UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

GUIA PARA EL DESARROLLO DE UNA AUDITORIA EN INFORMATICA

SEMINARIO DE INVESTIGACION
I N F O R M A T I C A

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN INFORMATICA
P R E S E N T A N
JESUS GARCIA PEREZ
CARLOS FRANCISCO MENDEZ CRUZ

ASESOR DEL SEMINARIO: C.P. Y L.A. JOSE ANTONIO ECHENIQUE GARCIA

MEXICO, D. F. **1997**

Agradecimientos

A la Universidad Nacional Autónoma de México por brindarme la oportunidad de desarrollarme profesionalmente.

A la Facultad de Contaduría y Administración por brindarme sus instalaciones para realizar una de mis metas.

A mi asesor C.P. y L.A. José Antonio Echenique García por brindarme su apoyo y colaboración para la elaboración del presente trabajo.

A mis profesores de la carrera por sus consejos y comentarios pero sobre todo, por compartir sus conocimientos conmigo.

A Adriana por su valiosa colaboración.

A Carlos por compartir este trabajo conmigo.

GRACIAS

Jesús

Agradecimientos

A la Universidad Nacional Autónoma de México por brindarme la oportunidad de desarrollarme profesionalmente.

A la Facultad de Contaduría y Administración por brindarme sus instalaciones para realizar una de mis metas.

A mi asesor C.P. y L.A. José Antonio Echenique García por brindarme su apoyo y colaboración para la elaboración del presente trabajo.

A mis profesores de la carrera por sus consejos y comentarios pero sobre todo, por compartir sus conocimientos conmigo.

A Adriana por su valiosa colaboración.

A Carlos por compartir este trabajo conmigo.

GRACIAS

Jesús

Dedicatorias

Con cariño y admiración:

A Dios por darme la vida.

A María de Jesús y Jesús por brindarme los momentos más felices de mi vida y por ser un excelente ejemplo para seguir adelante. Los amo.

A Mario, Pepe, Alicia, Agueda, Erika, Israel, Ana, Mireya, Gustavo, Mary, Mario Alberto, Mariana, Katya, Víctor Hugo y Frida, por estar siempre juntos y apoyarnos en todo momento. Los quiero mucho.

A Adriana por compartir los momentos más hermosos de mi vida. Gracias por tu amor, apoyo y comprensión. Te amo.

Jesús

CARLOS

DEDICATORIAS

Es imposible para mí dedicar a una sola persona este trabajo, ya que significa el cierre a cinco años de esfuerzo y dedicación a mi carrera y el primer paso para dejar atrás toda una época escolar que durante años llevé conmigo.

Dedico entonces mi trabajo a las siguientes personas que de alguna manera han logrado que siga viajando en el camino de mi vida:

A mis Padres, por el entusiasmo que han puesto en mí desde que nací, por sus preocupaciones, apoyo, esfuerzos y cada acto que de la manera mas desprendida han hecho por mí, los amo y estoy orgullosos de ambos.

A mis Hermanos Daniel, Gerardo, Rafael, Socorro y Beatriz, que hacen de mi vida cotidiana un gran esfuerzo de vida feliz.

A la Persona que ha compartido innumerables y hermosos momentos junto a mí durante la carrera y quien logró que mi recorrido en la facultad tuviera un sentido verdaderamente humano. A Marcela Fernández Izaguirre la persona mas linda que he conocido en mi vida.

A mi Tío, Hector Méndez Mejía, por el apoyo incondicional que me ha dado, por mi anillo de graduación y por la preocupación que ha puesto en mi familia.

A mis Amigos, las personas que lograron que de verdad disfrutara mi estancia en la Universidad.

CARLOS

GRACIAS A:

A la Universidad Nacional Autónoma de México, por dar vida útil a cinco años de mi crecimiento y por el maravilloso universo de recursos y situaciones que me brindo a diario.

A la Facultad de Contaduría y Administración, por contener en sus entrañas la carrera que me ha formado y por darme oportunidad de aprender de sus acervos, profesores y compañeros de carrera.

A mi Asesor, el C.P. y L.A. José Antonio Echenique García, Director de mi Facultad, por el apoyo y las facilidades que me brindó durante el desarrollo del presente trabajo.

A Marcela Fernández Izaguirre, por su apoyo moral y humano , sin el cual me hubiera sido imposible terminar esta tesis.

A mi compañero de tesis, Jesús García Pérez, por su esfuerzo, apoyo y amistad que lograron sacar adelante esta empresa.

A la Maestra Marina Toriz García, que despertó en mi la inquietud de conocer mas a fondo el mundo que envuelve la auditoria en informática y por sus grandes muestras de afecto y apoyo que durante el tiempo que tengo de conocerla me ha otorgado.

A los Maestros que realmente me hicieron sentir amor por lo que será mi futuro profesional, que me apoyaron y reconocieron mi potencial, a los que realmente dieron un poco de si por nosotros los alumnos y que siguen gastando sus fuerzas en mi querida Universidad.

ÍNDICE

INTRODUCCIÓN

Debido a la importancia que tiene en la actualidad la correcta toma de decisiones en las empresas, el manejo de la información ha captado un enorme interés por parte de los directivos, quienes buscan contar con la información suficiente y oportuna que les auxilie a determinar los cursos de acción más convenientes para lograr sus objetivos.

Lo anterior es solamente uno de los motivos que ha causado el elevado desarrollo tecnológico de las herramientas para el tratamiento de la información, concretamente de las computadoras.

El volumen de datos que se procesan actualmente en las organizaciones es muy diverso y puede variar por ejemplo, desde la modificación de los expedientes de los pacientes de un consultorio médico, hasta la actualización de las grandes bases de datos de un banco o una casa de bolsa. Así mismo, la tecnología del presente permite que dichas actualizaciones se realicen inclusive desde lugares distantes y a velocidades de tiempo real.

Por lo anterior, y para vigilar el grado de cumplimiento de políticas y procedimientos orientados al aseguramiento y uso de los recursos informáticos y de la seguridad, integridad y oportunidad de la información de la empresa, ha surgido la Auditoría en Informática, tema central de nuestra investigación.

Los motivos que nos llevaron a la elección de este tema son 3 principalmente: el papel tan importante que juega la auditoría en informática dentro de las organizaciones, lo conocedor y completo que puede llegar a ser un auditor en informática y, principalmente, la falta de divulgación que, desde nuestro particular punto de vista, existe de este tema.

Por tanto la presente tesis pretende ser un instrumento que sirva, principalmente, al profesional inexperto (auditor interno o externo), como una guía para el desarrollo de una auditoría en informática y, como lectura complementaria, al estudiante interesado en el tema.

La hemos dividido en cinco capítulos, durante los cuales mencionamos al centro de cómputo o área de informática, refiriéndonos al lugar en donde se centraliza o administra el proceso electrónico de los datos.

El primer capítulo trata sobre los conceptos generales que consideramos como necesarios para la mejor comprensión de nuestra investigación, tales como: auditoría, informática, centro de cómputo y seguridad. En el segundo capítulo nos adentramos a lo que es la auditoría en informática, sus antecedentes, sus diferentes concepciones, objetivos, técnicas, perfiles, software de apoyo y problemática. El tercer capítulo trata sobre las posibles áreas de revisión dentro de la empresa: administración de informática, dirección y niveles ejecutivos, usuarios de informática, control interno, ciclo de desarrollo e implantación de sistemas, sistemas de información, mantenimiento, redes locales y telecomunicaciones, hardware, software, seguridad, planeación de informática e investigación tecnológica. En el capítulo cuarto tratamos la metodología de la auditoría en informática y explicamos sus diferentes etapas. El capítulo quinto lo reservamos para la etapa de desarrollo donde exponemos los programas de trabajo por cada área susceptible de revisión.

OBJETIVO

Esta tesis tiene como objetivo el implementar una guía que sirva como herramienta al auditor en informática, en la revisión de los controles internos establecidos en el Área de Informática.

CAPÍTULO 1

Conceptos Generales

1.1. AUDITORÍA

1.1.1. ANTECEDENTES

Aún cuando los objetivos y conceptos que rigen a la auditoría en nuestros días eran totalmente desconocidos en la antigüedad, éstas han sido realizadas durante el transcurso de la historia con fines muy específicos, principalmente en asuntos de gobierno y comercio. Los historiadores creen que los registros contables tuvieron su origen alrededor del año 4000 a.C., cuando las antiguas civilizaciones del Cercano Oriente comenzaron a establecer gobiernos y comercios organizados. Desde el principio los gobiernos se preocuparon por llevar cuenta de las entradas y salidas de dinero y el cobro de impuestos.

En la Gran Bretaña, considerada como la cuna de la auditoría, las primeras auditorías eran de dos tipos. Las de las ciudades y poblaciones eran realizadas públicamente ante los funcionarios del gobierno y los ciudadanos y consistían en que los auditores oyeran la lectura de las cuentas hechas por el tesorero. Hacia finales del siglo XVI, los auditores de las ciudades marcaban las cuentas con frases tales como "oída por los auditores firmantes". El segundo tipo de auditoría implicaba un examen detallado de las cuentas que llevaban los funcionarios de finanzas de los grandes señoríos, seguido por una declaración de auditoría, es decir, un informe verbal ante el Señor del lugar y el Consejo. Estas auditorías no tenían por objeto probar la calidad de las cuentas, salvo que se detectara algún tipo de fraude.

A partir de la Edad Media, y a través de la Revolución Industrial, las auditorías fueron practicadas con el objeto de determinar si las personas que tenían alguna responsabilidad fiscal en el gobierno y en el comercio, estaban actuando y proporcionando informes honestamente. A medida que las industrias crecían durante la Revolución Industrial, los propietarios de dichas industrias se vieron en la necesidad de contratar a personas que ocuparan puestos con un alto grado de responsabilidad y, por consiguiente, fueron acudiendo, con frecuencia cada vez mayor, a los auditores para protegerse del peligro de fraude o robo por parte de funcionarios o empleados.

La auditoría comenzó a evolucionar desde un proceso auditivo hasta el examen riguroso de los registros escritos y la prueba de la evidencia de apoyo. A finales del siglo XVII se promulgó la primera ley (en Escocia) que prohibía que ciertos funcionarios actuaran como auditores de una ciudad, con lo que se introdujo el concepto de independencia del auditor.

El crecimiento de las empresas durante la Revolución Industrial y después de ella, estaba acompañada por un avance en los sistemas de contabilidad. Las sociedades anónimas se convirtieron en la forma predominante de organización, los administradores profesionales sustituyeron a los propietarios individuales, los sistemas de contabilidad fueron mejorados y estandarizados y los accionistas de las compañías tomaron conciencia de una adecuada protección de sus intereses a través de una auditoría independiente. De esta manera, fue reconocida la necesidad de un sistema de contabilidad sistemático y un programa de auditoría razonablemente completo, que auxiliaran en la prevención de fraudes y la obtención de información financiera digna de confianza.

Pese al progreso en la práctica de la auditoría, no fue sino hasta el siglo XIX, que trajo consigo la construcción de ferrocarriles y el crecimiento de las compañías de seguros, los bancos y otras empresas a base de acciones, cuando el auditor profesional se convirtió en parte importante del escenario empresarial.

1.1.2. CONCEPTO

En Cuba, durante el evento internacional "Informática 96" en la conferencia "Técnicas de la Microcomputación en la Auditoría", se define que: "La auditoría constituye una de las formas fundamentales de control de la gestión administrativa y consiste en el examen de las operaciones contables y financieras y de la aplicación de las disposiciones administrativas y legales que correspondan, con la finalidad de mejorar el control y grado de eficiencia en la utilización de los recursos, prevenir el uso indebido de éstos, fortalecer la disciplina de las entidades y coadyuvar al

1.1. AUDITORÍA

1.1.1. ANTECEDENTES

Aún cuando los objetivos y conceptos que rigen a la auditoría en nuestros días eran totalmente desconocidos en la antigüedad, éstas han sido realizadas durante el transcurso de la historia con fines muy específicos, principalmente en asuntos de gobierno y comercio. Los historiadores creen que los registros contables tuvieron su origen alrededor del año 4000 a.C., cuando las antiguas civilizaciones del Cercano Oriente comenzaron a establecer gobiernos y comercios organizados. Desde el principio los gobiernos se preocuparon por llevar cuenta de las entradas y salidas de dinero y el cobro de impuestos.

En la Gran Bretaña, considerada como la cuna de la auditoría, las primeras auditorías eran de dos tipos. Las de las ciudades y poblaciones eran realizadas públicamente ante los funcionarios del gobierno y los ciudadanos y consistían en que los auditores oyeran la lectura de las cuentas hechas por el tesorero. Hacia finales del siglo XVI, los auditores de las ciudades marcaban las cuentas con frases tales como "oída por los auditores firmantes". El segundo tipo de auditoría implicaba un examen detallado de las cuentas que llevaban los funcionarios de finanzas de los grandes señoríos, seguido por una declaración de auditoría, es decir, un informe verbal ante el Señor del lugar y el Consejo. Estas auditorías no tenían por objeto probar la calidad de las cuentas, salvo que se detectara algún tipo de fraude.

A partir de la Edad Media, y a través de la Revolución Industrial, las auditorías fueron practicadas con el objeto de determinar si las personas que tenían alguna responsabilidad fiscal en el gobierno y en el comercio, estaban actuando y proporcionando informes honestamente. A medida que las industrias crecían durante la Revolución Industrial, los propietarios de dichas industrias se vieron en la necesidad de contratar a personas que ocuparan puestos con un alto grado de responsabilidad y, por consiguiente, fueron acudiendo, con frecuencia cada vez mayor, a los auditores para protegerse del peligro de fraude o robo por parte de funcionarios o empleados.

La auditoría comenzó a evolucionar desde un proceso auditivo hasta el examen riguroso de los registros escritos y la prueba de la evidencia de apoyo. A finales del siglo XVII se promulgó la primera ley (en Escocia) que prohibía que ciertos funcionarios actuaran como auditores de una ciudad, con lo que se introdujo el concepto de independencia del auditor.

El crecimiento de las empresas durante la Revolución Industrial y después de ella, estaba acompañada por un avance en los sistemas de contabilidad. Las sociedades anónimas se convirtieron en la forma predominante de organización, los administradores profesionales sustituyeron a los propietarios individuales, los sistemas de contabilidad fueron mejorados y estandarizados y los accionistas de las compañías tomaron conciencia de una adecuada protección de sus intereses a través de una auditoría independiente. De esta manera, fue reconocida la necesidad de un sistema de contabilidad sistemático y un programa de auditoría razonablemente completo, que auxiliaran en la prevención de fraudes y la obtención de información financiera digna de confianza.

Pese al progreso en la práctica de la auditoría, no fue sino hasta el siglo XIX, que trajo consigo la construcción de ferrocarriles y el crecimiento de las compañías de seguros, los bancos y otras empresas a base de acciones, cuando el auditor profesional se convirtió en parte importante del escenario empresarial.

1.1.2. CONCEPTO

En Cuba, durante el evento internacional "Informatica 96" en la conferencia "Tecnicas de la Microcomputación en la Auditoría", se define que: "La auditoría constituye una de las formas fundamentales de control de la gestión administrativa y consiste en el examen de las operaciones contables y financieras y de la aplicación de las disposiciones administrativas y legales que correspondan, con la finalidad de mejorar el control y grado de eficiencia en la utilización de los recursos, prevenir el uso indebido de éstos, fortalecer la disciplina de las entidades y coadyuvar al

mantenimiento de la honestidad administrativa y a la preservación de la integridad moral de los trabajadores"[1].

El Comité especial del Instituto Americano de Contadores determina que auditoría "es el examen de los libros de contabilidad, comprobantes y demás registros de un organismo público, institución, corporación, firma o persona, o de alguna o algunas personas situadas en destino de confianza con el objeto de averiguar la corrección o incorrección de los registros y expresar opinión sobre los documentos suministrados, comúnmente en forma de un certificado"[2].

Andrés Montero señala que auditoría "es el examen metódico y ordenado de la contabilidad de una empresa, mediante la comprobación de las operaciones registradas y la investigación de todos aquellos hechos que puedan tener relación con las mismas, a fin de determinar su corrección"[3].

Montgomery dice que la auditoría "es un examen sistemático de los libros y registros de un negocio u otra organización con el fin de determinar o verificar los hechos relativos a las operaciones financieras y los resultados de éstas para informar sobre los mismos"[4].

Víctor Manuel Mendivil E. señala que "auditoría es la actividad por la cual se verifica la corrección contable de las cifras de los estados financieros; es la revisión misma de los registros y fuentes de contabilidad para determinar la razonabilidad de las cifras que muestran los estados financieros emanados de ellos"[5].

De las definiciones expuestas tomamos los elementos más importantes para conformar el siguiente concepto que tomamos como referencia para el desarrollo de la presente investigación:

La auditoría es el examen detallado de las operaciones contables-financieras y de la práctica de las políticas, normas, procedimientos y leyes que en su caso se den, logrando así mejorar el control y grado de eficiencia en la aplicación y administración de los recursos.

1.1.3. CLASIFICACIÓN DE LA AUDITORIA

El campo de acción del auditor puede ser muy amplio o restringido a determinados fines, según instrucciones recibidas de sus clientes o mandantes. Esto da origen a distintos tipos de auditoría. La auditoría se puede clasificar tomando en consideración:

- El alcance de la auditoría
- La época o período que abarca
- La persona que la realiza
- La finalidad del trabajo que será auditado

El alcance y la finalidad del trabajo a desarrollar

Auditoría de balance o de estados financieros

Es aquella que se realiza a base de pruebas selectivas y trata de determinar, exclusivamente la corrección de los saldos.

Auditoría detallada o de movimientos

Es aquella que se lleva a cabo mediante la revisión de todos y cada uno de los movimientos operados en la contabilidad en un ejercicio a fin de establecer su corrección o incorrección, pero sin llegar a determinar saldos, únicamente la revisión de los movimientos.

Esta clase de auditoría está en desuso, ya que a pocas personas les interesa conocer los movimientos sin determinar saldos, siendo además, muy tardado y costosa.

---

[1] Evento Internacional "Informática 95" La Habana Cuba Conferencia "Técnicas de la Microcomputación en la Auditoría".
[2] Defliese, Philip L., Auditoría Montgomery Capítulo 3
[3] Sánchez Alarcón, Fco. Javier. Programas de Auditoría Capítulo 2
[4] Defliese, Philip L., Auditoría Montgomery Capítulo 3
[5] Mendivil Escalante, Víctor Manuel, Elementos de Auditoría Capítulo 2

Auditoria exhaustiva

Es una combinación de las dos anteriores y consiste en la revisión de todos y cada uno de los movimientos operados en la contabilidad y en la determinación de los saldos.

Auditoria especial

Se efectúa a una cuenta o a un grupo de cuentas en particular. Este tipo de auditoria se puede efectuar a base de pruebas selectivas o en forma detallada. Algunos autores suelen llamarla concretamente con el nombre de la cuenta que se está auditando (auditoria de inventario, auditoria de caja, auditoria de compras, etc.).

