUNICACIONES



»»»»»El promedio es 55.38 ««««

pulse [ENTER] para continuar

Los instrumentos son fáciles de manejar, pues se ha buscado que tengan exactamente la misma presentación que tienen en el documento donde se encuentra la metodología.[1]

Muchos de los instrumentos tienen la misma estructura (están basados en cuestionarios) ,por consiguiente a manera de ejemplo se mostrará solamente uno de ellos, los instrumentos que evalúan por matriz y formularios se presentan al final.

El instrumento basado en cuestionario que servirá como demostración es el que evalúa la Administración de Datos, cuya presentación es la siguiente:

---

[1] Algunas veces el instrumento puede hacer referencia al documento, por lo que es recomendable que Ud. lo tenga a mano para evitar contratiempos.

6.3 AUDITORIA AL SUBSISTEMA DE ADMINISTRACION DE DATOS

La administración de datos tiene una caracteristica importante que debe ser considerada al practicar una auditoria de sistemas en esta área: La función del administrador de datos (DA) y del administrador de la base de datos (DBA).

Si alguna de estas funciones no está definida formalmente en la instalación, debe procederse a realizar las recomendaciones del caso para crear estos cargos y definir sus responsabilidades. En toda área de procesamiento de datos, sin embargo estas tareas son ejecutadas en alguna medida por el personal de la misma.

Es posible que en algunos sistemas no se cuente con un sistema de administración de bases de datos, en cuyo caso las funciones del DBA no serán definidas. También es factible que en algunas instalaciones esta área no requiera de personal destinado a tiempo completo para ejecutar las funciones, por lo que se puede compartir esta labor con el desempeño de otras tareas relacionadas.

La calidad de la administración de datos depende directamente de la existencia y de la calidad del DA y el DBA.

Asi se evalúa la integridad de la base de datos y las funciones del DA y DBA.

Presione cualquir tecla...

1. ¿Está definida formalmente la función del administrador de datos?

SI ( ) NO ( ) Respuesta S/N :

2. ¿Está formalmente definida la función del administrador de la base de datos?

SI ( ) NO ( ) Respuesta S/N :

3. ¿Existen controles sobre la definición de la base de datos? (busca correspondencia entre la base de datos y su definición)

SI ( ) NO ( ) Respuesta S/N :

4. ¿Existe control sobre la recuperación de los datos? (establece un mecanismo para recuperar la información en caso de fallas, pérdida o daño de la información)

SI ( ) NO ( ) Respuesta S/N :

5. ¿Existe control de acceso? (previene el riesgo del ingreso no autorizado a la utilización y/o modificación de la información contenida en la base de datos)

SI ( ) NO ( ) Respuesta S/N :

Este instrumento consta de 3 pantallas, que son bastante fáciles de entender, y cuando finaliza se digita n ó N para volver al menú que lo llamó.

El siguiente instrumento que se presenta es el que evalúa la Administración del área de Procesamiento de datos:

INSTRUMENTO EVALUADOR
DE LOS PLANES ECONOMICOS

Complete la imformación socilitada CODIGO : PR2-FM1

ELEMENTOS	valor	PUNTAJE	OBSERVACIONES
Grado de claridad	15	15	
Objetividad en metas	15	0	
Periodos estimados	10	0	
Definición de responsables.	10	5	No se tiene claro
Recursos necesarios	5	5	
Acciones concretas	10	0	
Utiliza sf. para la planificación	10	0	
Eficiencia en tiempo de ej. del Sf	5	0	No se tiene
Numero de ejecuciones	5	0	
Máquinas utilizadas	5	0	
Eficiencia del sistema	10	4	Necesita mejorar

AUDITORIA DE SISTEMAS INFORMATICOS

RESULTADOS PRELIMINARES :

- Promedio de la evaluación = 29

- Observaciones

Los planes deben mejorarse en cuanto a su objetividad, cumplimiento, claridad mala administración de recursos desconocimiento de acciones concretas y baja eficiencia de sistemas utilizados para la planificación.

PRESIONE CUALQUIER TECLA

INSTRUMENTO EVALUADOR
DE LOS PLANES OPERACION

Complete la imformación socilitada CODIGO : PR2-FM2

ELEMENTOS	valor	PUNTAJE	OBSERVACIONES
Grado de claridad	15	0	
Objetividad en metas	15	0	
Periodos estimados	10	0	
Definición de responsables.	10	0	
Recursos necesarios	5	0	
Acciones concretas	10	0	
Utiliza sf. para la planificación	10	0	
Eficiencia en tiempo de ej. del Sf	5	0	
Numero de ejecuciones	5	0	
Máquinas utilizadas	5	0	
Eficiencia del sistema	10	0	

AUDITORIA DE SISTEMAS INFORMATICOS

RESULTADOS PRELIMINARES :

- Promedio de la evaluación = 0

- Observaciones

Los planes op. deben mejorarse en cuanto a su alcance, cumplimiento, claridad mala administración de recursos desconocimiento de acciones concretas y baja eficiencia de sistemas utilizados para la planificación.

-PRESIONE CUALQUIER TECLA

INSTRUMENTO EVALUADOR
DE LOS OBJETIVOS GENERAL

Complete la imformación socilitada

CODIGO : PR2-FM3

ELEMENTOS	valor	PUNTAJE	OBSERVACIONES
Conceptualizacion	20	20	
Documentacion	5	5	
Aprobacion total	10	8	
Grado en que el ob.repres.un juici	15	12	
Claridad en fecha de fina. del obj	5	5	
Claridad en objetivos	15	15	
Precision y especificidad	5	5	
Concordancia con pol.,plan.y prgma	5	5	
Autoridad de resp.para ejecutarlos	5	5	
Efect.de los controles de los obj.	10	10	

AUDITORIA DE SISTEMAS INFORMATICOS

RESULTADOS PRELIMINARES :

- Promedio de la evaluación = 90

- Observaciones

Los objvos. se conceptualizan correctame, ademas se documentan adecuadamente tambien el objetivo representa un solo juicio, tomando en cuenta que el obj. es muy claro. Los objetivos son precisos y especificos.

PRESIONE CUALQUIER TECLA

INSTRUMENTO EVALUADOR
DE LOS OBJETIVOS ESPECIFICOS

Complete la información socilitada

CODIGO : PR2-EM4

ELEMENTOS	valor	PUNTAJE	OBSERVACIONES
Conceptualizacion	20	15	
Documentacion	5	3	
Aprobacion total	10	10	
Grado en que el ob.repres.un juici	15	10	
Claridad en fecha de fina. del obj	5	3	
Claridad en objetivos	15	10	
Precision y especificidad	5	2	
Concordancia con pol.,plan.y prgma	5	4	
Autoridad de resp.para ejecutarlos	5	5	
Efect.de los controles de los obj.	10	6	

AUDITORIA DE SISTEMAS INFORMATICOS

RESULTADOS PRELIMINARES :

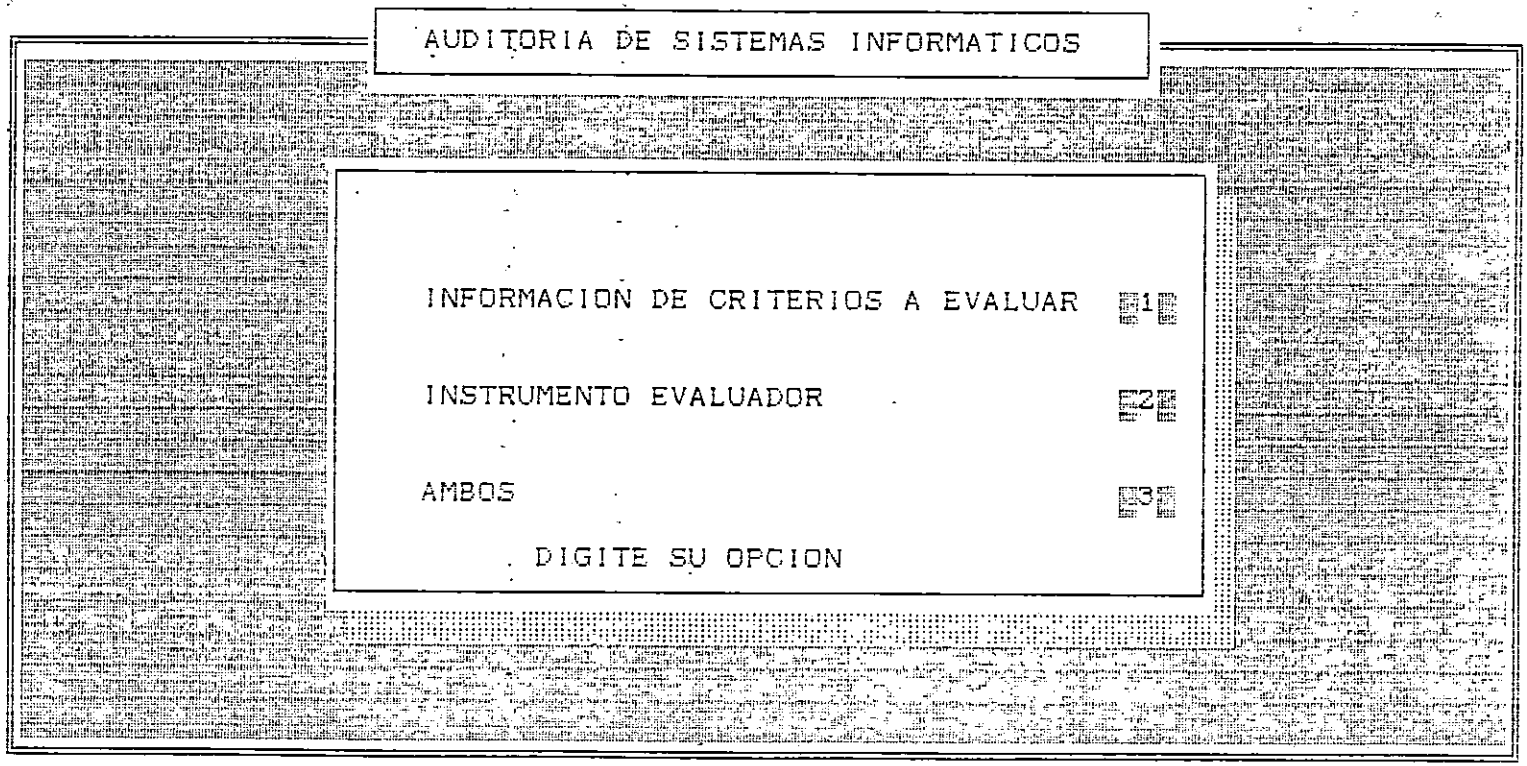
- Promedio de la evaluación = 68
- Observaciones