La época o el periodo que abarca.

Auditoria continua o permanente

Se realiza constante o continuamente, pudiendo efectuarse antes o después de registrar las operaciones en los libros. Es continua, porque normalmente en las empresas que la realizan, se cuenta con un auditor interno que revisa las operaciones antes o después de que sean registradas en los libros.

Auditoria esporádica o eventual

Se efectúa en forma ocasional, de acuerdo con las necesidades de los directivos de la empresa, por lo que no tiene un periodo definido.

Auditoria periódica

Se efectúa en periodos claramente definidos o determinados (cada mes, cada seis meses, cada año, etc.)

La persona que la realiza

Auditoria Interna

La efectua una persona que depende directamente de la empresa.

Auditoria Externa

Es la que realiza un contador publico como profesional independiente, teniendo la libertad de poder emitir su opinión sin ningún tipo de influencia.

La finalidad del trabajo que será auditado.

Auditoria Administrativa

La auditoria puede estar enfocada a la gestión de los negocios de la empresa, tanto en lo referente a su actividad esencial (agricola, industrial, comercial, etc.) como al manejo mismo de dicha actividad. Si tal es el caso, el auditor deberá contar con los conocimientos y con la experiencia suficientes para juzgar acerca de la eficiencia de los administradores al manejarla. Por tal motivo, con frecuencia, la auditoria administrativa se encomienda a técnicos especializados o firmas de consultores que cuenten con especialistas cuya opinión pueda ser útil para la mejor conducción de los negocios de la empresa.

Auditoría Operativa

Esta enfocada a la revisión de la administración de los procedimientos de la empresa, es decir, a la forma en que las operaciones se realizan y acerca de las cuales se informa a la administración. Esto implica tener conocimientos de organización para el mejor aprovechamiento de los elementos materiales y humanos con que cuente la empresa y evitar así que unos y otros se desperdicien, todo con la finalidad de mejorar su rendimiento operacional, haciendo que la empresa sea más eficiente.

Auditoría Financiera

Esta orientada hacia la fiscalización de los recursos monetarios de la empresa y su adecuado manejo. Por el carácter de estas actividades, el auditor comienza por examinar el contenido de los estados financieros y profundiza su investigación al estudio del sistema de control interno como un medio para fiscalizar las operaciones practicadas durante el ejercicio sujeto a la revisión.

Auditoría en informatica

Es la verificación de los controles y procedimientos que se llevan a cabo en el área de informática a fin de saber si se están cumpliendo con las políticas y objetivos de la empresa respecto a esa área, así como aspectos de la información como seguridad, confiabilidad, integración, veracidad y oportunidad.

1.1.4. NORMAS

La Contaduría Pública organizada, a través del Instituto Mexicano de Contadores Publicos, decidió establecer los requisitos mínimos, de orden general, que deben observarse para el desempeño de un trabajo de auditoría de calidad profesional. A estos principios basicos del trabajo de auditoría se les llama "Normas de auditoría" y, por naturaleza, deben ser de aceptación general para la profesión.

Concepto

"Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de éste trabajo"[6]

Clasificación

1. Normas personales

A) Entrenamiento técnico y capacidad profesional.
B) Cuidado y diligencia profesionales.
C) Independencia mental.

2. Normas de ejecución del trabajo

A) Planeación y supervisión.
B) Estudio y evaluación del control interno.
C) Obtención de evidencia suficiente y competente.

3. Normas de información

A) Relacion con los estados financieros y responsabilidad.

[6] IMCP, Comision de Normas y Procedimientos de Auditoría. Boletín C

B) Aplicación de principios de contabilidad generalmente aceptados.
C) Consistencia en la aplicación de los principios de contabilidad.
D) Suficiencia de las declaraciones informativas[7]

Normas personales

El *entrenamiento técnico* es el medio indispensable para desarrollar la habilidad práctica necesaria para el ejercicio de una profesión y junto con el estudio y la investigación integran el fundamento de la capacidad profesional.

La actividad profesional como todas las actividades humanas, está sujeta a la apreciación y al error. El profesionista debe esforzarse por reducir a un mínimo ese grado de error mediante un trabajo con *cuidado y diligencia profesionales*.

La *independencia mental* es consecuencia de la calidad de juez o árbitro que en cierto modo tiene la actividad del auditor.

Normas de ejecución del trabajo

Mediante la *planeación* del trabajo que se desarrollará, se establece una situación que garantiza razonablemente la atención de los puntos más importantes así como la aplicación de los procedimientos mínimos para la obtención de elementos de juicio suficientes y competentes para la opinión del auditor.

El Auditor se auxilia de ayudantes para ejecutar el trabajo, esto implica delegación de funciones, misma que no lo delega de su responsabilidad total, ésta circunstancia hace necesaria la *supervisión* del trabajo para estar seguro de que su ejecución cumple con los objetivos proporcionando información completa y adecuada.

Al formular el programa de trabajo el auditor debe establecer los procedimientos, su alcance y su oportunidad, lo cual depende mucho del tipo de empresa y de sus particularidades operativas; ello hace necesario el *estudio y evaluación del control interno* existente para que basado en el resultado obtenido, se determinen claramente dichos procedimientos, su alcance y su oportunidad.

Los resultados que obtenga el auditor deben ser *suficientes y competentes*, es decir, que den *"la certeza moral de que los hechos que se están tratando de probar, o los criterios cuya corrección se está juzgando, han quedado satisfactoriamente comprobados* y se refieran *a aquellos hechos, circunstancias o criterios que realmente tienen importancia en relación con lo examinado"*[8].

Normas de información

Como consecuencia de su trabajo el auditor emite una opinión en la que expresa el trabajo desarrollado y las conclusiones a las que ha llegado. Al documento donde plasma dicha opinión se le llama dictamen y, por la importancia que este tiene, se han establecido las *normas de información* que son las normas que regulan su calidad de desarrollo.

1.1.5. PROCEDIMIENTOS

La combinación en la práctica de dos o más técnicas de auditoría da origen a los denominados Procedimientos de Auditoría. La conjugación en la práctica de dos o más procedimientos de auditoría deriva en programas de Auditoría.

Concepto

En materia de procedimientos de auditoría, el Boletín F-01 de Normas y Procedimientos de Auditoría elaborado por la Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos, establece lo siguiente:

[7] IMCP, Comisión de Normas y Procedimientos de Auditoría. Boletín C.
[8] IMCP, Comisión de Normas y Procedimientos de Auditoría. Boletines Nums. 3 y E-03.

"Los procedimientos de auditoria son el conjunto de técnicas de investigación aplicables a una partida o a un grupo de hechos y circunstancias relativas a los estados financieros sujetos a examen mediante los cuales el contador público obtiene las bases para fundamentar su opinión"[9]

Debido a que generalmente el auditor no puede obtener el conocimiento que necesita para fundar su opinión en una sola prueba, es necesario examinar cada partida o conjunto de hechos mediante varias técnicas de aplicación simultánea o sucesiva

1.1.6. TÉCNICAS

Concepto

"Las técnicas de auditoria son los métodos practicos de investigación y prueba que el Contador Público utiliza para lograr la información y comprobación necesarias para poder emitir su opinión profesional"[10]

Clasificación

La Comisión de Normas y Procedimientos de Auditoria del Instituto Mexicano de Contadores Públicos, en su boletin F-01, ha propuesto la siguiente clasificación:

- Estudio General
- Análisis
- Inspección
- Confirmacion
- Investigación
- Declaraciones o certificaciones
- Observación y
- Cálculo

Estudio General

Es la apreciacion y juicio de las caracteristicas generales de la empresa, las cuentas o las operaciones, a través de sus elementos más significativos para concluir si se ha de profundizar en su estudio y la forma en que ha de hacerse.

Análisis

Es el estudio de los componentes de un todo para concluir con base en aquéllos respecto de éste. Esta técnica se aplica concretamente al estudio de las cuentas o rubros genéricos de los estados financieros.

Inspección

Es la verificacion física de las cosas materiales en que se tradujeron las operaciones. Se aplica al estudio de las cuentas cuyos saldos tienen una representación material (efectivos, mercancías, bienes, etc.)

Confirmación

Es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operacion, en la que participó y por la cual está en condiciones de informar válidamente sobre ella

[9] IMCP, Comision de Normas y Procedimientos de Auditoria. Boletin F-01
[10] IMCP, Comisión de Normas y Procedimientos de Auditoria. Boletin F-01

Investigación

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

Declaraciones y certificaciones

Es la formalización de la técnica anterior, cuando, por su importancia, resulta conveniente que las afirmaciones recibidas deban quedar escritas (declaraciones) y en algunas ocasiones certificadas por una autoridad (certificaciones).

Observación

Es una manera de inspección, menos formal, y se aplica generalmente a operaciones para verificar como se realiza en la práctica (como se paga la nómina, como se efectúa el recuento de los inventarios, etc.).

Cálculo

Es la verificación de la corrección aritmética de aquellas cuentas u operaciones que se determinan fundamentalmente por cálculos sobre bases precisas. (Intereses pagados o cobrados, depreciaciones, etc.).

1.1.7. PAPELES DE TRABAJO

En el curso de su trabajo, el auditor necesitará examinar los libros y los documentos que amparan las operaciones registradas y deberá conservar constancia de la extensión en que practicó ese examen.

Los extractos, análisis, notas y demás constancias que el auditor utiliza para plasmar su trabajo, se conocen como cédulas y en su conjunto debidamente clasificados y ordenados, forman los papeles de trabajo.

Además de que los papeles de trabajo constituyen la prueba material del trabajo realizado por el auditor, en ellos se deja constancia de la profundidad de las pruebas y de la suficiencia de los elementos en que se apoyó la opinión.

Concepto

"Los papeles de trabajo son los documentos en que el auditor registra los datos e informaciones obtenidas en su examen y los resultados de las pruebas realizadas"[11].

Los papeles de trabajo son propiedad del auditor, ya que él los preparó y son la prueba de su trabajo, sin embargo, esta propiedad no es "irrestricta" debido a que como contienen datos confidenciales, el auditor está obligado a mantener una discreción absoluta respecto a la información que contienen.

Clasificación

La clasificación de los papeles de trabajo puede ser, como lo menciona Mendivil Escalante, desde dos puntos de vista:

Por su uso:

a) Papeles de uso continuo;
b) Papeles de uso temporal;

[11] IMCP, Comisión de Normas y Procedimientos de Auditoría. Boletín B

Los papeles de trabajo pueden contener información útil para varios ejercicios (acta constitutiva, cuadros de organización, catálogos de cuentas, etc.). Por tener un uso continuo o permanente, a éste tipo de papeles de trabajo se les conserva en un expediente particular, especialmente cuando el trabajo del auditor es requerido por varios ejercicios contables.

También los papeles de trabajo pueden contener información útil para un ejercicio solamente (confirmaciones a una fecha dada, contratos a plazo fijo menor de un año, etc.). Dichos papeles se agrupan en un legajo para integrar un expediente de la auditoría del ejercicio que se trate.

Por su contenido:

a) Hoja de trabajo, es la cedula que muestra los grupos o rubros que integran los estados financieros.
b) Cédulas sumarias o de resumen; muestran las cuentas de Mayor que forman un rubro.
c) Cédulas de detalle o descriptivas, relacionan las partidas que componen una cuenta de Mayor o un saldo cualquiera.
d) Cédulas analíticas o de comprobación, contienen el trabajo efectuado para verificar la corrección de una partida u operación.

Elementos de los papeles de trabajo

De acuerdo al uso que se les vaya a dar, los papeles de trabajo pueden ser muy variados en su diseño y contenido, pero por lo general casi siempre contienen los siguientes *elementos* que los auxilian para que sean claros y concisos respecto de las operaciones a que se refieran, del trabajo que se está desarrollando y de las conclusiones a las que se llega:

- Nombre de la empresa a que se refieren
- Fecha del cierre del ejercicio examinado
- Título o descripción breve de su contenido
- Fecha en que se preparó
- Fuente de donde se obtuvieron los datos
- Descripción concisa del trabajo efectuado
- Conclusión

Índices

Los papeles de trabajo se marcan con un índice para facilitar su localización. Estas marcas son índices que indican claramente la sección del expediente donde deben ser archivados y donde podrán ser localizados posteriormente.

Índices cruzados

En ocasiones, existen ciertas cédulas en las que es necesario hacer referencia respecto de las cifras que aparecen en otra u otras cédulas, relacionando así, los dos aspectos de alguna operación. A éstas referencias, hechas recíprocamente en dos o más cédulas, se les llama *índices cruzados*.

La finalidad que se persigue con los índices cruzados, es la de lograr el mayor número posible de confirmaciones, "siguiendo la pista" de ciertas cifras dentro de los papeles de trabajo.

Marcas en los papeles de trabajo

Para facilitar la transcripción e interpretación del trabajo realizado en la auditoría, se acostumbra usar *marcas* que permiten transcribir de manera práctica y de fácil lectura algunos trabajos repetitivos.

La utilización de marcas de trabajo facilita la transcripción del trabajo que realiza el auditor y la interpretación de dicho trabajo por parte del supervisor que revisa

En ocasiones se puede llegar a definir ciertos trabajos repetitivos y, para los cuales se suele establecer una marca estándar que signifique lo mismo aún cuando se utilice en muy distintos papeles de trabajo. Lo anterior, acelera grandemente el proceso de ejecución del trabajo y la supervisión del mismo.

Algunos de los trabajos repetitivos más comunes y que pueden ser estandarizados a través de una marca estándar son los siguientes:

- Sumas, multiplicaciones y demás cálculos aritméticos verificados y encontrados correctos.
- Cifra encontrada contra el auxiliar y encontrada correcta
- Cifra cotejada contra el libro Mayor y encontrada correcta
- Verificación física realizada con resultados satisfactorios.
- Documento original verificado y encontrado correcto y con requisitos fiscales
- Operación o documento encontrado con la autorización adecuada.

La forma de las marcas debe ser distintiva y de lo más sencilla posible de manera que no pueda existir confusión con las demás marcas, así mismo, para lograr la distinción o identificación inmediata de las marcas, es recomendable utilizar color rojo o azul.

1.1.8. CONTROL INTERNO

Concepto

"El control interno de un negocio es el sistema de su organización, los procedimientos que tiene implantados y el personal con que cuenta estructurados en un todo para lograr tres objetivos fundamentales: a) la obtención de información financiera veraz, confiable y oportuna b) la protección de los activos de la empresa, y c) la promoción de la eficiencia en la operación del negocio"[12].

Otra definición de control interno es "el conjunto de políticas, procedimientos, normas, etc. que establece la dirección de una empresa con el fin de llevar a cabo sus actividades de manera ordenada y eficiente, salvaguardando los activos y asegurando la completitud y fiabilidad de sus registros"[13]

En el ámbito informático, el sistema de control interno pretende asegurar "la adecuación de la gestión de los activos informáticos y la fiabilidad de las actividades de los sistemas de información", MENKUS (1990)

Objetivos de control interno

Debe garantizar la obtención de información financiera correcta y segura ya que la información es un elemento fundamental en la marcha de las empresas pues con base en ella se toman las decisiones y se formulan los programas de acción.

Debe garantizar la protección de los activos, ya que éstos son los que permiten desarrollar la actividad principal de la entidad

Debe promover la eficiencia de operación complementando las labores de los individuos sin duplicarlas y haciendo expeditos de los trámites y el servicio.

Lograr que en la ejecución de las operaciones se cumplan las políticas establecidas por los administradores.

---

[12] IMCP, Comisión de Normas y Procedimientos de Auditoría. Boletín E-02

[13] Evento Internacional "Informática 96", La Habana Cuba. Conferencia "Técnicas de la Microcomputación en la Auditoría"

Evaluación del control interno

Antes de iniciar cualquier trabajo de auditoría es necesario evaluar la eficacia del sistema de control interno existente y comprobar que dicho sistema, siendo eficaz, se aplique sin alteraciones. La evaluación del control interno consta de dos fases: la investigación con los funcionarios y empleados y el estudio real de la operación para ver si efectivamente responde a lo marcado con la investigación anterior. Por lo anterior, el auditor puede realizar sus investigaciones redactando memoranda descriptiva de los procedimientos usados en cada departamento, formulando gráficas o elaborando cuestionarios, siendo éstos los métodos para efectuar el estudio del control interno de la empresa:

Método descriptivo

Consiste en la explicación, por escrito, de las rutinas establecidas para la ejecución de las distintas operaciones o aspectos específicos del control interno, es decir, es la formulación de memoranda donde se transcribe en forma fluida los distintos pasos de un aspecto operativo.

Método gráfico

Tiene como base la esquematización de las operaciones mediante el empleo de dibujos (flechas, cuadros, figuras geométricas, etc.) que representan a los departamentos, formas, archivos etc. y por medio de ellos se indican y explican el flujo de las operaciones.

Método de cuestionarios

En éste método se elabora previamente una relación de preguntas sobre los aspectos básicos de la operación a investigar y a continuación se procede a obtener las respuestas a dichas preguntas. Estas preguntas se formulan de tal suerte que una respuesta negativa advierta debilidades en el control interno y cuando es necesario, deben incluirse explicaciones más amplias que enriquezcan las respuestas.

Resulta más conveniente el empleo mixto de los tres métodos ya que de éste modo se logran resultados más completos y se soportan mejor las conclusiones.

1.1.9. DICTAMEN

Concepto

Siendo el propósito primordial de la mayoría de las auditorías, posibilitar al contador independiente a que se forme una opinión acerca de lo razonable de los estados financieros de la empresa por la cual fue contratado, es indispensable plasmar por escrito dicha opinión. El documento que se utiliza para tal motivo es el Dictamen de Auditoría.

Se ha establecido un lenguaje uniforme para el dictamen del auditor sobre los resultados de una auditoría practicada con el fin de determinar el grado en que los estados financieros se ajustan a los principios de contabilidad generalmente aceptados. A continuación se presenta un Dictamen del Auditor que es un ejemplo del estándar.

"Dictamen de contadores públicos independientes

Al consejo de administración y a los accionistas
de la American Brands, Inc

Hemos examinado el balance consolidado de American Brands, Inc. y sus subsidiarias al 31 de diciembre de 1985 y de 1984, así como los correspondientes estados consolidados de resultados, de utilidades retenidas y de cambios en la situación financiera por los años que terminaron el 31 de diciembre de 1985, de 1984 y de 1983. *Nuestros exámenes se llevaron a cabo de acuerdo con las normas de auditoría generalmente aceptadas e incluyeron por tanto las pruebas de los registros contables y otros procedimientos de auditoría que consideramos necesarios según las circunstancias.*

En nuestra opinión, los estados financieros antes mencionados presentan razonablemente la situación financiera consolidada de American Brands, Inc. y sus subsidiarias al 31 de diciembre de 1985 y de 1984 así

Evaluación del control interno

Antes de iniciar cualquier trabajo de auditoría es necesario evaluar la eficacia del sistema de control interno existente y comprobar que dicho sistema, siendo eficaz, se aplique sin alteraciones. La evaluación del control interno consta de dos fases: la investigación con los funcionarios y empleados y el estudio real de la operación para ver si efectivamente responde a lo marcado con la investigación anterior. Por lo anterior, el auditor puede realizar sus investigaciones redactando memoranda descriptiva de los procedimientos usados en cada departamento, formulando gráficas o elaborando cuestionarios, siendo éstos los métodos para efectuar el estudio del control interno de la empresa:

Método descriptivo

Consiste en la explicación, por escrito, de las rutinas establecidas para la ejecución de las distintas operaciones o aspectos específicos del control interno, es decir, es la formulación de memoranda donde se transcribe en forma fluida los distintos pasos de un aspecto operativo.