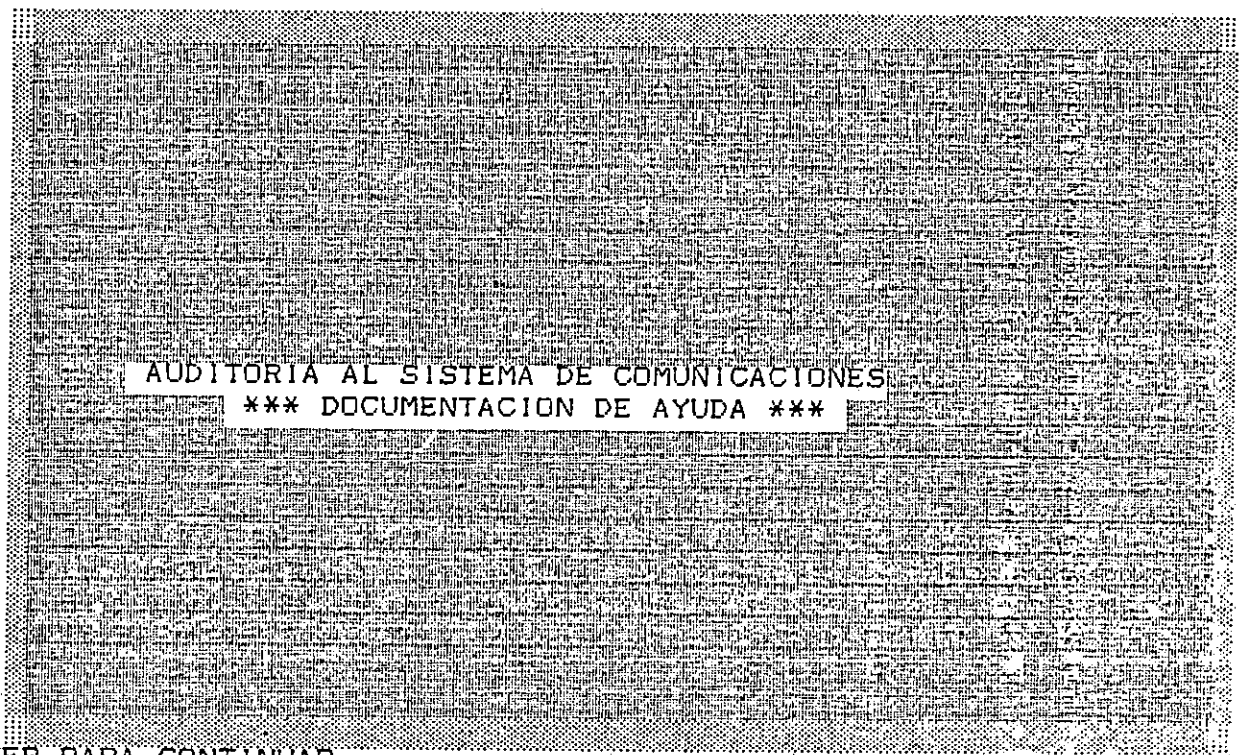
Los objvos. se conceptualizan correctame, ademas se documentan adecuadamente tambien el objetivo representa un solo jùicio, tomando en cuenta que el obj, es muy claro. Los objetivos son precisos y especificos.

PRESIONE CUALQUIER TECLA

Desea finalizar (s/n) ? n

A continuación se presenta el instrumento que se evalúa por matriz, el Subsistema de Comunicaciones:


AUDITORIA DE SISTEMAS INFORMATICOS
INFORMACION DE CRITERIOS A EVALUAR 1
INSTRUMENTO EVALUADOR 2
AMBOS 3
DIGITE SU OPCION



PULSE ENTER PARA CONTINUAR

METODOLOGIA

Para tener la certeza de que la red de comunicación de datos y las estaciones de trabajo de las microcomputadoras cuentan con todos los controles necesarios y que estos controles ofrecen protección adecuada, se construirá una matriz bidimensional en la que se incorporarán todos los controles que se encuentren presentes en ese momento en la red.

La matriz se construye identificando primero todas las amenazas que enfrenta la red y, después, todos los componentes de la red.