Método gráfico

Tiene como base la esquematización de las operaciones mediante el empleo de dibujos (flechas, cuadros, figuras geométricas, etc.) que representan a los departamentos, formas, archivos etc, y por medio de ellos se indican y explican el flujo de las operaciones.

Método de cuestionarios

En éste método se elabora previamente una relación de preguntas sobre los aspectos básicos de la operación a investigar y a continuación se procede a obtener las respuestas a dichas preguntas. Estas preguntas se formulan de tal suerte que una respuesta negativa advierta debilidades en el control interno y cuando es necesario, deben incluirse explicaciones más amplias que enriquezcan las respuestas.

Resulta más conveniente el empleo mixto de los tres metodos ya que de éste modo se logran resultados más completos y se soportan mejor las conclusiones

1.1.9. DICTAMEN

Concepto

Siendo el propósito primordial de la mayoría de las auditorías, posibilitar al contador independiente a que se forme una opinion acerca de lo razonable de los estados financieros de la empresa por la cual fue contratado, es indispensable plasmar por escrito dicha opinión. El documento que se utiliza para tal motivo es el Dictamen de Auditoría.

Se ha establecido un lenguaje uniforme para el dictamen del auditor sobre los resultados de una auditoría practicada con el fin de determinar el grado en que los estados financieros se ajustan a los principios de contabilidad generalmente aceptados. A continuación se presenta un Dictamen del Auditor que es un ejemplo del estándar:

"Dictamen de contadores públicos independientes

Al consejo de administracion y a los accionistas
de la American Brands, Inc

Hemos examinado el balance consolidado de American Brands, Inc y sus subsidiarias al 31 de diciembre de 1985 y de 1984, así como los correspondientes estados consolidados de resultados, de utilidades retenidas y de cambios en la situación financiera por los años que terminaron el 31 de diciembre de 1985, de 1984 y de 1983. Nuestros exámenes se llevaron a cabo de acuerdo con las normas de auditoría generalmente aceptadas e incluyeron por tanto las pruebas de los registros contables y otros procedimientos de auditoría que consideramos necesarios segun las circunstancias.

En nuestra opinion, los estados financieros antes mencionados presentan razonablemente la situación financiera consolidada de American Brands, Inc y sus subsidiarias al 31 de diciembre de 1985 y de 1984, así

como los resultados consolidados de sus operaciones y los cambios en su situación financiera por los años que terminaron al 31 de diciembre de 1985 de 1984 y de 1983, de conformidad con los principios de contabilidad generalmente aceptados aplicados de manera uniforme

Coopers and Lybrand

Avenida de las Américas 1251
Nueva York, Nueva York 10020
3 de febrero de 1986".[14]

Título

Con frecuencia se utiliza el título "Opinión del Auditor", pero resulta menos preciso, ya que la opinión es solo una de las partes que conforman el dictamen. En ocasiones también es empleada la frase "Certificado del Auditor", que es empleada erróneamente, debido a que el auditor externa sus conclusiones como una opinión, no como una afirmación de hechos. En todo caso, son los contadores públicos profesionales o la firma de contadores publicos profesionales, y no los estados financieros, los que están certificados o legalizados para poder realizar auditorías.

Párrafo del alcance

El primer párrafo del dictamen, conocido como parrafo del alcance, se refiere a lo que se ha hecho y a la forma como se hizo. Este párrafo comunica el mensaje de que se realizó una auditoría y que se llevo a cabo de acuerdo con las normas de auditoría generalmente aceptadas aplicando las pruebas y procedimientos que el auditor consideró necesarias. El párrafo del alcance describe los estados examinados y las fechas y periodos abarcados.

Párrafo de la opinión

El segundo párrafo, conocido como parrafo de la opinión del auditor, expone las conclusiones a que el auditor llegó durante el desarrollo de la auditoría.

La conclusión a que llega el auditor en la mayoría de las auditorías de estados financieros es que los estados "presentan razonablemente .. de conformidad con los principios de contabilidad generalmente aceptados aplicados de manera uniforme"

El párrafo de la opinión presentado como ejemplo, recibe el nombre técnico de "opinión sin salvedades", es decir, que no presenta excepciones ni incertidumbres. Existen otros tipos de opiniones como son: opinión con salvedades, opinión negativa y la negación de la opinión, siendo la opinión sin salvedades, la que normalmente se espera de una auditoría.

Las palabras "presentan razonablemente" no se deben interpretar separadamente de la frase "de conformidad con los principios de contabilidad generalmente aceptados", ya que la opinión positiva del auditor acerca de la presentación razonable de conformidad con los principios de contabilidad generalmente aceptados implica la creencia de que los estados financieros poseen ciertas cualidades.

La referencia a la uniformidad la exigen las normas de auditoría generalmente aceptadas. Cuando el informe incluye sólo el periodo actual, la referencia a la uniformidad se debe expresar como "en forma consistente al año anterior"

El dictamen de auditor está dirigido a la persona o personas que lo contrataron y aún cuando el auditor percibe sus honorarios de su cliente y dirige el dictamen al consejo de administración, el dictamen será utilizado fundamentalmente por personas ajenas a la empresa, tales como bancos, inversionistas y acreedores.

---

[14] Defliese, Philip L., Auditoría Montgomery Ejemplo de Dictamen de Auditoría Capítulo 1

1.2. INFORMÁTICA

1.2.1. ANTECEDENTES

Desde hace mucho tiempo el hombre ha tratado de liberarse de los trabajos manuales y repetitivos, entre los que están las operaciones de cálculo y redacción de informes.

La palabra cálculo tiene sus orígenes en el término latino **calculus**. Se utilizaba hace miles de años para denominar a unas pequeñas piedras que por medio de unas ranuras efectuadas en el suelo se usaban para contar.

A partir de este elemento de cálculo, aparecieron en diversos lugares otros elementos similares, denominados comúnmente como **ábaco**, el cual se constituyó en el primer dispositivo manual de cálculo y que servía para representar números en el sistema decimal y realizar operaciones con ellos.

Las técnicas de cálculo se siguieron desarrollando a través de los siglos. En 1642 Blas Pascal, matemático y filosofo francés, desarrolló la primera máquina calculadora mecánica. En 1672 el matemático alemán Gottfried Von Leibniz mejoro el invento de Pascal, obteniendo la calculadora universal que podía sumar, restar, multiplicar, dividir y extraer raíces.

Ya en el siglo XIX, en el año 1801, Joseph Marie Jackuard construyó un telar automático con entrada de datos por tarjetas perforadas para controlar la confección de los tejidos y sus dibujos.

En el año de 1822, Charles Babbage, matemático inglés, d señó la máquina de diferencias con fundamentos mecánicos, basados en ruedas dentadas, para la resolución de funciones y obtención de tablas de dichas funciones. En 1833 Babbage diseñó la máquina analítica, similar a la computadora actual, pues disponía de programa, memoria, unidad de control, periféricos de entrada y periféricos de salida. La idea de su construcción surgió de la necesidad de realizar automáticamente tablas de logaritmos y funciones trigonométricas. Debido a este diseño, Babbage es considerado el padre de la Informática.

Sobre el año 1885 Herman Hollerith, funcionario de la oficina de censo de los Estados Unidos, vio como se tardaban diez años en realizar el censo anual de su país y observó que la mayoría de las preguntas del censo tenían como respuesta si o no, lo que le hizo idear en 1886 una tarjeta perforada para contener la información de las personas censadas y una máquina capaz de leer y tabular dicha información. En 1896, Hollerith fundó la empresa Tabulating Machines Company la cual se fusiono con otras empresas en 1924 para constituir la actual International Business Machines (IBM).

En 1936 Alan M. Turing, matemático inglés, desarrolló la teoría de una máquina capaz de resolver todo tipo de problemas, llegando a la construcción teórica de las maquinas de Turing. Con los estudios de Turing, se inicio la Teoría matemática de la computación, en la que se define un algoritmo como la representación formal y sistemática de un proceso.

En 1937, Howard H. Aiken de la Universidad de Harvard, desarrolla la idea de Babbage junto con científicos de su departamento e ingenieros de IBM. Como resultado de este desarrollo, construyeron la primera computadora electromecánica basada en relés, ruedas dentadas, embragues electromecánicos, etc., denominada Calculadora Automática de Secuencia Controlada, y que se llamo MARK -I.

La MARK-I se termino de construir en 1944 y tenía elementos de entrada, memoria principal, unidad aritmética, unidad de control y elementos de salida. Utilizaba como entrada tarjetas perforadas y cinta perforada.

En 1940, John W. Mauchly y J. Presper Eckert, junto con científicos de la Universidad de Pennsylvania construyeron en la escuela Moore de Ingeniería Eléctrica, la primera computadora electrónica, denominada ENIAC, que entró en funcionamiento en 1945. Fue un proyecto del ejército de los Estados Unidos para el cálculo de la trayectoria de proyectiles por medio de tablas.

En 1944 el doctor John Von Neumann, ingeniero y matemático húngaro nacionalizado norteamericano, desarrolla la idea de programa interno y describe el fundamento teórico de construcción de una computadora electrónica denominada Modelo de Von Neumann. La idea de Von Neumann era la coexistencia en el tiempo de datos e instrucciones en la computadora y la posibilidad de ser programados, no estando las ordenes cableadas.

En 1951, Mauchly construye la primera computadora de serie puesta a la venta, ésta fue la UNIVAC-I (Computadora Automática Universal), utilizando cintas magnéticas.

Desde que en 1951 surgiera la UNIVAC-I como la primera computadora comercial, hasta nuestros días existen multitud de modelos cada vez más potentes, baratos y pequeños.

Casi todas las transformaciones han sido causadas por descubrimientos o avances en el campo de la física y la electrónica.

- En 1904 el inglés Fleming inventó la válvula de vacío.
- En los años 50 y con el descubrimiento de los semiconductores aparecieron el diodo y el transistor.
- Basándose en el transistor, se construyeron circuitos capaces de realizar funciones lógicas, con lo que surgieron las puertas lógicas y sus circuitos derivados.
- Años después, comenzó la miniaturización con la construcción de los circuitos integrados que consistían en tratamientos físico-químicos sobre una película de silicio, que permiten configurar diferentes circuitos de puertas lógicas.
- En 1971 apareció el microprocesador, en el que se consiguió implementar toda la UCP de una computadora en un solo elemento integrado.

1.2.2. CONCEPTO

Etimológicamente la palabra informática se deriva de la palabra francesa *informatique* que a su vez se compone de la contracción de los vocablos "information" (información) y "automatique" (automática) que significa Información Automática.

Una de las definiciones más comúnmente aceptadas en la actualidad es la creada por la Academia Francesa en 1962 que dice que la Informática es "La ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automatizadas, de la información y de la comunicación en los ámbitos técnico, económico y social"[1]

Durante el transcurso del tiempo, se ha tratado de afinar este concepto y en 1973 se publica en México una de las primeras obras de habla hispana que pretende presentar una concepción de la informática. En dicha obra se plantea a la informática como "el estudio que define las relaciones entre medios (equipo), datos y la información necesaria en la toma de decisiones, desde el punto de vista de un sistema integrado".

Posteriormente otros autores presentaron definiciones propias como las que se mencionan a continuación:

El Diccionario de la Lengua Francesa define a la Informática como el "conjunto de técnicas de la colección, clasificación, almacenamiento, transmisión y utilización de la información tratada automáticamente con la ayuda de programas a través de computadoras"[2].

Enzo Molina define a la Informática como "la ciencia de los sistemas inteligentes de información. Es la ciencia relativa al estudio de las necesidades de información de los sistemas, mecanismos e insumos necesarios para producirla y aplicarla"[4].

Como se puede observar, las definiciones anteriores muestran dos elementos comunes que les da cierta coherencia a pesar de tratarse de diferentes puntos de vista. Estos elementos son la información y el tratamiento automático de la misma, los cuales se pueden resumir en una definición, la cual servirá de base para el desarrollo de la presente investigación: *Informática es la ciencia que estudia el tratamiento automático y racional de la información.*

1.2.3. ÁREAS DE DESARROLLO

La Informática ha podido desarrollarse en diferentes áreas, y cada una de ellas podría ser un tema interesante para el desarrollo de un seminario de investigación, sin embargo, en este apartado, se tratarán de una manera general aquellas que por su desarrollo han sido de gran

---

[1] Molina Ravetto, Enzo, Informática, una nueva ciencia. Pág. 18.
[2] Lambarri Valencia, Alejandro, Curso de Auditoría Informática. Pág. 20.
[3] Petit Robert, Diccionario de la Lengua Francesa. Pág. 100.
[4] Molina Ravetto, Enzo, Introducción a la Informática. Pág. 28.

utilidad para el desarrollo de otras areas de la ciencia. Las areas en las que ha tenido mayor desarrollo la Informática son:

- Teleinformática
- Inteligencia Artificial
- Desarrollo de Sistemas

Teleinformática

La Informática ha permitido el manejo y proceso de la información, pero en la actualidad dicha información se requiere procesar en un lugar distinto de donde es producida. Ante este problema, de la distancia entre el lugar donde se produce la información y donde se requiere para ser procesada, es como surge la Teleinformatica, que utiliza y une la Informática y las Telecomunicaciones.

Mediante esta técnica se pueden interconectar a cortas y/o grandes distancias computadoras, terminales y otros equipos, usando para ello algun modo de comunicación como las lineas telefónicas, cables coaxiales, microondas, etc.

La Teleinformática se puede definir como "la técnica que trata de la comunicación de datos entre equipos informáticos distantes"[5].

Inteligencia Artificial

La Inteligencia Artificial "es la rama de las ciencias de las computadoras que se ocupa de que éstas se comporten en forma que se parezcan al comportamiento humano inteligente"[6].

La investigación en este campo tiene tres objetivos principales: saber más acerca del cerebro humano, enseñar a la computadora como comprender el lenguaje natural y ampliar la gama de la utilidad de la computadora en la solución de problemas.

La mayor parte de la investigación en Inteligencia Artificial se dedica al desarrollo de técnicas de solucion de problemas que supera la gama de metodos algoritmicos normales que usan las computadoras. Tales técnicas resultan importantes en la construccion de sistemas expertos: programas que pueden resolver problemas a partir de una base especifica de conocimiento.

La investigación en Inteligencia Artificial tambien se ocupa de mejorar la capacidad de la computadora para reconocer patrones recurrentes de todos tipos, ya que esta capacidad constituye un importante elemento en la planeación y la predicción.

Desarrollo de Sistemas

Un sistema informatico consiste en un conjunto de programas, junto con el equipo fisico necesario, que operan sobre unos datos de entrada para producir la salida deseada.

Su desarrollo se compone de estudio y análisis del sistema, diseño, programacion, prueba, implantación, evaluación y mantenimiento.

La explotación u operación de un sistema informático consiste en la utilización y aprovechamiento del sistema informático desarrollado. Consta de previsión de fechas de realización de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema y supervisión de trabajos.

El soporte técnico, tanto para los usuarios como para el propio sistema, se ocupa de seleccionar y generar el sistema operativo adecuado y su mantenimiento, diseño de la estructura de la base de datos, estudio y evaluación de las necesidades y rendimientos del sistema y ayuda directa a usuarios.

Entre las aplicaciones donde la informática ha sido una herramienta importante se pueden citar las siguientes:

- Empresariales

---

[5] Alcalde Lancharo, Eduardo y otros autores. Informatica Basica. Pag. 176

[6] Radlow, James. Informatica y computadoras en la sociedad. Pag. 182

- Industriales
- Técnico/Científicas
- Médicas
- Militares
- Educativas
- Domésticas
- Entretenimiento

Aplicaciones Empresariales

Uno de los mayores impactos de la informática, ha sido el que ha afectado a los trabajos administrativos de la oficina. Algunas de las tareas administrativas que se pueden realizar por medio de las computadoras son la administración del personal, el procesamiento de la nómina, el control de inventarios, la administración del almacén, facturación, contabilidad, etc.

Dentro de las aplicaciones empresariales cabe destacar el desarrollo de sistemas de información, cuyo objetivo principal es ayudar en la toma de decisiones a partir del análisis de los datos relacionados con dicho sistema.

Aplicaciones Industriales

En los procesos de fabricación la computadora ha sido una importante herramienta, siendo sus principales usos el control de procesos industriales, la robótica industrial, el diseño asistido por computadora, etc.

Aplicaciones Técnico/Científicas

En cualquier campo de la investigación, la informática se ha constituido en una herramienta imprescindible. Algunas de las aplicaciones técnico/científicas son la predicción meteorológica, el control ambiental, control de tráfico, control de comunicaciones, control de satélites e ingenios espaciales, programas de simulación, etc.

Aplicaciones Médicas

Las aplicaciones de la computadora en la medicina van desde el control clínico de pacientes hasta la investigación de nuevos métodos de tratamiento de enfermedades. Otras aplicaciones son el diagnóstico clínico, mantenimiento de historiales, cuidados intensivos, etc.

Aplicaciones Militares

Desgraciadamente el uso de la computadora en aplicaciones militares, ha sido primordial frente a las demás aplicaciones. Sin embargo, cabe destacar que es esta la principal razón del gran desarrollo de la informática. Como ejemplo de las aplicaciones militares están los sistemas computarizados de radar, conducción automatizada de misiles, espionaje militar por satélite artificial, sistemas de seguridad y defensa, etc.

Aplicaciones Educativas

Las aplicaciones en la educación se enfocan principalmente a la enseñanza asistida por computadora y tutoriales. En la actualidad, mas que en las aplicaciones educativas, se debe dirigir nuestra atención a la necesidad inminente de estudiar las herramientas computacionales que en cada área de estudio son esenciales para poder desarrollarse y sobresalir.

Aplicaciones Domésticas

Gracias a la reducción de costos la computadora personal se ha popularizado llegando a la mayoría de las medianas y pequeñas empresas, introduciéndose finalmente en multitud de hogares.

La utilización de la computadora personal dentro del ámbito doméstico proporciona grandes posibilidades, utilizándose para muy diversas tareas como son la contabilidad casera, la planificación de menús y dietas, los sistemas de control de luz, calefacción, electrodomésticos, los sistemas de seguridad, entretenimiento, etc. Además, mediante la conexión a una red, se incorporan otras aplicaciones como el correo electrónico, acceso a base de datos de información general por vía internet realización de operaciones financieras, cursos de enseñanza a distancia, etc.

1.3. CENTRO DE CÓMPUTO

1.3.1. ANTECEDENTES

Al principio de la Revolución Industrial, los diseñadores de centros de cómputo los ubicaban de manera que fueran visibles a los ojos de cualquiera, ya que estos eran tomados como símbolo de prosperidad y de estatus ante la competencia y del mundo de los negocios en general.

Sin embargo, fueron muchos los centros de cómputo que se vieron afectados por actos voluntarios o involuntarios que destruyeron parte de sus instalaciones. Esto provocó que se reubicaran. Lo que queda claro es que desde su inicio fueron tomando mucha importancia para las empresas que se orientaron a la utilización en grandes proporciones de equipo de cómputo.

No fue sino hasta fines de la década de los 60's que se iniciaron las construcciones específicamente diseñadas para centros de cómputo sin prever que los avances de la tecnología dejarían obsoletas muchas de las medidas entonces pensadas, como solución a los problemas de seguridad.

IBM Canadá fue la primera empresa en desarrollar centros de cómputo como una forma de aliviar la acumulación de proyectos atrasados que experimentan muchos negocios. Se hicieron varios intentos por establecer sistemas de información en Estados Unidos, pero no fue sino hasta principios de la década de los 80's cuando el concepto de centro de cómputo arraigo finalmente en las empresas norteamericanas. En ese momento, con la creación de programas de hoja de cálculo y muchos otros paquetes de aplicación, se aseguro el éxito del centro de cómputo.

Las compañías estadounidenses pronto modificaron el concepto original a fin de satisfacer sus propias necesidades. La mayor parte de las empresas grandes ya tienen algún tipo de centro de información en funcionamiento, sino es que varios. No existe un centro de información representativo; cada uno se ha desarrollado en la forma que mejor se adapta a los requerimientos de su compañía. No obstante, el objetivo principal de todos los centros de cómputo sigue siendo el mismo: proporcionar adiestramiento y servicio para las necesidades de cómputo de sus usuarios.

La utilidad de los centros de cómputo no termina una vez que los usuarios adquieren conocimientos básicos de computación. Los ambientes de cómputo de las organizaciones cambian constantemente y es responsabilidad del personal del centro de cómputo mantenerse al tanto de los avances en computación, de manera que puedan ayudar a los usuarios a dominar los nuevos productos electrónicos y de programación. La mejor manera en que los centros de cómputo pueden servir a sus compañías es estando conscientes de las necesidades cambiantes de sus usuarios.

En décadas pasadas la información se protegía de alguna manera; al proteger el centro de cómputo, en la actualidad con la descentralización, trasportabilidad y uso de sistemas de telecomunicaciones se ha hecho más vulnerable la información, sin importar que el equipo que la procesa se encuentre bien protegido. Hoy en día se debe tomar en cuenta que cada terminal conectada al equipo principal es una extensión por la cual se pueden modificar archivos, alterar procesos, generar actualizaciones y destruir archivos importantes.

1.3.2. CONCEPTO

Según un diccionario de computación el centro de cómputo se define como "El departamento que alberga los sistemas de computación y el equipo relacionado. La biblioteca de datos es parte del centro de cómputo, y los departamentos de entrada de datos y programación de sistemas pueden caer también bajo su jurisdicción. Usualmente está provisto de una sección de control que acepta trabajo y distribuye las salidas a los diferentes departamentos usuarios."[1]

Esta es una definición corta de un centro de cómputo, ya que no indica el por qué de su existencia y mucho menos menciona de la importancia que tiene. Proponemos otra definición más orientada a la importancia de este: "Un centro de cómputo representa una entidad dentro de la organización, la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna".[2]

---

[1] Freeman, Alan, Diccionario de Computación. Pag. 195

[2] Hernández Jimenez, Ricardo, Administración de Centros de Cómputo. Pag. 20

La ventaja competitiva que da tener la información, clara, veraz y en el momento crítico, con la cual se logre la mejor toma de decisiones en una organización, es una de las razones por las que existe un centro de cómputo. Ahora diversificado en su forma de operar, es una pieza fundamental en la estructura organizacional de toda entidad.

El centro de cómputo es responsable de centralizar, custodiar y procesar la mayoría de los datos con los que opera una compañía. Su función primordial es apoyar la labor administrativa para hacerla más segura, fluida, y simplificada: el centro de cómputo es uno de los engranes vitales dentro de una maquinaria organizacional que provoca que muchos otros engranes se detengan o funcionen sistemáticamente.

El lugar donde reside la computadora, y a donde van a trabajar los usuarios, recibe tradicionalmente el nombre de "centro de cómputo". Decimos "tradicionalmente" porque con la aparición de las microcomputadoras, por un lado, y de nuevas técnicas de cómputo (telecomunicaciones, bases de datos distribuidas), por el otro, ya no es estrictamente necesario que ambos, usuarios y computadora, estén en el mismo lugar. Actualmente al centro de cómputo también se le conoce como centro de procesamiento de datos, área de informática, área de sistemas, departamento de sistemas y departamento de informática.

Las grandes computadoras de antes, con enormes gabinetes y delicados parámetros de ambientación, provocaban que el centro de cómputo pareciera un cuarto aislado de todo acceso humano al que sólo los muy expertos podían ingresar. Este misticismo y aislamiento de las salas de cómputo se volvió tradicional y actualmente se piensa que sin esto no hay centro de cómputo.

La verdad es que esto no es cierto ya que el centro de cómputo debe verse como el lugar físico en donde se realizan las funciones de procesamiento de información más importantes y fundamentales de una entidad. Actualmente las telecomunicaciones hacen que este concepto centralista se vuelva obsoleto pero aún no podemos negar que siempre habrá un lugar en donde las bases de datos se almacenen y se manipulen para obtener información decisiva o el lugar donde se establezcan los servidores principales de una organización que contengan los programas, datos y aplicaciones vitales para la operación del negocio. Si logramos entender esta nueva concepción de un centro de cómputo podremos adecuar las técnicas de auditoría a un tipo de auditoría más productiva.

Un centro de cómputo típico está dividido en áreas funcionales, que suelen estar agrupadas en dos familias: operativas, y de apoyo administrativo. Las primeras incluyen, entre otras, las salas de máquinas, la sala de impresoras y la sala de terminales (o de perforadoras, si es que todavía se usan).

El lugar donde reside la UCP y las unidades de disco y cintas magnéticas es de acceso restringido y controlado estrictamente, y es supervisado y manejado por los operadores de la computadora. Entre sus funciones importantes tenemos las de realizar respaldos periódicos de todos los archivos del sistema a cintas o cartuchos magnéticos, así como resolver los pedidos especiales que los usuarios hacen.

Cuando la sesión ha terminado, el usuario se dirige a la zona de impresoras para recoger sus resultados impresos (si es que los produjo). Ahí lo atenderán otros operadores, que se dedican a recoger los listados que las impresoras producen, para separarlos y acomodarlos en casilleros especiales, destinados a los usuarios del sistema de cómputo.

Las áreas de apoyo administrativo de un centro de cómputo, por otro lado, incluyen la dirección, la subdirección, una oficina de consultas y asesorías (donde los interesados pueden consultar manuales y resolver dudas), y oficinas especializadas de ingeniería y sistemas.

Toda máquina requiere atención y mantenimiento periódicos, por lo que los centros grandes de cómputo tienen uno o varios ingenieros residentes para estas funciones. Una sección de este departamento se dedica a mantener al día los inventarios de papel para impresión, que pueden llegar a ser de tamaño considerable.

Igualmente se requiere el apoyo de ingenieros de software y de sistema operativo, que vigilan constantemente que los sistemas de programación de la computadora funcionen adecuadamente y con eficiencia.

Es todo este grupo de personas el que provee el apoyo y la coordinación para que el usuario pueda llevar a cabo su trabajo en la computadora, para hacer, corregir, probar o correr programas; explotar bancos de información, o usarla de casi cualquier manera que su experiencia o imaginación dicten.

Toda esta atención y control es necesario mantenerlos con los demás usuarios, preservando la privacia de cada uno de ellos, y evitando en todo momento la sobrecarga del equipo y baja en la eficiencia de atención.

1.3.3. AREAS OPERATIVAS

Consultando algunos autores descubrimos que las principales areas que encontramos en un Centro de Cómputo son de manera general:

- Desarrollo de sistemas
- Operación
- Soporte Técnico
- Administración

Un *sistema informático* consiste en un conjunto de programas, junto con el equipo físico necesario, que operan sobre unos datos de entrada para producir la salida deseada en cualquier problema empresarial.

Su *desarrollo* se compone de estudio y análisis del sistema, diseño, programación, prueba, implantación, evaluación y mantenimiento.

La *operación* del sistema informático consiste en la utilización y aprovechamiento del sistema desarrollado. Consta de prevision de fechas de realizacion de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema y supervisión de trabajos.

El *soporte técnico*, tanto para los usuarios como para el propio sistema, se ocupa de seleccionar, generar y mantener el sistema operativo adecuado, diseño de la estructura de la base de datos, gestión de los equipos de teleprocesos, estudio y evaluación de las necesidades y rendimientos del sistema y ayuda directa a usuarios.

Por último, las *funciones de gestión y administración* de un Centro de Cómputo engloban operaciones de supervisiones, planificación y control de proyectos, seguridad general, gestion financiera y de personal.

No existe un modelo único de organización del Centro. Este se estructura de muy diversas maneras, según su tamaño, su ubicación funcional y el tipo de aplicaciones que desarrolle.

Un enfoque sobre la organización del área de informatica es la siguiente, la cual se basa en la descripción de puestos que la conforman.

Gerente de sistemas

Es la cabeza técnica y administrativa de todas las actividades del procesamiento de datos de la empresa. Es responsable del desarrollo de todo el procesamiento de datos que se lleva a cabo dentro de la empresa, incluyendo selección de equipos, análisis de sistemas, programación y operaciones. Proporciona enlace con los usuarios autorizados de los servicios de procesamiento de datos y desarrolla técnicas y métodos mejorados para ayudar a todas las actividades cooperativas. Sus principales funciones son:

- Proporcionar estimado de costos
- Recomendar nuevos usos para el equipo de cómputo o el abandono de usos actuales que no sean de utilidad.
- Mantener y desarrollar sistemas de computadora.
- Revisar el desempeño del personal y el equipo
- Evaluar la aplicabilidad de nuevos desarrollos técnicos
- Reportar a la gerencia sobre el desempeño de las funciones del sistema de cómputo y el progreso de los planes de desarrollo del procesamiento de datos

Gerente de programación

Proporciona dirección administrativa y técnica para el desarrollo de nuevos programas y el mantenimiento de los programas en operación. El gerente de programación está en contacto directo

con el personal de sistemas, el personal de operaciones y los responsables de los departamentos usuarios. Sus principales funciones son:

- Revisar y aceptar la especificación de sistemas y seleccionar la configuración adecuada del equipo
- Organizar los proyectos de programación y asignar personal a las tareas.
- Desarrollar estimados de costos y tiempo de programación.
- Preparar calendarios de proyectos
- Revisar el desempeño de los programadores.
- Revisar el diseño de programas con los programadores.
- Evaluar el desempeño operacional de los programas.
- Reportar al gerente de procesamiento de información la actividad, progreso y desempeño en el área de programación

Programador

Participa en el análisis, diseño de programas, codificación y otras tareas de programación requeridas para producir reportes o cómputos matemáticos o para mantener archivos de información. Ayuda en la solución de dificultades de operación encontradas en la ejecución de los programas. Sus principales funciones son:

- Preparar todos los elementos de documentación del programa
- Preparar datos de prueba y organiza el calendario de pruebas de programa
- Analizar el desempeño del programa durante la prueba
- Diseñar los procedimientos de conversión
- Preparar material de entrenamiento y entrenar a los operadores y usuarios del programa

Almacenista de documentación

Almacena y circula la documentación de los programas. Sus principales funciones son:

- Proporcionar operaciones, programas e instrucciones de operación de conformidad con el calendario
- Almacenar los materiales y documentación de los programas en forma organizada y accesible
- Asegurar que la información este completa

Gerente de sistemas y procedimientos

Proporciona asistencia analítica y técnica en la identificación y solución de los problemas de sistemas de la empresa. Sus principales funciones son:

- Definir el alcance y las tareas de estudio de sistemas
- Programar las tareas y asignar personal al sistema.
- Revisar la documentación preparada por el personal de sistemas.
- Revisar el progreso de los proyectos
- Presentar recomendaciones sobre los sistemas a la gerencia de sistemas.
- Revisar el desempeño y dirigir la acción correctiva.

Jefe de proyectos

Es asignado a proyectos de programación para proporcionar dirección y control. Participa en su organización y planeación. Tiene responsabilidad del proyecto y del personal de programación que le sea asignado. Sus principales funciones son:

- Organizar y dirigir la ejecución de las tareas de programación llevadas a cabo por los programadores.
- Diseñar la lógica para programas individuales o sistemas de programas.
- Seleccionar el lenguaje de programación y subrutinas estándar.
- Determinar la configuración óptima del equipo
- Definir el calendario de pruebas y los requerimientos para datos de prueba.
- Organizar y preparar la documentación del programa
- Dirigir las actividades de la biblioteca de programas y cintas.
- Controlar el inventario de accesorios y materiales de procesamiento de datos.
- Desarrollar un sistema para el control y coordinación de datos
- Proporcionar estándares de desempeño y métodos operativos.
- Especificar procedimientos para el registro de tiempo de personal y máquinas
- Revisar continuamente el cumplimiento de procedimientos y estándares.
- Proporcionar servicios administrativos al departamento de sistemas

Grupo de control de sistemas

Sus principales funciones son

- Estandarizar y optimizar las operaciones del centro de cómputo e identificar, diseñar y documentar procedimientos internos de trabajo.
- Proporcionar servicio y asesoría técnica a usuarios en la utilización del equipo de información
- Elaborar y establecer procedimientos de seguridad para la misma, así como para el acceso al equipo y al centro de cómputo

Supervisor de operacion del equipo

Supervisa la operación del computador. Revisa el desempeño del equipo y de personal y desarrolla técnicas para mejorar el desempeño. Revisa nuevas aplicaciones y programas y proyecta su efecto sobre la operacion del equipo para evaluación de la gerencia. Sus principales funciones son:

- Mantener registros exactos sobre la utilización del equipo
- Cumplir los requerimientos programados de procesamiento
- Proporcionar asesoría técnica en la evaluación, selección e instalación del equipo
- Evaluar el desempeño del personal para efectos de administración de sueldos, entrenamiento y promoción

Cintotecario

Sus principales funciones son

- Controlar el uso de los carretes de cinta o paquetes de discos
- Retirar del servicio, conforme se requiera, carretes de cinta o paquetes de discos
- Registrar la circulación del material registrado en la biblioteca

Gerente de apoyo técnico

Su principal función es:

- Administrar los recursos técnicos, humanos y materiales del área de informática o del área de sistemas con el objeto de garantizar el suministro de información.

Programadores de sistemas

Sus principales funciones son:

- **Revisar y trabajar con el software de la computadora para establecer un ambiente de procesamiento confiable**
- **Documentar cada programa que desarrollan.**

Analistas de seguridad

Su principal función es:

- **Desarrollar medidas de protección para la computadora para evitar que personas no autorizadas tengan acceso a la información de los archivos.**

Administrador de la base de datos

Coordinar generalmente a los programadores analistas y técnicos que mantienen y supervisan las operaciones con las bases de datos. Sus principales funciones son

- **Diseñar y coordinar las medidas de seguridad de la información para restringir el acceso no autorizado**
- **Diseñar los archivos de la base de datos y supervisar su implementación**
- **Preparar y mantener un diccionario de datos y/o un manual del usuario que indique los procedimientos estandarizados para consultar la base de datos**
- **Controlar toda la documentación de base de datos.**
- **Supervisar todas las actividades con las bases de datos para garantizar la respuesta rápida del sistema, el apoyo satisfactorio al usuario y la seguridad de la información[3]**

1.3.4. EQUIPO DE CÓMPUTO

Actualmente los centros de cómputo dejaron de ser el lugar para alojar a la gran mainframe o el cuarto donde sólo macrocomputadoras y unidades de cinta magnética se resguardaban. Los adelantos de hardware, que siempre se han inclinado a la disminución del volumen de los equipos y el incremento en el uso de sistemas en red basados en servidores poderosos y de grandes capacidades de almacenamiento que ya no son tan enormes y delicados como las viejas macrocomputadoras, hacen que el centro de cómputo tradicional se haya convertido en lugares más pequeños pero no menos importantes. Pero lo que para nosotros es importante hacer notar, es que actualmente los auditores en informática, al llegar a un centro de procesamiento de datos, se van a encontrar con una amplia variedad de tipos de equipos, los cuales harán que su plan de auditoria se adapte a la arquitectura de cada tipo de computadora.

"Todos los sistemas de computación se parecen en que contienen componentes de hardware de entrada, de procesamiento central y de salida. Todos estos ejecutan operaciones básicas de máquina bajo la dirección de programas almacenados, los cuales pueden ser cambiados rápidamente para permitir el procesamiento de diferentes aplicaciones. Por supuesto, cuando las aplicaciones difieren completamente se necesitan diferentes recursos para procesarlos. En otras palabras, la computadora personal usada en la casa para jugar a los invasores del espacio, difícilmente puede ser usada en el Centro de Control de Misiones de la NASA para vigilar el lanzamiento de una nave espacial.

Generalmente, entre más grande es el sistema, mayores son su velocidad de procesamiento, su capacidad de almacenamiento y su costo"[4]. Estas diferencias son notables en servidores de bases de datos y computadoras personales, mientras que los primeros entre mas transacciones deban soportar más caros son, las segundas entre mas implementos de multimedia y

[3] Apuntes del curso de Auditoria en Informática impartido por Ing. M. en C. C. Manuel Toriz Garcia.
[4] Sanders, Donald H., Informática Presente y Futuro. Pág. 24 a 27.

comunicación tengan más altos son sus precios. No debemos perder de vista que actualmente en muchos centros de cómputo medianos y sobre todo chicos, no existe un presupuesto que apoye la compra de servidores y solo se acoplan máquinas PC con suficiente memoria en disco duro como servidores de archivos y aplicaciones.

Aquí presentamos una división de equipos de computo de acuerdo al tamaño, pero hacemos notar que las variantes de uso en nuestros días para los equipos deben tomarse en cuenta. Podemos encontrarnos con pequeños centros de computo con redes de microcomputadoras, una de ellas servidor, que procesa información muy importante la cual debe ser protegida con una seguridad física consistente del equipo

"Los sistemas en el límite más bajo de esta escala de tamaños son llamados microcomputadoras y minicomputadoras. Las microcomputadoras son los sistemas más pequeños para usos generales. Pero éstas pueden ejecutar las mismas operaciones y usar las instrucciones de programa que muchas computadoras grandes. Las minicomputadoras son también sistemas para usos generales, pero éstas suelen ser mas poderosas y más caras que las microcomputadoras. En tamaño físico, las minicomputadoras pueden variar de un modelo de escritorio, hasta el tamaño de un archivero pequeño.