- Una amenaza a la red de comunicación de datos es cualquier evento adverso potencial que pueda dañar la red, interrumpir los sistemas que se encuentran utilizando la red, o provocar pérdidas económicas a la organización. Por ejemplo, la pérdida de mensajes es una amenaza potencial.
- Un componente es una de las partes individuales que, cuando se ensamblan juntas, integran la red de comunicación de datos. Un componente puede considerarse un bien que se encuentra sometido a revisión o un bien sobre el que se está intentando mantener control. Así, los componentes son Hardware, Software, Circuitos, y otras piezas de la red.

Pulse [ENTER] para continuar

En las figuras SC-1 y SC-2, se definen varias amenazas generales a una red de comunicación de datos. En las figuras SC-3 y SC-4, se definen varios componentes generales de una de dichas redes.

Para la identificación y la documentación de los controles de una red es necesario identificar las amenazas y componentes especificos que se relacionan con cualquier red que esté utilizando la organización. Una vez que se han identificado las amenazas y componentes especificos de la organización, entonces es posible relacionar con tales amenazas y componentes los controles individuales que se encuentran en el lugar.

Una vez que se han identificado las amenazas y las partes componentes, el paso que sigue es colocar una breve descripción de cada amenaza en la parte superior de la matriz.

De igual manera, en el eje vertical izquierdo de la matriz se escribe una breve descripción de cada componente, como se muestra en la figura SC-5.

Pulse [ENTER] para continuar

Una vez que se han etiquetado los ejes horizontal y vertical, el paso siguiente es identificar todos los controles especificos que se estan utilizando actualmente en la red de comunicación de datos. Estos controles in situ deben describirse y colocarse en una lista numerada. Por ejemplo, supóngase que se han identificado 24 controles que estaban utilizándose en la red. Se describe cada uno, además de numerarlos consecutivamente del 1 al 24. La lista de controles numerados no tienen clasificación alguna: el primer control es el número 1 sencillamente porque es el primer control identificado. Luego, cada uno de los controles identificados se coloca en el cuadro apropiado de la matriz. Esto se logra leyendo la descripción de cada control en la lista de control y luego planteando las dos preguntas siguientes:

1. Cuál o cuáles amenazas mitigará o detendrá este control?
2. Cuál o cuáles componentes salvará o preservará este control?

Pulse [ENTER] para continuar

Por ejemplo, si la descripción del control 1 es "asegurar que el sistema pueda conmutar mensajes de una estación/terminal caída hacia una estación/terminal alternativa", entonces se debe escribir el número 1 en la primera entrada (cuadro) en el ángulo superior izquierdo. Se asignó esta posición porque un cotnrol que asegura que el sistema puede conmutar mensajes cuando una estación se ha caído ayuda a controlar errores y también es un control que salvaguarda la computadora principal o el procesador de entrada (o ambos) o reside en ellos. Un control también puede aparecer en varios otros cuadros. La cuestión es que al responder a las dos preguntas anteriores sea posible colocar cada control en los cuadros idóneos de la matriz.

La matriz terminada con los controles mostrará la relación que tiene cada control in situ con respecto a la amenaza que se supone que dicho control mitiga y el componente al que salvaguarda o controla.

Pulse [ENTER] para continuar

El último paso en el diseño de una matriz de controles para una red de comunicación de datos especifica es evaluar la idoneidad de los controles. Esto se logra revisando cada subconjunto de controles según se relaciona con dada área de amenaza y de componente de la matriz. Por ejemplo, se evalúa el subcon junto de controles que constituye una columna abajo de una amenaza. El objetivo de esté paso es responder la pregunta especifica "se tienen los controles específicos y son adecuados con respecto a cada amenaza especifica?".

Este tipo de revisión también puede efectuarse para otros diferentes subconjuntos de controles. Por ejemplo, es posible evaluar subconjuntos individuales de controles según se relacionen con amenazas (columnas), componentes (filas), cuadro individuales y cuadros vacios. El método matricial constituye una herramienta perfecta para efectuar un microanálisis de controles en una red de comunicación de datos. La matriz muestra claramente la relación entre diferentes subconjunto de controles y áreas de amenazas especificas, componentes, cuadros individuales y cuadros vacios.

Pulse [ENTER] para continuar

Algunas casillas individuales pueden ser de especial interes para una red o compañía, y por lo tanto tales casillas se deben revisar con cuidado.

Las casillas vacias significan falta de control, lo que puede ser un serio problema.

.Errores y omisiones. Transmisiones accidentales o intencionales de datos que contienen errores, incluyendo las omisiones accidentales o intencionales de datos que se debieron introducir o transmitir en el sistema en línea. En este tipo de riesgo se incluyen entre otras cosas datos inexactos, datos incompletos, malfuncionamiento del hardware, etc.

.Pérdida o cambio de mensajes. Pérdida de mensajes al ser transmitidos por el sistema de comunicación de datos, o su cambio accidental o intencional durante la transmisión.

Pulse [ENTER] para continuar

.Desastres y siniestros (naturales u ocasionados por el hombre). Interrupción temporal o a largo plazo de la comunicación normal de datos. Con este riesgo se hace inoperante el sistema normal de comunicación de datos en línea de la organización.

.Pérdida de privacía. Entrega accidental o intencional de datos acerca de un individuo, suponiendo que tal entrega de información no es parte de las actividades normales de negocios de la organización.

.Extravío/robo. Extravío o robo de información que se debe mantener confidencial a causa de la naturaleza de su propietario. En cierto modo, ésta es una forma de pérdida de privacía, pero la información que se extrae no pertenece a un individuo. La información se puede divulgar de manera inadvertida (accidental) o ser objeto de un robo intencional. En este riesgo también se incluye el robo de bienes como en los casos de malversaciones, fraude o desfalco.

Pulse [ENTER] para continuar

.Confiabilidad (tiempo de funcionamiento). Confiabilidad de la red de comunicación de datos y su "tiempo de funcionamiento". En esto se incluye la capacidad de la organización de mantener la red de comunicación de datos en operación y el tiempo medio entre fallas (TMEF), así como el tiempo para reparar el equipo cuando funciona mal. La confiabilidad del hardware y del software y el mantenimiento de estas dos par tes son de gran interés.

.Reparación y rearranque. Capacidades de recuperación y reinicio en la red de comunicación de datos en caso de falla. En otras palabras, cómo opera el software en modo de falla? En este concepto de recuperación y rearranque se incluye el respaldo para porciones clave de la red de comunicación de datos y el plan de contingencia para respaldo, en caso de falla en cualquier punto de la red de comunicación de datos

Pulse [ENTER] para continuar

.Manejo de errores. Metodología y controles que se utilizan para manejar los errores en un sitio remoto distribuido o en un sitio de computadora centralizada. En este concepto se incluyen los procedimientos para el manejo de errores en un sistema de procesamiento distribuido (en el sitio distribuido). El objetivo de esto es asegurar que cuando se encuentren errores, se corrijan rápidamente y los datos se introduzcan en el sistema para su procesamiento.

.Validación y verificación de datos. Validación de datos, ya sea al momento de su introducción o durante la transmisión. La validación puede efectuarse en el sitio remoto (terminal inteligente), en el sitio central (procesador de comunicación de entrada) o en un sitio de inteligencia distribuida (concentrador o procesador de comunicación de entrada remota).

Pulse [ENTER] para continuar

.Computadora principal. Su forma más común es la de una computadora central a la que transmite la red de comunicación de datos y de la que ésta recibe información. En un sistemadistribuido con igual capacidad de procesamiento en cada modo distribuido, puede no haber una computadora central identificable, sino sólo otra computadora distribuida delmismo tamaño.

.Software. Programas logisticos con los que opera la red de cmunicación de datos. Estos programas pueden residir en la cmputadora central, en un sistema de computadoras distribuidas, en el procesador de comunicación de entrada, en un concentrador o un multiplexor estadistico remotos o en una terminal remota inteligente (o en una combinación de ellos). En este software se pueden incluir los métodos de acceso, un monitor de teleproceso completo, programas que residan en los rpocesadores de entrada y programas que residan en ter tinales inteligentes.

Pulse [ENTER] para continuar

.Procesador de comunicación de entrada. Dispositivo de hardware que interconecta todos los circuitos (lineas) de comunicación de datos con la computadora central o las com putadoras distribuidas y realiza algunas de las siguientes funciones: conversión de código y velocidad, protocolo, de tección y corrección de errores, verificación de formato, autenticación, validación de datos, agrupación de estadis ticas de datos, exploración/direccionamiento, inserción/borrado de códigos de control de linea y funciones semejantes

Pulse [ENTER] para continuar

.Multiplexor, concentrador, conmutador. Dispositivo de hardware mediante los cuales la red de comunicación de datos opera de manera más eficiente. El multiplexor es un dispositivo que combina en una corriente de datos, varias señales de datos simultáneas de estaciones independientes. El concentrador realiza las mismas funciones que el multiplexor, a excepción de que aquél tiene "inteligencia" y por tanto puede desarrollar algunas de la funciones del proce sador de comunicación de entrada. Un conmutador es un dispositivo con el que se hace la interconexión de dos circuitos (líneas) cualesquiera conectados a él. Puede haber dos tipos distintos de conmutador: uno que realiza la conmutación de mensajes entre estaciones (terminales) y que se puede ubicar en las instalaciones de la red de comunicación de datos que pertenecen a la organización y son operadas por ella; otro que realiza la conmutación de líneas o circuitos, con el cual se interconectan varios circuitos y que se puede localizar en la oficina central de la compañía te lefónica y ser propiedad de ella. Por ejemplo, la conmutación de mensajes es realizada por las organizaciones, y la compañía telefónica se encarga de la conmutación de circuitos.

Pulse [ENTER] para continuar

.Circuitos (líneas) de comunicación. Medios de transmisión de la empresa de comunicaciones que se utilizan como en la FIGURA SC3

COMPONENTES GRALES DE UNA RED DE COMUNICACION DE DATOS
.Enlaces (un enlace es la interconexión de cualesquiera dos

terminales/estaciones) para interconectar las terminales/esta ciones de la organización. Entre estos circuitos de comunicación se incluyen medios para satélite, instalaciones de conmutación pública con marcación, líneas privadas punto a punto, lineas multiplexadas, lineas privadas en configuración multipunto o de abonado y muchos otros.