En la escala de tamaño, las macrocomputadoras son sistemas que pueden ofrecer más rapidez de procesamiento y más capacidad de almacenamiento que una minicomputadora común. Puede haber algo en común entre el costo, la velocidad y la capacidad de almacenamiento de las minicomputadoras más grandes y las más pequeñas macrocomputadoras.

Finalmente, las supercomputadoras, planeadas para procesar complejas aplicaciones científicas, son las más grandes, rapidas y caras computadoras del mundo".[5]

Esta división es la más difundida y aceptada en el medio informático y sigue siendo válida para los equipos modernos, con todo y sus adelantos tecnologicos; a continuación ampliamos las características de cada tipo de computadora.

Microcomputadoras

"Una microcomputadora es el sistema más pequeño de propósito general que puede ejecutar instrucciones de un programa para llevar a cabo una amplia variedad de tareas. Un sistema de microcomputadora tiene todos los elementos funcionales que se encuentran en cualquier sistema grande. Esto es, está organizado para llevar a cabo el almacenamiento, la lógica matemática, el control y las funciones de salida.

La mayoría de las microcomputadoras son unidades compactas y tan ligeras que pueden ser trasladadas con facilidad. Están diseñadas para ser utilizadas por una sola persona. Además de la CPU, la microcomputadora común tiene un tablero para que el operador introduzca la información, grabadoras de cinta magnética y/o lectoras de disco flexible que se utilizan para introducir datos y programas y para recibir la salida procesada. Se utilizan cintas magnéticas y discos flexibles para el almacenamiento secundario fuera de línea. Una pantalla de despliegue visual y/o una impresora de caracteres se utilizan para preparar la salida en una forma legible para el humano".[6]

Los microprocesadores fueron diseñados por tres compañías: el Z-80 de Zilog, el 6809 de Motorola y el 8088 de Intel, aunque el avance en este campo continua mes con mes.

Las microcomputadoras basadas en estos y otros procesadores, son de marcas tan diversas como Apple, Canon, Cromemico, Hewlett Packard, IBM, IMS, NEC, Radio Shack y Xerox, entre otras. Actualmente se habla de las microcomputadoras "computadoras de uso personal", que son lo suficientemente baratas y accesibles para ser empleadas por pequeñas organizaciones y negocios, donde se destinan a tareas como control de nómina, contabilidad e inventarios. También comienzan a ser de uso más extendido en aplicaciones "creativas" en computación y como pasatiempo.

---

[5] Sanders, Donald H., Informatica Presente y Futuro. Pág. 240 a 247

[6] Sanders, Donald H., Informatica Presente y Futuro. Pág. 247 a 248

Historia

Desde antes de 1968 un ingeniero electrónico al servicio de Datapoint Corporation, Victor Poor, había estado trabajando en el diseño de computadoras de propósito especial. Cada vez que se necesitaba un dispositivo especial, Poor y otros ingenieros comenzaban el diseño en una hoja de papel limpio. Poor pensó que si en vez de realizar un diseño para cada procesador se pudiera producir uno con una sola pastilla de silicio, en el cual se colocaran los elementos básicos de cualquier procesador, este se podría producir en forma masiva con la capacidad de ser programado en diversas formas para realizar las tareas específicas a que fuera designado. En 1969 Poor y Harry Pyle desarrollaron un modelo con estas características y lo presentaron a Texas Instruments y a Intel Corporation, y aun cuando en ese momento ninguna compañía comenzó algún proyecto, un año después se fabricaría el primer microprocesador.

Intel fabrica en 1970 el primer procesador destinado a una calculadora. Cubría las características de estar montado en una sola pastilla y ser programable para realizar varias funciones. Fue llamado Intel 4004 y manejaba, al mismo tiempo, datos en palabras de 4 bits.

El avance de la microelectrónica prosigue a una velocidad impresionante, y ya por los años de 1972-1973 surge en el mercado una nueva familia de circuitos integrados de alta densidad, que reciben el nombre de "microprocesadores". Las "microcomputadoras" que se diseñan con base en estos circuitos son extremadamente pequeñas y baratas, por lo que su uso se extiende al mercado de consumo industrial. Actualmente hay microprocesadores en muchos aparatos de uso común, como relojes, televisores, hornos, juguetes, etc.

Con el surgimiento de los microprocesadores de 8 bits comenzó la era de comercialización de este tipo de máquinas para uso personal. La primera computadora de este tipo fue la ALTAIR 8800 ofrecida en menos de 400 dólares y en 1975 se instaló la primera tienda de microcomputadoras en Santa Mónica, California.

Minicomputadoras

"Es una pequeña máquina de propósito general...Puede variar en tamaño desde un modelo instalable sobre el escritorio, hasta una unidad con más o menos el tamaño de un archivero de cuatro gavetas. Para ser más precisos, existen puntos en común entre los sistemas micros más poderosos y el nivel inferior de las minicomputadoras. En términos de costo y capacidad de proceso, los sistemas mini típicos sobrepasarán a una microcomputadora en capacidad de almacenamiento, velocidad de operaciones aritméticas y capacidad para soportar gran variedad de dispositivos periféricos de rápida operación. A diferencia de un sistema micro que está orientado a atender a un sólo usuario, los sistemas minis pueden ser diseñados para mejorar en forma simultánea las necesidades de proceso de varios usuarios"[1]

Historia

El desarrollo de las minicomputadoras se dio desde el inicio de los años 70's. Las primeras minicomputadoras fueron creadas para aplicaciones especializadas y muy pocas para aplicación general. En los años 60's, la tendencia del mercado de equipos era la creación de sistemas muy grandes y con enormes capacidades de procesamiento que lograran sostener todo el trabajo de una empresa importante. Para muchas organizaciones este resolvía sus problemas de procesamiento de volúmenes grandes de información, en cambio a otras les ocasionaba conflictos en costo, tamaño y procesamiento de aplicaciones específicas que una máquina grande no podía ejecutar de manera óptima.

Con la necesidad de máquinas poderosas, pero de bajo costo, fue que surgieron fabricantes de minicomputadoras como Digital Equipment Corporation, IBM, Hewlett Packard, Tandem y Honeywell. En un principio el mercado de estas nuevas máquinas estuvo dominado por la serie PDP-8 de DEC (Digital Equipment Corporation), actualmente en desuso.

Otras minicomputadoras populares son la serie PDP-11, los modelos "Nova" y "Eclipse" de Data General, las nuevas máquinas "VAX" (Virtual Address Extended) de DEC, la serie 3000 de

[1] Sanders, Donald H., Informática Presente y Futuro. Pag. 241

Hewlett Packard y los modelos 34, 36 y 38 de IBM. Actualmente son muchos los fabricantes de equipos tanto grandes como medianos. Entre otros, podemos mencionar a Wang, Honeywell (modelos 200 y nivel 6), Amdahl (competidora inglesa), Onyx, General Electric, Siemens (alemana), etc.

En la unión Soviética son de amplio uso las computadoras de la serie SU ("Sistema Unificado", Ryad), que también han pasado por varias "generaciones". La primera de ellas era una duplicación de la arquitectura de la serie 360 de IBM, con los modelos ES 1060. A fines de la década de los 70's surgió Ryad-2 cuya arquitectura sigue a la de la serie 370.

Los países socialistas han desarrollado una serie de computadoras dedicadas al control industrial, además de las máquinas de la serie "Minsk" y "BESM". Estos equipos fueron utilizados para procesar aplicaciones específicas, hoy en día algunas de estas máquinas procesan a la misma velocidad que sistemas más grandes.

Macrocomputadoras

"Una computadora, generalmente más poderosa que una microcomputadora común o una minicomputadora, es a menudo llamada macrocomputadora.

Hasta que aparecieron las minicomputadoras y las microcomputadoras, prácticamente todo lo que se computaba se hacía con macrocomputadoras. Además de proporcionar en un lugar central todo el poder de proceso requerido para toda una organización, una macrocomputadora se comunica con y ejerce control sobre procesadores más pequeños".[8]

Supercomputadoras

Las supercomputadoras son las computadoras más grandes, rápidas y caras que se han fabricado. Dado que estas se planean normalmente para procesar aplicaciones científicas complejas, la velocidad de cómputo del sistema es lo más importante, lo cual significa que puede sumar cientos de millones de números en un segundo debido al tamaño de su memoria principal, que a menudo puede contener 10 o 20 millones de palabras, y a su aun más grande memoria secundaria, que por lo común es 20 veces el tamaño de su memoria principal.

Las supercomputadoras ocupan por completo un salón grande y cuestan millones de dólares. Las capacidades de las supercomputadoras son útiles para efectuar cálculos científicos y de ingeniería muy complejos, y en particular para intercalar, clasificar y analizar grandes cantidades de datos.

Por ejemplo, los satélites que analizan las masas continentales y los océanos de la Tierra, proporcionan a los científicos miles de millones de datos, por lo que se necesitan supercomputadoras para clasificar aquellos que tienen interés particular y ameritan atención científica, ya que aun un gran equipo de científicos podría ahogarse con tantos datos.

Historia

A las supercomputadoras a menudo se les denomina "devoradoras de números" porque son computadoras especializadas para trabajar con números, aquella computadora que tenga mayor capacidad para devorar números en cualquier momento dado, es la supercomputadora del momento. Las supercomputadoras no son lo mismo que las computadoras de quinta generación, que tienen la finalidad de ser una nueva clase de maquinas para resolver problemas. Sin embargo, éstas van siendo empujadas hacia su propia metamorfosis de quinta generación, junto con la circuitería integrada y los medios de almacenamiento.

Los fondos para investigación y desarrollo de supercomputadoras provienen en parte del gobierno de Estados Unidos, que es su principal cliente. Un censo de supercomputadoras que se realizó en 1983 mostró que existían veinticinco en Estados Unidos, de las cuales la mitad pertenecían al gobierno. ¿Por qué hay tan pocas? por una razón: muy pocas industrias o negocios necesitan máquinas tan poderosas que puedan ejecutar una operación básica en 12.5 mil millonésima de segundo. Y por otra estas máquinas son tan costosas como poderosas. El precio

[8] Sánders, Donald H., Informática Presente y Futuro. Pág. 257 a 256.

de la Cray I, fabricada por Cray Research (uno de los tres fabricantes de estas computadoras) tiene un precio inicial de 8 millones de dólares. En un año, la compañía vendió seis máquinas, en un total de 50 millones de dólares. Desde el punto de vista del comprador, esto es mucho dinero, desde el del vendedor, no ofrece mucho incentivo, ya que el fabricante de una microcomputadora que capture la atención del público, y su bolsillo, puede lograr estas ganancias en unas semanas, por ejemplo el día que apareció la Macintosh en el mercado, Apple recibió ordenes con valor de 3.5 millones de dólares.

Las supercomputadoras propiedad del gobierno de los Estados Unidos realizan una variedad de importantes tareas. Algunas se emplean para realizar cálculos de alto secreto en investigaciones de armamento en laboratorios ubicados en Nuevo México y California. Otras trabajan en problemas de pronóstico meteorológico en varias localizaciones en Estados Unidos y en el extranjero, así como en investigación relacionada con la atmosfera de la Tierra. En estas últimas aplicaciones, la información acerca del clima se obtiene a partir de todo el mundo por medio de aeroplanos, estaciones terrestres y satélites espaciales, y se almacena en la computadora, que después analiza los datos y produce los pronosticos.

Para mejorar el pronostico meteorológico, entre otras cosas, el gobierno federal de Estados Unidos está presionando para que se produzcan supercomputadoras aún más veloces que las que ahora posee. Ya que en 1983 una Cray I podía efectuar 100 millones de cálculos por segundo, este parece ser un deseo frívolo. Pero el pronostico meteorológico actual está lejos de ser por completo exacto, porque las supercomputadoras actuales no pueden evaluar con rapidez las innumerables variables que constituyen un pronóstico. Con la tecnología actual, sucede que la tormenta que ayer se anunció para mañana cae hoy, encontrando a las personas desprevenidas.

Se espera que la nueva generación de supercomputadoras trabaje 100 veces más rápido que la más veloz supercomputadora que hoy se emplea, lo cual significa que pronto existirán computadoras capaces de efectuar 10 mil millones de cálculos por segundo.

1.4. SEGURIDAD EN INFORMÁTICA

1.4.1. ANTECEDENTES

En Estados Unidos se firmó una ley de seguridad en cómputo el 8 de enero de 1988 por el presidente Ronald Reagan. Este fue uno de los primeros pasos para mejorar la seguridad y privacidad de la información contenida en los sistemas federales de computación.

En dicho documento se establece una autoridad central para el desarrollo de pautas para la protección de información no reservada, pero sensible, almacenada en las computadoras del gobierno. También se promueve que cada agencia de gobierno formule un plan de seguridad en computación a la medida de sus propias circunstancias y basado en las pautas establecidas, además obliga a cada agencia a entrenar a su personal informático acerca de las amenazas y vulnerabilidad de sus sistemas de computación.

Durante muchos años, la computadora ha sido un buen pretexto para realizar publicidad sensacionalista acerca de las experiencias divertidas o escalofriantes respecto a uso de las mismas, una consecuencia inmediata es la existencia de gran cantidad de artículos y bibliografía sobre el tema. La investigación patrocinada por el gobierno para dar seguridad a los sistemas de cómputo se incrementó en Estados Unidos y en Europa, lo cual propicio la publicación de muchos libros y artículos acerca del abuso y la seguridad sobre estas. Esta es una de las razones por las que las empresas especializadas en servicios de asesoría para la seguridad en computación han proliferado. En más de un caso tales empresas son dirigidas en la actualidad por individuos que poseen antecedentes delictivos y han cometido robo o fraude en grandes instalaciones de computación.

Si se analiza el asunto con atención, resulta claro que se ha desarrollado un área nueva de preocupación gerencial: el abuso en el manejo de las computadoras o el desastre a causa de robo, fraude, sabotaje o interrupción en las actividades de cómputo. La seguridad de las computadoras no es todavía un tema que se considere en forma apropiada. Muy pocos de los libros que se han escrito proporcionan un marco general lo suficientemente amplio para abordar este complejo problema. Por tanto, se destacan de manera específica las áreas tradicionales como la seguridad física y contra incendios. Entonces muchas instituciones que han cubierto estas áreas viven en una situación ficticia de seguridad, mientras en realidad el nivel de seguridad de las computadoras se encuentra por debajo del estándar aceptable y el nivel de compromiso de la gerencia con la efectividad real es bajo.

La conciencia sobre el problema puede surgir temporalmente en caso de desastre o de abuso en los recursos de computación, pero la efectividad como rutina es, cuando mucho, esporádica. Las actitudes mas frecuentes son: "estamos satisfechos con la seguridad en nuestra computadora" y "no es probable que eso suceda aquí".

En contraste con los antecedentes sobre la seguridad en computación, que generalmente es superficial, existen ciertos factores que han modificado el contexto dentro del cual se usan las computadoras y han aumentado el nivel de seguridad que se requiere.

Concentración del procedimiento de aplicaciones mas grandes y de mayor complejidad

La principal causa del incremento en los riesgos de computación probablemente sea el aumento en la cantidad de aplicaciones que se da a las computadoras y la consecuente concentración de información y procesamiento. Además, la tendencia creciente hacia la incorporación de sistemas mayores y más complejos que incluyen procesamiento en línea y en tiempo real, así como el uso frecuente de bases de datos o archivos sofisticados constituye un problema adicional.

El uso de los sistemas de bases de datos está cada vez más difundido y gran cantidad de información confidencial se almacena de este modo. Como consecuencia de ello, cualquier organización puede sufrir "amnesia corporativa" debido a algún desastre en las computadoras, y de que venga una suspensión prolongada del procesamiento.

Dependencia en el personal clave

Además del peligro de algún desastre, existen otras situaciones potencialmente riesgosas de las cuales la más importante es depender de individuos clave. Si bien es cierto que la situación existe en todas las funciones de una institución, la relativa novedad de la experiencia con computadoras y la brecha respecto a la comunicación entre los técnicos expertos y la gerencia, crea problemas específicos. Los programas de computadora generalmente se vuelven cada vez más complejos, por lo que una sola persona provista del conocimiento técnico de la programación y/o del equipo, se encuentra en una posición de control única. Este tipo de conocimiento ha conducido a situaciones donde las empresas se han visto expuestas al chantaje o la extorsión.

Desaparición de los controles tradicionales

La brecha en la comunicación entre el personal técnico, los gerentes de línea y el personal de auditoría, suele causar dificultades para formular las implicaciones prácticas de este desarrollo en los términos comerciales convencionales. Muchas de las nuevas aplicaciones del cómputo omiten las auditorías tradicionales y los controles impresos por razones de volumen. Las aplicaciones contienen verificadores automáticos que aseguran la integridad de la información que se procesa. Este gran cambio en el criterio sobre el control de los empleados y las brechas respecto a la comunicación, crean situaciones de seguridad totalmente diferentes.

Huelgas, terrorismo e inestabilidad social

El nivel actual de riesgo en computación se debe revisar también dentro del contexto de inestabilidad y terrorismo urbanos en muchas partes del mundo. Ha habido ataques físicos a instalaciones donde se trata del personal interno de la compañía y no de agitadores. Estos ataques internos pueden tomar la forma de una huelga, esta, aunque no violenta puede ser tan perjudicial como el ataque físico.

Mayor conciencia de los proveedores

La investigación y el apoyo por parte de los proveedores se ha incrementado en el área de la seguridad. Hasta hace pocos años este tema no constituía motivo de gran preocupación para los proveedores, pero la conciencia acerca de la exposición a los riesgos los ha obligado a destinar presupuestos considerables para la investigación sobre seguridad en cómputo. Como resultado han surgido manuales con mejor calidad para los usuarios, lo que permite procurar mayor seguridad a las computadoras.

1.4.2. CONCEPTO

En seguida proponemos varias definiciones de seguridad para tratar de comprender mejor todo lo que engloba este concepto.

"La seguridad es la condición de estar "seguro" y eso significa estar libre, exento de riesgos, de daños o de males"[1]

La definición anterior no quedaría clara si no definimos lo que es riesgo.

El riesgo es la "posibilidad presente de la ocurrencia de un hecho infausto"[2]

Los autores Jerome S. Miller y Robert Riegel clasifican el riesgo como puro y como especulativo. Los riesgos especulativos no son propiamente riesgos aunque se les de tal nombre, ya que solamente significa la posibilidad de la ocurrencia de un hecho que pueda ser adverso o favorable.