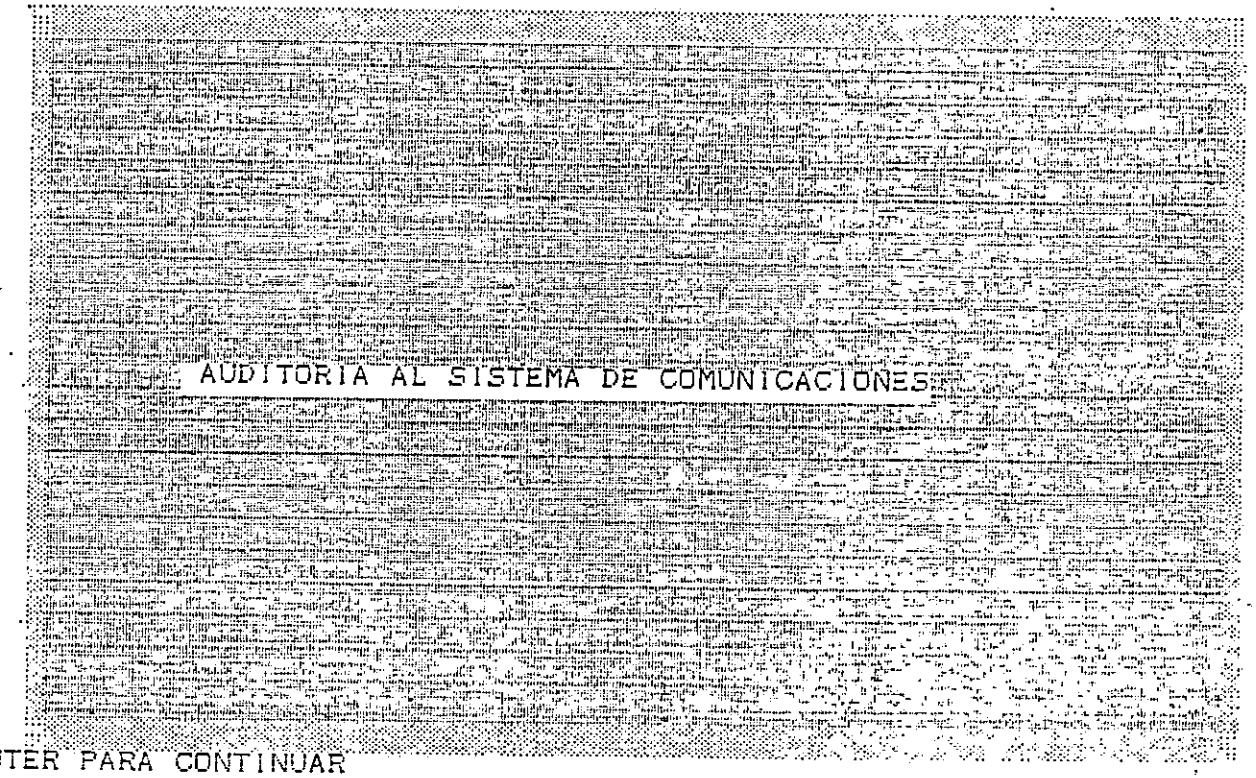
.Línea de abonado (local). Medio de comunicación entre las instalaciones del usuario y el equipo central de la compañía telefónica o la central de cualquier otra empresa especial de comunicaciones. Generalmente se supone que la línea local consiste en pares de alambres metálicos.

Pulse [ENTER] para continuar

.Modem. Dispositivo de hardware utilizado para convertir las señales de datos provenientes de las terminales (señal digital) a una forma eléctrica (señal analógica) que se acepta para su transmisión por los circuitos de comunicación que la compañía telefónica u otra empresa especial de comunicaciones posee y mantiene.

.Personal. Individuos responsables de introducir los datos, operar y mantener el equipo de la red de comunicación de da tos, escribir los programas de software para comunicación de datos, y administrar toda la red de comunicación de datos; también aquellos que se encuentran en las estaciones/termi nales remotas.

Pulse [ENTER] para continuar



PULSE ENTER PARA CONTINUAR

1) AMENAZAS GENERALES A UNA RED DE COMUNICACION DE DATOS

a1 .Errores y omisiones.
a2 .Pérdida o cambio de mensajes.
a3 .Desastres y siniestros
a4 .Pérdida de privacia.
a5 .Extravio/robo.
a6 .Confiabilidad (tiempo de funcionamiento).
a7 .Reparación y rearranque.
a8 .Manejo de errores.
a9 .Validación y verificación de datos.

PULSE ENTER PARA CONTINUAR

2) COMPONENTES GRALES DE UNA RED DE COMUNICACION DE DATOS

c1 .Computadora principal.
c2 .Software.
c3 .Procesador de comunicación de entrada.
c4 .Multiplexor, concentrador, conmutador.
c5 .Circuitos (lineas) de comunicación.
c6 .Linea de abonado (local).
c7 .Modem.
c8 .Personal.
c9 .Terminales/inteligencia distribuida.

PULSE ENTER PARA CONTINUAR

En la matriz siguiente, encontrará usted los códigos correspondientes a cada una de las amenazas generales (PARTE SUPERIOR DE LA MATRIZ). Así mismo, en el eje vertical izquierdo de la matriz, podrá leer los códigos de cada componente de la red.

PULSE ENTER PARA CONTINUAR

PARA LLENAR LA MATRIZ

El último paso en el diseño de una matriz de controles para una red de comunicación de datos especifica es evaluar la idoneidad de los controles. Esto se logra revisando cada subconjunto de controles según se relaciona con dada área de amenaza y de componente de la matriz. Por ejemplo, se evalúa el subcon junto de controles que constituye una columna abajo de una amenaza. El objetivo de este paso es responder la pregunta especifica "se tienen los controles especificos y son adecuados con respecto a cada amenaza especifica?".

De acuerdo al número de controles, de cada componente y cada amenaza, usted colocará dicho número en la martriz

PULSE ENTER PARA CONTINUAR

Este tipo de revisión también puede efectuarse para otros diferentes subconjuntos de controles. Por ejemplo, es posible evaluar subconjuntos individuales de controles según se relacionen con amenazas (columnas), componentes (filas), cuadro individuales y cuadros vacios.

El método matricial constituye una herramienta perfecta para efectuar un microanálisis de controles en una red de comunicación de datos. La matriz muestra claramente la relación entre diferentes subconjunto de controles y áreas de amenazas especificas, componentes, cuadros individuales y cuadros vacios.

PULSE ENTER PARA CONTINUAR

Algunas casillas individuales pueden ser de especial interes para una red o compañia; y por lo tanto tales casillas se deben revisar con cuidado.

Las casillas vacias significan falta de control, lo que puede ser un serio problema

Proceda a llenar la matriz

PULSE ENTER PARA CONTINUAR

	a1	a2	a3	a4	a5	a6	a7	a8	a9
c1						11			
c2	10		15	12	12	12	15		
c3	10	10	10	10			10	10	10
c4	10	10	10			10	10	10	10
c5	10	10	10	10	10	10	10	10	10
c6	10	10	10	10	10	10	10	10	10
c7			10	10	10	10	10		
c8					10	10	10	10	
c9	10					10	10		

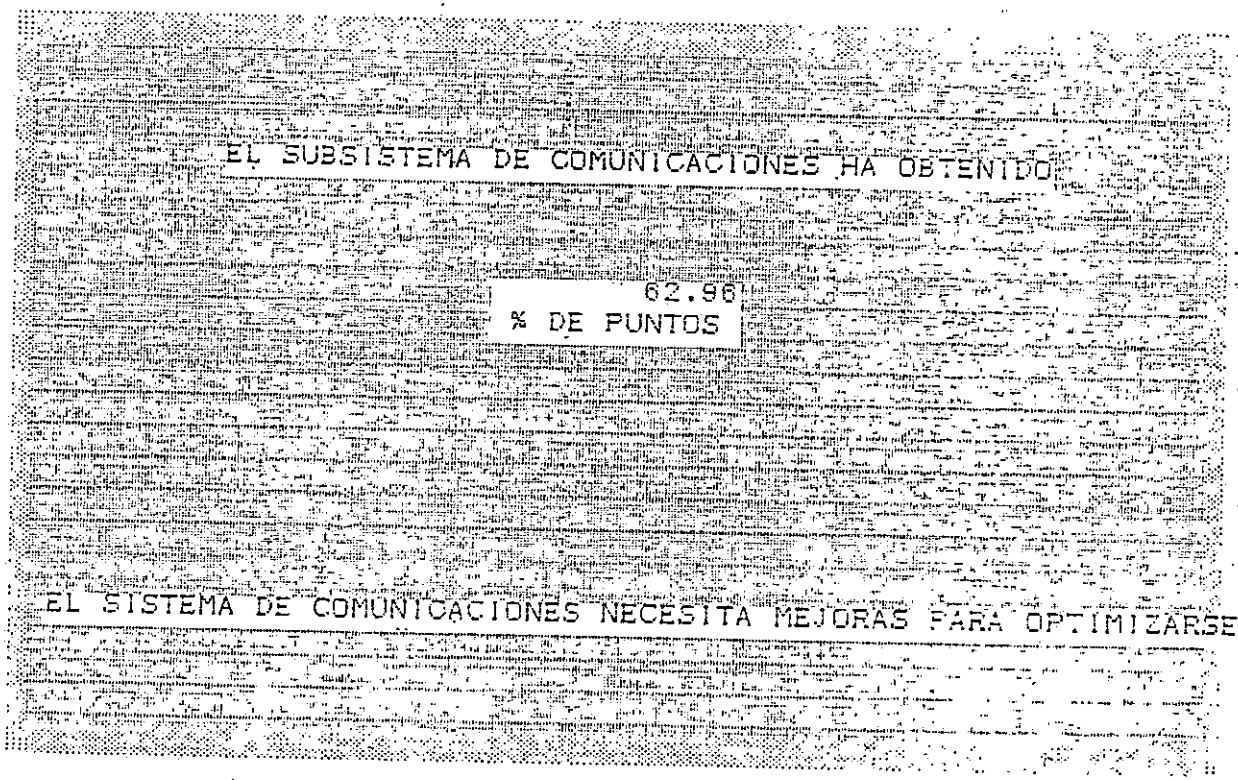
```
resultados
 el componente computador principal no esta protegido de errores y omisiones
 el componente computador principal no esta protegido de perdida de mensajes
 el componente computador principal no esta protegido de desastres,siniestros
 el componente computador principal no esta protegido de perdida de privacia
 el componente computador principal no esta protegido de extravio o robo
 el componente computador principal no esta protegido de recuperacion
 el componente computador principal no esta protegido de manejo de errores
 el componente computador principal no esta protegido de verificacion de dato
 el componente      softwarwe       no esta protegido de perdida de mensajes
 el componente      softwarwe       no esta protegido de manejo de errores
 el componente      softwarwe       no esta protegido de verificacion de dato
 el componente procesadores de Comm no esta protegido de extravio o robo
 el componente procesadores de Comm no esta protegido de confiabilidad
 el componente      multiplexores   no esta protegido de perdida de privacia
 el componente      multiplexores   no esta protegido de extravio o robo
 el componente      modems          no esta protegido de errores y omisiones
 el componente      modems          no esta protegido de perdida de mensajes
 el componente      modems          no esta protegido de manejo de errores
```