Por otra parte, el riesgo puro siempre significará conexión con sucesos infaustos y por ende tendrá consecuencias adversas. Como ejemplos de ello tenemos el incendio, la inundación, el

[1] Aguirre Martínez, Eduardo. Seguridad Integral en las Organizaciones. Pag 9
[2] Aguirre Martínez, Eduardo. Seguridad Integral en las Organizaciones. Pag 9.

terremoto, el robo, la perdida de la vida o de la salud, etc. La segundad en las empresas tratará siempre de los riesgos puros.

En la plática de conceptos básicos de seguridad, ofrecida el 1o. de Diciembre de 1994 en el Día Internacional de la Seguridad en Cómputo por Diego Zambon, se trataron temas relacionados con ¿qué es segundad?, y se pueden rescatar las siguientes conclusiones:

¿Qué es Seguridad en Cómputo?

Los términos como "seguridad", "protección" y "privacidad" pueden tener más de un significado, dependiendo de quien lo aplica, y en qué ámbito se aplica; esto se puede notar en el hecho de que incluso los profesionales que trabajan en el area de seguridad no siempre coinciden en lo que estos terminos significan.

Una definición bastante practica de seguridad es: "Un sistema es seguro si se puede confiar en que él y su software se comporten como los usuarios esperan que lo hagan"[3]. La palabra clave en esta definición es la confianza; cualquier cosa que no sea confiable no es segura. De igual manera, si algo no tiene privacidad no se puede decir que es seguro. La privacidad consiste en proteger la información contra ser leída por alguien que no tenga autorización explícita para hacerlo, esto incluye no sólo proteger la información en su totalidad, sino tambien las piezas individuales de información que puedan ser utilizadas para inferir otros elementos de información confidencial. La confidencialidad de la información surge de la importancia de esta y del riesgo que se corre en que sea usada por personas ajenas a lo planeado. Esta es sólo una de las razones que dan importancia a la seguridad física aplicada de manera adecuada a un centro de cómputo, sólo con ésta se logra que la confidencialidad de la información perdure.

Otra razón que forza a guardar una seguridad en cualquier centro de computo es la integridad de los datos, podemos entender esto como proteger la información contra ser modificada sin el permiso de su dueño. Esta información incluye no sólo la que está almacenada directamente en los sistemas de cómputo, sino elementos menos obvios, como respaldos, documentación, registros de contabilidad del sistema, etc. Muchas veces no involucramos dentro de nuestros controles, los dedicados al resguardo correcto de los respaldos de sistemas, definiciones y contenido de bases de datos, programas fuente y de la documentación generada por las areas de desarrollo y planeación de sistemas en un caso de desastre se puede perder trabajo de largo tiempo de planeación y desarrollo.

La disponibilidad de los servicios de un área de computo, ya sean en sistemas o en disponibilidad de información, es de suma importancia en cualquier empresa con deseos de mantenerse competitiva en el mercado o en su negocio. Proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada, es parte de la definición de seguridad en computo.

Podemos decir que la consistencia (asegurar que el sistema siempre se comporte de la forma esperada), es función de un soporte técnico o de un mantenimiento preventivo y correctivo adecuados, pero si los factores que afectan el funcionamiento de un sistema no son internos o parte del mismo, sino que son agentes externos como suministro de corriente, ataques de personas extrañas al negocio, sabotaje o complot, etc., no queda más que invertir en mejorar los controles internos en materia de seguridad en cómputo, un ejemplo de estos controles es la regulación de acceso, que consiste en controlar quién utiliza el sistema o cualquiera de los servicios ofrecidos en un área de computo.

Dentro de la definición de seguridad, hay que destacar la vulnerabilidad, es decir, los puntos en los cuales un sistema es susceptible de ser atacado, ya que si no existiera un sistema o centro de cómputo vulnerable, nunca encontraríamos como implementar un concepto de seguridad en computo en la empresa. La vulnerabilidad se pueden detectar en las areas:

- Físicas
- Naturales
- Hardware y Software
- Medios de almacenamiento

[3] Diego Zambon, Dia Internacional de la Seguridad en Computo, 1o. de Diciembre de 1994

- Comunicaciones
- Humanas

Las principales amenazas a la que esta expuesto son de tipo

- Naturales y fisicas
- No intencionales
- Intencionales

Para que podamos definir nuestras políticas de seguridad e implementar los controles, necesitamos hacer una evaluación de riesgos. Aunque todos los tipos de seguridad son importantes, sus prioridades varían de una organización a otra. Diferentes ambientes tienen diferentes preocupaciones de seguridad, y por lo tanto deben establecer sus políticas y mecanismos de acuerdo a ellos. El administrador del sistema necesita entender perfectamente las necesidades del ambiente en el que trabaja, para definir los procedimientos adecuadamente.

La pregunta que se ha mantenido desde que las computadoras recibieron su primer atentado es ¿podemos eliminar completamente los riesgos?. Según Spafford "el único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias armados muy bien pagados. Aun así, no apostaría mi vida por él".

El primer paso para poder lograr una seguridad total en computo es responder a las siguientes preguntas

¿Qué se quiere proteger?
¿Contra qué se quiere proteger?
¿Cuánto tiempo, dinero y esfuerzo se esta dispuesto a invertir para protegerlo?

Para llevar a cabo estos terminos, es necesario un enfoque amplio de que es la seguridad, para lograrlo se involucran en su definicion aspectos divididos en dos áreas.

Aspectos administrativos

- Politicas definidas sobre seguridad en computación
- Organización y división de las responsabilidades
- Seguridad física y contra incendios
- Políticas hacia el personal
- Seguros

Aspectos técnicos y de procedimiento

- Seguridad de los sistemas
- Seguridad en las redes
- Seguridad en el equipo
- Seguridad de las aplicaciones, datos y archivos
- Estándares de programación y operación de sistemas
- Función de la auditoría interna y externa
- Planes de contingencia

Realmente ningún área por si sola es la más importante, si falta alguna se pierde la concepción de una seguridad total y por tanto el área de informática se convertirá en vulnerable.

1.4.3. CLASIFICACIÓN

Existen múltiples tipos de seguridad en cómputo. Como usuarios y como administradores, es necesario conocer al menos los tipos básicos, para decidir cuáles son los más importantes para nosotros.

Proponemos la siguiente clasificación de seguridad de acuerdo a las actividades de un área de informática:

Seguridad lógica

"En la situación actual de criminología, los delitos de "cuello blanco" han incluido la modalidad de los delitos hechos mediante la computadora o los sistemas de información de los cuales el 95% de los detectados han sido descubiertos por accidentes y la gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como la computadora ha modificado las circunstancias tradicionales del crimen, muestra de ello son los fraudes falsificaciones y venta de información hechos a las computadoras o por medio de computadoras.

En la actualidad se ha dado otro factor que hay que considerar, el llamado "virus" de las computadoras, el cual aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Se trata de pequeñas subrutinas escondidas en los programas que se activan cuando se cumple alguna condición, por ejemplo, haber obtenido una copia en forma ilegal, y cuando ejecutarse en una fecha o situación predeterminada. El virus normalmente lo ponen los diseñadores de algún tipo de programa para "castigar" a quienes lo roban o lo copian sin autorización o bien por alguna actitud de venganza en contra de la organización.

El crecimiento de los fraudes por computadora ha hecho patente que la potencialidad de los crímenes crece en forma más rápida que en los sistemas de seguridad. Los motivos de los delitos por computadora normalmente son por:

- Beneficio personal
- Beneficios para la organización
- Síndrome de Robin Hood
- Jugando a jugar
- El departamento es deshonesto
- Odio a la organización
- El individuo tiene problemas financieros
- La computadora no tiene sentimientos ni delata
- Equivocación de ego
- Mentalidad turbada

Se considera que hay cuatro factores que han permitido el incremento en los crímenes por computadora. Estos factores son:

1. El aumento del número de personas que se encuentran estudiando computación
2. El aumento del número de empleados que tienen acceso a los equipos
3. La facilidad en el uso de los equipos de cómputo
4. El incremento en la concentración del número de aplicaciones y, consecuentemente, de la información"[4]

Seguridad física

El objetivo de la seguridad física es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos debido a

[4] Echenique García, José Antonio. Auditoría en informática. Pag 102 a 105

contingencias como incendio, inundación, huelgas disturbios, sabotaje, etc. y continuar en un medio de emergencia hasta que sea restaurado el servicio completo.

En este tipo de seguridad se toma en cuenta desde el tipo de aire acondicionado que se usa en el centro de cómputo, el piso falso, las alarmas y medidas de control de incendio (detectores y extinguidores), ductos de desagüe y calefacción, salidas de emergencia, ventanas y las referentes al material y construcción del edificio del centro de cómputo ya que existen materiales que son altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despiden polvo.

También en lo posible se deben tomar precauciones en cuanto a la orientación del centro de cómputo y se deben evitar en lo posible los grandes ventanales, los cuales además de que permiten la entrada del sol pueden ser arriesgados para la seguridad del centro de cómputo.

Una parte importante de la seguridad física del centro de cómputo son los seguros y los planes de contingencia para caso de desastres, sin ellos sería muy complicado salir adelante después de cualquier suceso fortuito.

Seguridad en el personal

"Un buen centro de cómputo depende, en gran medida, de la integridad, estabilidad y lealtad del personal, por lo que, al momento de reclutarlo es conveniente hacerle exámenes psicológicos, médicos y tener muy en cuenta sus antecedentes de trabajo.

Se debe considerar los valores sociales y, en general, su estabilidad ya que normalmente son personas que trabajan horas extras, con gran presión y que no haya una adecuada política de vacaciones debido a la dependencia que se tiene con algunas personas, lo cual va haciendo que se crean "indispensables". Se debe verificar que existan adecuadas políticas de vacaciones y de reemplazo.

También se deben tener políticas de rotación de personal que disminuyan la posibilidad de fraude, ya que un empleado puede estar haciendo otra actividad en un mes y sería muy arriesgado cometer un fraude, sabiendo que la persona que esté en su lugar puede detectarlo fácilmente.

Se deberá también evaluar la motivación del personal, ya que un empleado motivado normalmente tiene un alto grado de lealtad y disminuirá la posibilidad de ataques intencionados a la organización"[5]

Seguridad en telecomunicaciones

Este tipo de seguridad se aplica a los sistemas de comunicación y los programas de manejo asociados a éstos. El mayor riesgo reside en el acceso no autorizado a una red, con el propósito de obtener información confidencial o de hacer uso indebido de los datos almacenados en el servidor por ejemplo, eliminarlos o moverlos de directorio. Un caso real que fue difundido, en relación a este tipo de delitos, fue el de la empresa Pacific Telephone, donde un especialista en telecomunicaciones logró tener acceso a un manual de operación de redes y, mediante el empleo de éste y usando su terminal, manejo recursos de la compañía para cometer fraude contra la misma.

El aspecto del acceso a información confidencial en instituciones de alta seguridad, se convierte en un problema sumamente grave y de consecuencias catastróficas. Actualmente se ha logrado rastrear una línea de transmisión telefónica, pero aún es complicado rastrear el origen de una señal proveniente de un equipo de cómputo que puede estar en cualquier parte del mundo, con una dirección electrónica robada o colgado a una red por medio de un nodo provisional. Por esta razón, hoy en día la medida más segura de transmitir información por una red, sin que sea manipulada por terceros, consiste en usar un código para encriptamiento o criptografía.

[5] Echenique García, Jose Antonio, Auditoría en informática Pag 109

CAPÍTULO 2

Auditoría en Informática

2.1. ANTECEDENTES

Las computadoras son hoy en día los más fieles y seguros servidores del hombre en los campos de la ciencia y la técnica. Sin embargo tanto su fidelidad como la seguridad que ellos brindan responde única y exclusivamente a la aplicación de una tecnología que el hombre ha materializado mediante su trabajo en estos equipos. Es decir, las computadoras han sido, son y serán un producto del trabajo del hombre y como tal están subordinadas a éste, le sirven de medio auxiliar para realizar tareas que llevarían gran cantidad de tiempo y que además tendrían poca precisión.

En las condiciones del mundo actual, las técnicas asociadas a la computación electrónica han tomado un auge tal, que ya no es absurdo pronosticar que estos equipo son decisivos en el desarrollo económico de un país. Las computadoras son fundamentales en la planificación, el desarrollo de la ciencia, el procesamiento de las informaciones imprescindibles para la dirección de un país, de una rama, de una empresa o de una fabrica.

A partir de la segunda mitad de la década de los 40's se ha visto surgir y desarrollar cuatro generaciones de computadoras. En estos años se han fabricado decenas de miles de máquinas de todos tipos y tamaños: grandes, medianas y pequeñas, incluyendo las ya famosas minis y microcomputadoras. Se han inventado nuevos equipos para la entrada y salida de datos, se han perfeccionado las memorias auxiliares de cintas, discos y tarjetas magnéticas. Han sido incorporadas redes especiales de comunicación para el trabajo a distancia.

Junto a todo lo anterior, también ha ido desarrollándose todo un complejo de técnicas para facilitar el análisis, la programación y la explotación. Decenas de lenguajes de programación, nuevos métodos matemáticos y sistemas de operación meticulosamente elaborados se aplican hoy en día en las instalaciones de cálculo.

La computadora actual es de 300 a 1000 veces más potente que las primeras, sus memorias inmensamente mayores y a la vez son mucho más fáciles de programar y utilizar.

Hasta tiempos recientes, el costo fundamental de los recursos asociados a la informática venía determinado por el costo de los recursos físicos. Desde el mismo momento en que buscó un mayor aprovechamiento y efectividad de las técnicas y tecnologías desarrolladas en el campo del hardware, el software fue cambiando la relación de valores, hasta llegar a nuestros días en que el costo de los recursos lógicos y humanos sobrepasan la mitad de la inversión total.

Derivado de todo el desarrollo que han tenido las técnicas asociadas a la computación y teniendo en cuenta que dichas técnicas no están al alcance ni son el dominio de la mayoría, los trabajos que entraña la automatización de cualquier tarea son vistos como si fueran realizados por una "caja negra". Es decir, se tiene noción de que es necesario, para que el computador trabaje, introducirle determinada información y con ella obtener las tablas de salida deseadas. Sin embargo, el sistema que mueve y enlaza los hechos que a diario se realizan en la "caja" no es fácil de comprender, o mas precisamente no se conoce si no se tiene la preparación técnica debida.

El desconocimiento por parte de los auditores de las técnicas con las cuales se trabaja una computadora, en principio limitó la comprobación de cuentas en los dispositivos que prestan los servicios de tratamiento de la información en forma automática. Posteriormente, este trabajo se fue introduciendo por un proceso de aproximaciones sucesivas, de forma tal, que dentro de la auditoría en informática pueden situarse cuatro momentos, que son:

a) La auditoría alrededor de la computadora: aquí se realizaban los procedimientos clásicos de evaluación de cuentas considerando los resultados que se obtenían a partir de la información de entrada, sin ver nunca como se hacían las cosas en la computadora.
b) La auditoría sin la computadora: en este caso se llegaba, además, a comprobar la existencia o carencia de normas de documentación y, de existir, si éstas se cumplían. No se analizaban los procedimientos y los informáticos se reservaban algo así como el "derecho de autor".
c) La auditoría dentro de la computadora: aquí hay un conocimiento satisfactorio de las técnicas asociadas a la computación y los auditores son capaces de comprobar cómo se hacen las cosas en la computadora. Es decir, no sólo comprueban los resultados a partir de las entradas y verifican las existencias de determinadas normas, sino que además

analizan cómo se comportan estos factores dentro de la máquina y qué beneficios o grado de satisfacción se logra a partir de los procedimientos concebidos.

d) La auditoría con la computadora en este caso el auditor alcanzó el pleno dominio de las técnicas correspondientes y es capaz no sólo de auditar los sistemas informaticos, sino que ademas utiliza la computacion como una herramienta propia para desarrollar los procedimientos de comprobación en general que se consideren necesarios. Es decir que aquí se utiliza la computadora como un medio para poder hacer uso de técnicas como el muestreo, u otras del campo de las matemáticas aplicadas que le sirvan para evaluar el comportamiento de la gestión empresarial en general.

El objetivo de la auditoria clásica es el de comprobar y analizar los "libros de contabilidad" y documentos de cualquier tipo de organización, empleando métodos propios, con el fin de exponer hechos y situaciones económicas y financieras. En la auditoría en informática este objetivo no queda excluido sino mas bien ampliado. Dado que los valores de las cuentas contables y la información general de la empresa se encuentran registrados en soportes magnéticos, se requiere

a) Análisis de todo el proceso de explotación y su realización con los supuestos establecidos en el diseño.
b) Análisis de la eficiencia conque trabaja el centro de procesamiento de datos.
c) Análisis de la utilidad que tiene para la empresa las informaciones que se estan obteniendo en los distintos procesamientos y su relacion con los costos mismos.

La auditoria, para poder cumplir sus objetivos, requiere al menos de la realizacion de dos funciones especificas básicas: el control y el análisis.

La auditoría como elemento de control nos va a servir para descubrir cuales son las causas que ocasionan determinadas desviaciones con respecto a los planes y normas establecidos para el funcionamiento del centro. Un centro de computo no debe existir sin una determinada organización que garantice la mejor forma de combinar, tanto los recursos materiales como humanos y las relaciones que entre ellos se producen y con el mundo exterior, en un tiempo y espacio determinado. En este sentido, la organizacion de un centro de computo debe estar explicitamente definida a fin de garantizar los planes y normas necesarios para el buen funcionamiento del centro.

Considerando los planes y normas establecidos, y cumpliendo con el principio de dirección sobre la unidad entre la administracion y la información, la direccion general de la empresa y del centro de computo conocerán, por informes periodicos, la marcha del centro y del cumplimiento de los presupuestos establecidos. Obviamente, por esta misma via conocerán de los principales factores que están conspirando contra el buen funcionamiento del centro.

Conocida la situación sobre el funcionamiento del área de informatica y tomadas las decisiones consecuentes contra las desviaciones encontradas, la dirección de la empresa o la del centro de cómputo pueden solicitar una auditoria que investigue sobre las causas que ocasionan las desviaciones, determine con claridad las responsabilidades y proponga las medidas necesarias que permitan subsanar los efectos negativos y eviten su repetición.

La auditoría, como elemento de análisis, debe definirle a la dirección de la empresa cual es la posición de la misma con respecto a un nivel de desarrollo de la informática. En este caso la auditoria debe evaluar el grado de aplicación de la técnica en el sistema informativo, sus cualidades, deficiencias, etc. Ademas es necesario saber el estado de los equipos conque se trabaja, los procedimientos tecnicos que se realizan y las personas que intervienen. Esta función se lleva a cabo básicamente cuando se van a introducir por primera vez los tratamientos automaticos de informaciones, o cuando se requiere alguna modificacion en la configuración de máquina existente.

Hemos enunciado estas dos funciones de la auditoria por separado porque responde originalmente a objetivos diferenciados. Sin embargo, esto no quita que en la practica una u otra puedan presentar intersecciones, es decir, en una auditoria, como elemento de control, pueden detectarse situaciones que afecten el funcionamiento del centro de cómputo, producto del nivel de desarrollo que se tenga o viceversa.

En cualquier caso, el por qué de la auditoria en un centro de computo viene dado por la necesidad de obtener un diagnóstico de la situacion existente que sirva de punto de partida para un

proceso de toma de decisiones que modifique la línea de acción y trace una trayectoria para cierto tiempo.

Presentamos a continuación una cronología que puede servir de referencia sobre el surgimiento de la auditoría en informática:

1956 Frank S. Howell. Uso el computador en la conciliación de las cuentas de inventario.
1961 Félix Kaufman escribió el libro "El Computador Electrónico y la Auditoría".
1963 Carol Wiss dio un curso de una semana sobre Auditoría y Procesamiento Electrónico de Datos.
1968 Hanskins y Sells desarrollan un software llamado "Auditape"
1970 El Instituto Canadiense de Contadores publica las "Guías del Control del Computador".
1971 El Internal Revenue Service emite la regla 71-20 que oficializa las regulaciones de procesamiento de datos.
1972 Proliferan los grupos de auditoría de procesamiento de datos.
1973 La AICPA emite el "Statements on Audit Standars"
1977 Se crea el estándar de encriptación de datos (DES) por la Oficina Nacional de Estándares en los Estados Unidos de Norteamerica[1]

[1] Apuntes del curso de Auditoría Informática de la M. en C.C. Marina Tortz García

2.2. CONCEPTO

Para el M.A. José Antonio Echenique García la Auditoría en Informática es "la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones" [1].

En la obra del L.I. Enrique Hernández Hernández, "Auditoría en Informática, un enfoque metodológico", se presentan otras definiciones:

"Un proceso formal ejecutado por especialistas del área de auditoría y de informática, se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el aseguramiento y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente" [2].

"Las actividades ejecutadas por los profesionales del área de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.). Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual ha de contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y optimización permanente de la tecnología de informática en el negocio" [3].

"El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que pasa por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc." [4].

"Proceso metodológico que tiene el propósito principal de evaluar todos lo recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opera con un criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad de la organización" [5].

Otra definición es la siguiente: "Es la verificación de los controles y procedimientos que se llevan a cabo en el área de informática a fin de saber si se están cumpliendo con las políticas y objetivos de la empresa respecto a esa área y a la información en general en aspectos tales como: seguridad, confiabilidad, integridad, veracidad y oportunidad entre otros" [6].

De las definiciones anteriores, se tomaron los aspectos más significativos para integrar nuestra definición de Auditoría en Informática con la que se trabajará durante el desarrollo del presente trabajo.

De ésta manera tenemos que la Auditoría en Informática es *un proceso metodológico ejecutado por profesionales del área de informática y de auditoría, que tiene por objetivos verificar y evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al aseguramiento y uso eficiente de los recursos informáticos y garantizar la seguridad, integridad, y oportunidad en el manejo de la información en la organización.*

---

[1] Echenique García, José Antonio. Auditoría en Informática. Pág. 15.
[2] Hernández Hernández, Enrique. Auditoría en informática, un enfoque metodológico. Pág. 17.
[3] Hernández Hernández, Enrique. Auditoría en Informática, un enfoque metodológico. Pág. 17.
[4] Hernández Hernández, Enrique. Auditoría en Informática, un enfoque metodológico. Pág. 17.
[5] Hernández Hernández, Enrique. Auditoría en informática, un enfoque metodológico. Pág. 17.
[6] Apuntes del curso de Auditoría en Informática de la M. en C.C. Marina Toriz García.

2.3. OBJETIVO

En los últimos años se ha incrementado aceleradamente la instalación de las computadoras en las organizaciones. Dicho incremento tiene como objetivo el mejoramiento constante en la manipulación de la información y trae consigo una fuerte inversión, con la cual se busca la conformación de una infraestructura compuesta no solo por los equipos de computación, sino también por el software, el personal, el tiempo de capacitación, la papelería, los consumibles, entre otros, para cumplir con el objetivo principal de obtener la información necesaria y oportuna para administrar adecuadamente las operaciones propias de la actividad empresarial.

Durante años se ha considerado a la información, junto con todos aquellos elementos que la afectan directamente, como un activo digno de salvaguardarse. Lo anterior como consecuencia del interés de disponer de ella y del costo que esto puede ocasionar.

La evolución de los conocimientos y de la tecnología en el manejo de la información, han ocasionado que la "auditoría tradicional evolucione" y surja un tipo de auditoría orientada a la detección y disminución de riesgos y errores en el manejo de la información. Este tipo de auditoría, denominada Auditoría en Informática, tiene como objetivo principal verificar y evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al aseguramiento y uso eficiente de los recursos informáticos y garantizar la seguridad, integridad, y oportunidad en el manejo de la información en la organización.

Aún cuando la Auditoría en Informática tiene un objetivo general, existen objetivos específicos que corresponden a cada una de las áreas susceptibles de revisión en el centro de cómputo y que se mencionarán posteriormente.

El determinar para qué es necesaria una auditoría en un centro de cómputo es un aspecto de tremenda importancia. En el por qué encontramos el objetivo o móvil que nos lleva a una auditoría, pero en el para qué debemos delimitar cuáles son las situaciones concretas que nos pueden dar la misma. Estas situaciones tienen que ser evaluadas por el diagnóstico, por que además el mismo tiene que proponer determinadas recomendaciones que permitan una acción consecuente con los problemas detectados en la investigación. Entre los factores que pueden ser enjuiciados en una auditoría hay algunos que pueden responder a las características particulares de la empresa en cuestión y otros que tienen un carácter mas general. Dentro del último grupo, los más relevantes nos deben permitir conocer:

a) La relación costo-beneficio. Este es un elemento que trata de medir lo que nos cuesta la automatización y su relación con los beneficios que de ella se logran. Los costos se pueden cuantificar fácilmente, pero los beneficios de contar con determinada información en un tiempo, calidad y precisión dada resulta más difícil. Los beneficios habría que cuantificarlos siguiendo determinados criterios, como pueden ser: resultados en la producción a partir de la introducción de la informática, costo del sistema según procedimientos anteriores, costo de procesamiento en un centro de uso colectivo, costo de no tener la información deseada, etc.
b) La eficiencia de la producción informática. La obtención de los resultados en el tiempo previsto es esencial en el trabajo del centro y en el grado de satisfacción de los usuarios. Sin este elemento la toma de decisiones no tendría el efecto y eficacia deseada. La regularidad en el cumplimiento de los plazos previstos es un elemento necesario para conocer la utilidad del sistema informativo como apoyo al sistema de dirección.
c) La situación del personal. El diagnóstico deberá evaluar también la plantilla del centro de cómputo, la calificación del personal, la cantidad en relación con el tamaño del centro, el grado de desarrollo de las tareas, las características de la actividad fundamental, etc. El grado de satisfacción del personal en la aplicación de la técnica en particular y perspectiva de desarrollo son otros factores que requieren un análisis determinado.
d) La posición del centro de cómputo dentro de la estructura de la empresa. En este punto se debe evaluar cuáles fueron los criterios para ubicar el centro en la estructura orgánica de la empresa. Estos criterios pudieron haber sido: situar la responsabilidad al área que se define como mayor usuario; establecer un centro como mayor usuario; establecer un centro para cada usuario importante, o situarlo al nivel más alto de la estructura

jerárquica, cada uno con sus pro y sus contra. Igualmente se debe analizar la división interna del centro; aunque para esto no hay fórmulas únicas, si debe guardar determinada relación con la posición del centro dentro de la empresa, el tamaño del equipamiento y posibilidades del software, carga de trabajo y potencial existente, concepción metodológica del proceso informático, etc. Lo justo o lo adecuado de cada uno de estos elementos deben ser evaluados por la auditoría.

e) La calidad de los sistemas. No menos importancia tiene el enjuiciar la calidad de los sistemas desde un punto de vista funcional. En cada sistema debe analizarse las salidas que se produce y su utilidad, cantidad y calidad, las entradas que se requieren y el proceso de captación que necesitan; los ficheros con los cuales trabaja y si sus organizaciones son las precisas; y por último, el encadenamiento de los procedimientos que se requieren para obtener los resultados deseados.

f) El grado de actualización de la metodología de trabajo establecida. La metodología concebida para los trabajos de análisis, programación y explotación debe ser igualmente analizada para medir su incidencia dentro de la organización del proceso informático. Además, este es un factor que debe ser analizado de forma de poder evaluarlo en relación con el nivel de desarrollo alcanzado en un momento dado en las distintas técnicas asociadas a los sistemas automatizados.

g) El nivel de integración de informática. En este sentido es necesario conocer los criterios que se utilizan para introducir las distintas aplicaciones dentro de la empresa como un sistema, cómo juegan estos criterios con la existencia de un plan general de tratamiento de la información, y su integración con las funciones particulares de cada unidad de la empresa.

h) Las características del hardware y del software. Este punto debe considerar la validez de las decisiones que se tomaron al definir la configuración de la máquina y su correspondiente software. Igualmente debe dar elementos sobre la proyección que el equipamiento presenta, o las necesidades de ampliar el parque, modificarlo o ir a una solución distribuida de los tratamientos, etc.

i) El nivel de seguridad de los recursos físicos e informativos del centro. En este sentido el diagnóstico debe estudiar las reglas de control establecidas y los dispositivos con que se cuenta para evitar que el sistema acepte datos incorrectos, que los datos almacenados sufran algún tipo de daño o alteración, que la información de salida sea exacta y se ofrezca en el momento adecuado, todo lo cual permitirá reducir al máximo los principales riesgos que tienen que enfrentar los sistemas de procesamiento de datos, etc. Es necesario evaluar no sólo la existencia del dispositivo o regla de seguridad que en particular se requiere, sino además, si el mismo se corresponde con el costo de lo que se quiere controlar.

Es evidente que al determinar hacer una auditoría para conocer todos o algunos de los aspectos aquí enunciados, el diagnóstico no puede quedar en una declaración de principios, sino que además cada aspecto debe tener soluciones alternativas que permitan un mejor funcionamiento del servicio que se presta. Por tanto para cada uno de los puntos anteriormente tratados deben existir determinadas recomendaciones que garanticen una utilización más racional de los recursos con que cuenta para la función de automatización de los sistemas informáticos.

2.4. TÉCNICAS DE AUDITORÍA EN INFORMÁTICA

Uno de los factores primordiales para el auditor en informática en el desempeño eficiente de su trabajo, es el conocimiento y aplicación de los métodos, técnicas y herramientas comúnmente aceptados para el área de informática en las organizaciones.

En la medida en que el auditor en informática posea experiencia y conocimientos actualizados sobre los diferentes aspectos que evaluará, tendrá buenos o malos resultados en el desarrollo de su trabajo.

Como se mencionó en el capítulo primero, las técnicas de auditoría son los métodos prácticos de investigación y prueba que el auditor utiliza para lograr la información y comprobación necesarias para poder emitir su opinión profesional.

En el caso del Auditor en Informática, las técnicas que utiliza para el buen desempeño de sus funciones, generalmente son las mismas que las utilizadas en la auditoría tradicional y que fueron tratadas en el capítulo primero :

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaraciones o certificaciones
- Observación, y
- Cálculo

El auditor en informática debe adecuar o modificar las técnicas antes mencionadas, de manera que le sean útiles para efectuar la revisión al departamento de informática en sus diferentes áreas de trabajo (administración, dirección, control interno, desarrollo de sistemas, redes, telecomunicaciones, seguridad, planeación, investigación, entre otras).

El auditor en informática debe conocer las diferentes técnicas de auditoría que se utilizan mediante la computadora y elaborar la documentación que debe generarse como evidencia del trabajo realizado, garantía de su futura operación y mantenimiento.

El uso de la computadora con todas sus posibilidades como una herramienta de auditoría, tanto externa como interna, es cada vez más frecuente y necesaria, ya que incrementa sensiblemente la eficacia y eficiencia en esta disciplina, le proporciona mejores alternativas al auditor, y en muchos casos resulta la única manera de analizar y evaluar los procesos automatizados, es decir, desarrollar auditoría en informática sin usar la computadora, es improcedente.

El utilizar la computadora como una herramienta para llevar acabo el proceso de auditoría es conocido comúnmente como "Técnicas de Auditoría Asistidas por la Computadora" (CAAT, Computer Aided Audit Technique).

Algunas de estas técnicas son conceptos desarrollados específicamente para apoyar a objetivos de auditoría en informática; otras técnicas han sido desarrolladas aprovechando las facilidades naturales de las computadoras, de los sistemas operativos y del software de base.

Algunas consideraciones que se deben tener para el uso de técnicas de auditoría asistidas por la computadora son

- Personal altamente capacitado
- Falta de pistas de auditoría en reportes o pantallas de consulta
- Mayor alcance en presencia de control interno débil
- Búsqueda de excepciones, errores o irregularidades
- Margen de tolerancia para excepciones o diferencias
- Manejo del volumen o cantidad de registros a imprimir a detalle
- Cuando sea posible, cuantificación del efecto total de la excepción, error o irregularidad detectado
- Documentación de pruebas de auditoría con la computadora

Utilización de paquetes de auditoria comerciales

Paquete de auditoría es el término empleado para un conjunto de programas que tienen la capacidad de procesar uno o varios archivos de datos en medios magnéticos, funcionando bajo el control de parametros definidos y aplicados por el auditor.

Esta es una técnica ampliamente usada por lo auditores en informática, ya que permite al auditor analizar uno o más archivos del sistema computarizado.

Este tipo se software de auditoría, normalmente es capaz de producir totales, dar sumas cruzadas, seleccionar una muestra estadística, seleccionar transacciones, comparar totales y ejecutar cálculos sobre diversos elementos contenidos en uno o varios archivos. Esta técnica de auditoría esta orientada a probar datos pero ayuda poco a probar la lógica de los programas de cómputo.

Desarrollo de programas de auditoria a la medida de las necesidades

Esta técnica esta mas difundida en empresas o instituciones que no están en posibilidades de adquinr un paquete de auditoría, o se trata de entidades cuyas actividades son unicas en el país y no esta disponible un paquete comercial que satisfaga las necesidades específicas de auditoría.

El empleo de esta técnica exige que se disponga de especialistas por parte del equipo de auditoría y puede resultar costoso, ya que involucra la elaboración, prueba, ejecución y documentación de los programas de auditoría, aunque son mas flexibles que los paquetes de auditoría.

2.4.1. TÉCNICAS DE APOYO A LA ADMINISTRACION

Existen tecnicas especificas orientadas al apoyo de la administracion de la función de auditoría que han sido claramente identificadas, sin embrago las posibilidades que se tiene en este aspecto son prácticamente ilimitadas en las diferentes etapas del proceso administrativo, como por ejemplo en la planeación, supervision y control de los trabajos de auditoría.

Seleccion del área a auditar

Esta es una tecnica computarizada, cuya aplicación esta fundamentalmente orientada a organizaciones que operan en localidades multiples, ayudando al auditor en la selección de cuáles de ellas auditar.

El objetivo de esta técnica es el optimizar el uso de los recursos limitados de auditoría, señalando las áreas con mayores problemas potenciales y direccionando su atención a las de mayor relevancia. Esta técnica consiste en el desarrollo de una matriz del perfil de localidades, proporcionando información clave de cada localidad.

Los indicadores fundamentales pueden ser financieros o aspectos de control que puedan ser usados para evaluar la situación de la localidad y su nivel de desempeño.

Scoring

Esta es una técnica de planeación que ayuda al auditor en informática a seleccionar sistemáticamente el sistema de información computarizado a ser auditado y, esta orientada a maximizar la eficiencia de auditoría. La técnica identifica las características cuantificables en el sistema automatizado en particular, que son significativas desde el punto de vista de análisis de riesgos. Dichas características son ponderadas y combinadas para obtener la calificación de un sistema. Varios sistemas automatizados pueden ser calificados en ésta forma y, entonces puede ser comparado el beneficio potencial al revisar un sistema u otro. Algunos factores que pueden ser considerados al aplicar esta técnica pueden ser:

- El sistema tiene impacto financiero o no
- La cantidad de archivos que maneja o controla

- El número de módulos y programas por módulo
- La tecnología usada, recursos que utiliza, empleo de comunicaciones o no
- El número de reportes que genera
- El número e importancia de usuarios involucrados
- La experiencia de personal de informática
- El grado de involucracion del usuario y el auditor en el ciclo de vida de desarrollo del sistema

Multisite Audit Software

Esta técnica de auditoria puede ser usada por organizaciones en que la operación de sistemas automatizados se lleve a cabo en centros de cómputo regionales y el desarrollo del sistema sea centralizado.

La aplicación de éste tecnica considera el desarrollo de programas de cómputo para auditoria que serán usados para probar aplicaciones automatizadas en operaciones en múltiples localidades. Para un efectivo empleo de ésta técnica es necesario que los equipos computarizados sean similares.

Esta técnica abate costos, aumentando los beneficios en cuanto a la eficiencia, reducción de entrenamiento, incremento en control y estandarización de los programas de cómputo utilizados en auditoria. Las etapas para desarrollar ésta tecnica se enuncian a continuación:

- Identificar las areas a auditar
- Definir los objetivos de auditoria
- Analizar el sistema auditado
- Definir procedimientos de auditoria
- Desarrollar los programas de cómputo para pruebas de auditoria
- Probar los programas de cómputo para pruebas de auditoria
- Preparar la documentación técnica y de operacion
- Distribuir el software
- Solicitar la retroalimentación del personal de campo y
- Evaluar los resultados de la prueba y sacar conclusiones

Centro de competencia

Un centro de competencia es un centro de cómputo establecido en una localidad central que es responsable de la ejecución de los programas de cómputo para pruebas de auditoria. El centro de competencia recibe archivos de datos de otras localidades, ejecuta los programas de cómputo, y distribuye los resultados a los diversos auditores.

Las responsabilidades que generalmente se reconocen en un centro de competencia son las siguientes:

- Desarrollar el software de auditoria para requerimientos especificos que no puedan ser satisfechos por paquetes comerciales
- Instalar y ejecutar el software de auditoria y distribuir los resultados
- Custodiar la biblioteca de respaldos de archivos de datos y software de auditoria
- Mantener procedimientos de recuperación
- Dar asistencia técnica en ejecución del software de auditoria
- Establecer y mantener actualizados procedimientos de recepción, transmisión, almacenamiento, destrucción y seguridad de archivos de datos y programas
- Obtener el hardware y software para cumplir con las responsabilidades anteriores

2.4.2. TÉCNICAS PARA AUDITAR SISTEMAS COMPUTARIZADOS

La auditoria de sistemas computarizados es una de las areas de participación fundamentales de la auditoria en informática y está orientada a la verificación de los controles en la

etapa de entrada, proceso y salida de datos, para promover que los resultados del sistema sean confiables y de calidad.