pulse [enter] para continuar

continuacion de resultados

el componente	modems	no esta protegido de verificacion de dato
el componente	Personal	no esta protegido de errores y omisiones
el componente	Personal	no esta protegido de perdida de mensajes
el componente	Personal	no esta protegido de desastres,siniestros
el componente	Personal	no esta protegido de perdida de privacia
el componente	Personal	no esta protegido de verificacion de dato
el componente	Terminales	no esta protegido de perdida de mensajes
el componente	Terminales	no esta protegido de desastres,siniestros
el componente	Terminales	no esta protegido de perdida de privacia
el componente	Terminales	no esta protegido de extravio o robo
el componente	Terminales	no esta protegido de manejo de errores
el componente	Terminales	no esta protegido de verificacion de dato

pulse [enter] para continuar



pulse cualquier tecla para regresar al menú anterior

BIBLIOGRAFÍA

LIBROS:

- Jerry FitzGerald, Comunicación de datos en los negocios, Editorial Limusa/Grupo noriega editores. Primera edición 1992.

- David Kruglinsky, Sistemas de Administración de bases de datos, Osborne/Mc. Graw-Hill. 1986.

- Watne, Donald y Turney, Peter, Auditing E.D.P. systems. Prentice Hall. 1a. edición.

- Wilson, Warren E., Conceptos sobre ingeniería de sistemas, Editorial Limusa. 1987.

- Seen, James a., Sistemas de información para la administración. Editorial Iberoamericana. 1988.

- Holmes, Artur W., Principios básicos de auditoría. Editorial CECSA. 1979.

- Rosen, R. y otros, Procedimientos de auditoría en computación.

- Davis, Gordon B., La auditoría y el procesamiento electrónico de información.

- Hernández Jiménez, Ricardo., El alma de la computadora.

- Mullen, Jack B., The practioner's guide to E.D.P. auditing. New York Institute of Finance.

- Harper, Stanley; O'neil-Dunne, Jarlath & Xenia Ley Parker, Handbook of E.D.P. auditing systems. F.I.U. Miami University, E.E.U.U.

- Instituto Mexicano de Contadores Públicos, Guía para la auditoría computarizada.

- Davis, Gordon B. & Olson, Margareth, Sistemas de Información Gerencial. Mc Graw Hill.

TESIS:

- Campos García, josé Luis. Los sistemas de procesamiento electrónico de datos y la evaluación del control interno. Escuela de Ingeniería Industrial. U.C.A.

ARTÍCULOS:

- Outerial, Luis Eduardo. Guía para la auditoría operativa de los sistemas de computación de datos. Administración de Empresas. Argentina,

- Delpeiro, Oswaldo H. La auditoría del centro de cómputo. Administración de Empresas. Argentina.

- Nardelli, Jorge R. Evaluación del control interno en un centro de cómputos. Administración de Empresas. Argentina.

- Perry-Warner. Sistemas de procesamiento electrónico: su contabilidad y mecanismos de seguridad. Administración de Empresas. Argentina.

OTROS

- Seminario "Auditoría y control en procesamiento de datos" impartido por GBM de El Salvador.

- Arévalo Rojas, Mario Arturo. Aplicación de sistemas expertos para el diagnóstico de fallas en el computador. Escuela de Ingeniería Eléctrica. U.C.A.

- Recinos, Cecilia. Texto de auditoría de sistemas. Licenciatura en computación. U.C.A.