En esta área de participación es en donde se han desarrollado mas técnicas de auditoría en informática, ya que aquí se verifica el procesamiento de los sistemas en operación. El objetivo principal de estas técnicas es verificar que los procesos y los controles incorporados en los sistemas computarizados, los hagan confiables y no existan debilidades que los expongan a riesgos significativos.

En esta área también se verifica que el sistema este funcionando de acuerdo a los requerimientos del usuario y a la normatividad externa e interna.

Lote de datos de prueba

La utilización de esta técnica consiste en la preparación de juegos de datos de entrada al sistema que le presenta un repertorio de transacciones reales y ficticias, para que serán procesados por el programa usado en la operación normal de los procesos, con el objeto de identificar resultados predeterminados, verificación de la efectividad del rechazo de información errónea y no autorizada en sistemas en línea, donde los archivos se actualizan en el momento en el que se realizan las transacciones. La prueba de auditoría no se realiza al mismo tiempo que la producción normal, sino posteriormente.

Estas pruebas son normalmente almacenadas en archivos temporales para evitar interferencia con la operación normal y real.

El auditor deberá tener cuidado en todas las ramificaciones de los sistemas para no alterar información real, así como considerar todas las condiciones variables incorporadas en los programas ejemplos:

- Rutinas de validación de transacciones de entrada en línea
- Cálculos de nomina, facturas, impuestos, descuentos, sumarizaciones, antigüedad de saldos, etc.
- Valuación de inventarios físicos, explosión de materiales, clasificaciones, etc.

Esta técnica tiene la característica de que puede ser utilizada por personal con poca experiencia en procesamiento de datos, requiriendo poca asistencia técnica.

Simulación paralela

Esta técnica consiste en el desarrollo por el auditor de su propio programa, a través de especialistas, para realizar el mismo proceso que efectúa el programa de producción del sistema auditado, utilizando la misma información fuente, "archivos de datos vivos", para luego comparar los resultados de ambos. El propósito de esta técnica es comprobar la lógica de los programas en operación. Su uso es conveniente en sistemas que manejan grandes volúmenes de datos.

Datos de prueba integrados (Integrated test facility)

En este caso se establece una entidad ficticia dentro del proceso (división, subsidiaria, sucursal, etc.) en donde se almacenarán los datos del auditor, pero con la peculiaridad de que serán procesados al mismo tiempo y las transacciones reales se registran, teniendo como marco de referencia el ciclo de operación normal de los sistemas de información.

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

Esta técnica es muy útil en sistemas complejos y con un grado elevado de transformación de la información, sin dejar huella visible como en el caso de sistemas en línea.

Al aplicar esta técnica deberá cuidarse la debida autorización de la gerencia y la correcta y oportuna coordinación con los diversos departamentos involucrados, pues se introducirá información falsa en el flujo normal y deberá eliminarse posteriormente de los archivos reales.

Módulos de auditoría integrados (Embedded audit modules)

Esta técnica consiste en incorporar módulos, programas o rutinas en los programas de la producción normal del sistema de información computarizado auditado y ejecutarlos en el momento de operación

Estos módulos como programas o rutinas del auditor son insertados en los puntos de los programas determinados por el auditor, señalando los criterios de selección de transacciones. Funcionan permanentemente en los sistemas conforme estos operan realmente de manera que operaciones no usuales o fuera de ciertos límites son detectadas y registradas inmediatamente en archivos para uso de auditoría y utilizar métodos manuales o automatizados para analizarlos.

Esta técnica requiere la participación del auditor en las especificaciones para el desarrollo y mantenimiento de los sistemas de información computarizados

Se requiere para el empleo de esta técnica de amplios conocimientos de computación e integración con los diversos departamentos que estén involucrados

Registros extendidos

La técnica de registros extendidos reúne los datos para propósitos de análisis y evaluación de auditoría a ser incorporados en los archivos o bases de datos de la producción normal del sistema de información a auditarse

Análisis de la lógica de los programas

Consiste en solicitar el programa fuente correspondiente a programas de producción, estando plenamente seguro de ello y estudiarlo para determinar su confiabilidad

Esta técnica es útil en sistemas sencillos, pero en sistemas complejos puede resultar muy riesgoso, además de la asistencia técnica que se requiere

Imagen del contenido de memoria

Tanto a los auditores como al personal del centro de cómputo, frecuentemente encuentran difícil la reconstrucción de la toma de decisiones de los programas de computo.

La causa es una posible deficiencia en tener juntos todos los elementos involucrados en el proceso de datos. Esta técnica consiste en imprimir cierta parte de la memoria, como son los valores que tienen ciertas variables en el momento de la toma de decisiones y analizar la información

En estos casos se requiere de una lógica especifica a ser programada en el sistema y hace necesarios amplios conocimientos técnicos para leer la sección extraída

Esta técnica ayuda al auditor a responder preguntas de porque un sistema automatizado genera resultados cuestionables si se alimentan ciertos datos de entrada

2.4.3. TÉCNICAS PARA LA REVISIÓN DE CONTROLES GENERALES

Existen algunas técnicas que se han desarrollado para el apoyo de la auditoría, aunque en este caso su orientación no es sólo a una aplicación especial, sino a la verificación de controles generales. Algunas de ellas pudieran ser interpretadas y utilizadas como técnicas para la revisión de sistemas de información computarizados, sin embargo para estos efectos se les ha considerado en su posible aplicación genérica

Seguimiento o rastreo (Tracing)

Esta técnica consiste en listar los pasos de la lógica de los programas de cómputo, es decir, el flujo que sigue una transacción en el procesamiento electrónico de ella, permitiéndole al auditor verificar el cumplimiento de políticas y procedimientos establecidos por la organización.

La técnica de rastreo muestra las instrucciones ejecutadas en un programa y su secuencia.

Generalmente el "tracing" no es una técnica desarrollada por el auditor pero puede aplicarla en su trabajo. Normalmente "tracing" son rutinas opcionales proporcionadas por el proveedor.

Mapeo (Mapping)

El mapeo es una técnica que puede utilizarse para identificar la lógica que no ha sido probada de un programa específico. Esta técnica también identifica la cantidad de tiempo de cpu consumida por cada segmento de un programa de cómputo.

El intento original del mapping fue el ayudar a los programadores a asegurar la calidad de sus programas. Sin embargo, los auditores pueden utilizar la técnica del mapping para localizar códigos (instrucciones) no ejecutados. El análisis derivado del empleo de ésta técnica, puede proporcionar al auditor una imagen de la eficiencia en la operación de los programas de cómputo, y pueden revelar segmentos de un programa no autorizado incluidos con fines ilícitos.

Este software monitorea la ejecución de un programa de computo contando el número exacto de veces que cada instrucción del programa es ejecutada, también midiendo el tiempo de cpu consumido por cada una de ellas.

El resultado de éste tipo de software incluye alguna o toda la información siguiente:

- Una lista de cualquier segmento del programa no ejecutable
- Una lista de los pasos que consumieron más tiempo
- Una lista del programa fuente mostrando el numero total de veces que cada instrucción fue ejecutada

Bitácora (Job accounting data analysis)

El análisis de la información relativa al uso de la computadora, archivos utilizados, programas ejecutados, tiempo máquina empleado, interrupciones, registros procesados, cambios de programas, etc., podrá darle al auditor excelentes pistas de auditoría.

La interpretación de la bitácora puede resultar difícil para el personal con pocos conocimientos de computación.

2.5. PERFIL DEL AUDITOR EN INFORMÁTICA

La elección de quién debe hacer la auditoría puede estar enmarcada en alguna de las alternativas siguientes: interna, externa o una combinación de ambas.

La auditoría interna la puede realizar una empresa que por su volumen de actividad y grado de complejidad puede tener una cantidad de especialistas tal que le permita seleccionar el más adecuado para hacer un análisis desde "dentro". Este caso es el menos frecuente.

La auditoría externa puede ser la más indicada, ya que requiere un mayor nivel de competencia, imparcialidad y objetividad. Los problemas se identifican más fácilmente desde fuera.

La actividad combinada es otra alternativa que no se excluye porque siempre la auditoría interna tiene determinadas limitaciones que pueden ser suplidas o complementadas con una auditoría externa.

Definido el tipo de auditoría, es de vital importancia la elección del auditor. En el plano técnico, este profesional debe conocer los fundamentos de las computadoras, tener nociones de análisis y programación, así como de operación y organización del trabajo informático. En el plano personal, debe poseer una gran capacidad de análisis y síntesis, y competencia profesional que le facilite el diálogo con especialistas. Debe reunir, además, buenas condiciones para el trato humano y tener conocimientos de contabilidad, análisis económicos, organización, y de las características y objetivos de la empresa.

Con estos conocimientos los auditores deben estar en condiciones de solicitar, de manera precisa, de los especialistas que formen parte de equipo auditor, los programas y trabajos necesarios, y también deben saber interpretar y valorar sus resultados.

El conjunto de conocimientos que deberá tener el auditor en informática dependerán de las características de la empresa, tecnología, centralización y descentralización de las funciones de informática. Sin embargo, en el desempeño de la auditoría de informática deben formarse equipos multidisciplinarios, aprender a trabajar juntos y complementarse en cuanto a conocimientos y experiencias. El auditor en informática, al igual que cualquier auditor, debe estar familiarizado con la organización y las funciones de cada una de las áreas de la empresa, así como las operaciones que se realizan. Existen dos grandes áreas de participación de la auditoría en informática:

1. La Auditoría de los Controles Específicos, la cual abarca el ciclo de vida del desarrollo de un sistema de información, en el que el auditor debe revisar que exista una metodología y que ésta a su vez, sea adecuada al entorno tecnológico de la entidad, además de supervisar que se cumpla en el caso de un sistema de información. Y la auditoría de sistemas de información en operación.

2. La Auditoría de los Controles Generales, la cual abarca la revisión de los aspectos cuyas debilidades afectan a cualquier recurso informático en general, como lo es:

   - La administración de la función de informática
   - Adquisiciones de bienes informáticos
   - La seguridad física y lógica
   - Sistema operativo

Los conocimientos con los que debe contar el Auditor en Informática son, entre otros los siguientes:

- Conocimientos del diseño conceptual de las aplicaciones
- Descripción y organización de los datos
- Del ambiente en que operan
- Conocimiento y experiencia profunda en labores de auditoría[1]

[1] Apuntes del curso de Auditoría en Informática de la M. en C.C. Marcia Toriz García

2.6. SOFTWARE DE AUDITORÍA EN INFORMÁTICA

Como se mencionó anteriormente, un paquete de auditoría es el término empleado para un conjunto de programas que tienen la capacidad de procesar uno o varios archivos de datos en medios magnéticos, funcionando bajo el control de parámetros definidos y aplicados por el auditor.

Estos programas han sido desarrollados por diferentes proveedores y por firmas de contadores o consultores, y pueden ser adquiridos, con el propósito de que de una manera rápida y sencilla el auditor, después de un breve entrenamiento, pueda obtener la evidencia suficiente y competente que requiera el caso, siendo su empleo sencillo y menos costoso que programas desarrollados a la medida.

Este tipo de software de auditoría normalmente es capaz de producir totales, dar sumas cruzadas, seleccionar una muestra estadística, seleccionar transacciones, comparar totales y ejecutar cálculos sobre diversos elementos contenidos en uno a varios archivos.

Históricamente este tipo de software ha operado en modo batch, pero actualmente permiten la ejecución en línea. Los archivos de datos pueden estar en diferentes dispositivos magnéticos, tales como cintas o discos, y en diferente organización, por ejemplo secuencial o de acceso directo. Los parámetros de entrada aplicados por el auditor especifican el tipo de archivo que se este procesando, el proceso lógico a ser aplicado a los archivos y el tipo de salida requerido (por ejemplo el tipo de reporte). Así, el auditor puede utilizar los paquetes de auditoría comerciales para probar un sistema computarizado en diferentes partes y de diversas formas. Las funciones más comunes de los paquetes de auditoría son:

- Sumarización
- Sumas cruzadas
- Selección de datos y presentación detallada
- Diversos cálculos matemáticos
- Formateo de reportes
- Comparación de 2 generaciones del mismo archivo de diferentes fechas, o dos archivos diferentes a la misma fecha
- Clasificación
- Empleo de muestreo estadístico
- Comparación de diferentes archivos

Algunos beneficios de utilizar paquetes de auditoría comerciales son los siguientes:

- De fácil uso para el auditor
- El paquete puede procesarse en hardware independiente
- Análisis independiente de archivos, sin depender del personal del centro de cómputo
- Uso efectivo y eficiente del computador sin necesidad de entrenamiento intensivo y complejo
- Modificación de los procedimientos de auditoría para adaptarlos a los cambios operativos con esfuerzos reducidos
- Un paquete de auditoría puede utilizarse en la revisión de varios sistemas de información

Pasos para utilizar los paquetes de auditoría:

- Definir los objetivos de auditoría
- Preparar las especificaciones de la entrada de datos
- Preparar las especificaciones del procesamiento
- Preparar las especificaciones de las salidas (reportes y pantallas de consulta)
- Procesar los archivos de datos ejecutando el paquete de auditoría
- Revisar y evaluar los resultados de la prueba

Funciones de un paquete de auditoria

Los paquetes de auditoria más conocidos actualmente son para realizar una revisión de los registros almacenados en las bases de datos o se aplican en el reconocimiento del grado de seguridad en redes de una plataforma determinada. No descartamos otros como los dedicados a la seguridad física, a los accesos al equipo de computo, etc., pero los mencionados anteriormente son los que más han proliferado

En seguida listamos las principales funciones con las que debe contar un paquete de auditoria que permita una revisión a la consistencia y confiabilidad de una base de datos:

- Lectura de archivos y creación de archivos de trabajo
- Facilidades para introducir datos y crear archivos propios de auditoria
- Selección de registros basada en determinados parámetros (Criterio del Auditor)
- Muestreo estadistico
    - Selección de registros:
        - Al azar
        - A intervalos
        - Secuenciales
        - Regulares
        - Todos
- Distribución de Frecuencia
    - Perfil de la población
- Operaciones aritméticas
- Totales y subtotales
- Edad de los registros
- Comparación de archivos
- Generación de informes
    - Formato Patron
    - Formato libre
- Salidas para programas del usuario
- Posibilidades de prueba de programas

Podemos notar que aparecen funciones que sirven para generar reportes y papeles de trabajo de auditoria. En capitulos anteriores se explicó la importancia de contar con un respaldo de cada una de las revisiones que hacemos como auditores, para que si son madera de una observación se cuente con el soporte necesario para someterse a revisión de la compañia auditada.

Algunos paquetes de auditoria

Encontramos algunos paquetes dedicados a diversas actividades de apoyo al auditor, entre los más importantes y conocidos se encuentran

AUDIT

Un enfoque que consiste en revisar los procedimientos de auditoria empleados en forma manual y determinar su aplicación a través del computador.

AUDITAPE

Inclusión de rutinas especiales de cómputo en los procesos normales de operación, como puede ser la revisión de egresos de caja.

AUDITRONIC

Para auditoría de inventarios, en estas pruebas se pueden efectuar comparación de registros de inventarios contra archivos que contengan las compras efectuadas al respecto[1]

IDEA (Interactive Data Extraction and Analysis)

IDEA es un sistema diseñado para soportar las decisiones que se toman sobre datos importantes para la empresa basadas en un análisis por medio de la computadora. La creación de IDEA se basó en la resolución de dos problemas: el primero fue desarrollar una entrada para distintos tipos de bases de datos con el fin de construir un conjunto relevante de indicadores o factores. El segundo fue la formalización de métodos y reglas que soporten una correcta interpretación de estadísticas calculadas sobre bases de datos y de esta manera se logre la mejor toma de decisiones.

Actualmente IDEA ha resuelto estos problemas; es un sistema inteligente de extracción de datos con el cual es posible presentar y calcular importantes grupos de estadísticas específicas.

Para un futuro el análisis e interpretación de estos indicadores será basado en una tecnología de sistemas expertos, actualmente se está diseñando y desarrollando sobre esto.

La gente que produce estadísticas, a menudo combina cantidades almacenadas en diferentes sistemas y alojadas en distintas lugares. Esta tarea requiere librar algunas dificultades, desde tener diferentes manejadores de bases de datos con distintos procedimientos de acceso a los registros hasta contar con varias bases de datos que tengan múltiples formatos y codificaciones. IDEA está tratando de formalizar la interacción entre la lógica de obtener los datos, los cuales son usados en el proceso de toma de decisiones, y la organización física de la bases.

"IDEA es una herramienta que puede incrementar fácilmente la productividad de un auditor, contador o gerente de finanzas que necesite desplegar, analizar, manipular o extraer datos de algun sistema. Este software brinda su mayor funcionalidad cuando lo utilizan auditores de procesamiento electrónico de datos y especialistas en sistemas.

Existe una versión para windows que utiliza las interfaces estándar y hace más fácil las consultas en archivos de datos, el cálculo de totales o promedios, la detección de transacciones fuera de criterios establecidos o con datos extraños o inusuales. Ventajas del software:

- Funciones de análisis sencillas.
- Consultas, extracciones, estratificaciones y sumarizaciones de archivos de datos.
- Se permiten agregar columnas calculadas para verificar la exactitud de las operaciones.
- Detección de datos duplicados y faltantes.
- Indexación, ordenamiento y reportes con varios niveles de control de totales y vista de impresión preliminar.
- Editor gráfico amigable para construcción de expresiones.
- Planeación, extracción y evaluación.
- Gran importación y exportación de datos incluyendo soporte de ODBC, ASCII, EBCDIC y otros tipos complejos de datos encontrados en sistemas basados en mainframe, mini y microcomputadora. Con el ODBC se puede importar archivos de Access, Excel, Paradox, Oracle, Sybase y muchos otros."[2]

ACL

Su función es apoyar a los usuarios en el manejo y análisis de información para incrementar su productividad y la capacidad de respuesta en la generación de resultados interactivos y de reportes.

Se creó como un programa interactivo para enseñar auditoría por medio de la computadora y ahora ha extendido su aplicación al área de finanzas, contabilidad, compras y

[1] Apuntes del curso de Auditoría en Informática de la M. en C.C. Martha Torre García.
[2] IDEA on the Web. http://www.cica.ca/idea/

ventas. Corre en ambientes de PC's, Macintosh, mainframes y redes Novell y próximamente saldrá la versión para Windows NT.

Está orientado a cualquier persona que lleve a cabo análisis exhaustivos de información y se aplica en todas las áreas de información ejecutivas para el procesamiento de información en campos de texto, numéricos y de fechas.

Este paquete es desarrollado por la compañía canadiense ACL Service Limited. Permite crear campos calculados, determinar antigüedad de transacciones comparadas a una fecha de referencia específica, calcula estadísticas de campos numéricos y automatiza tareas repetitivas. Puede producir gráficas, crear resúmenes, conteos de registros, ordenar e indexar archivos y ver datos en un formato de hoja de cálculo[3].

AUDITORÍA FINANCIERA/DICTAMEN

Para automatización de papeles de trabajo de auditoría. El más reciente y muy completo de una empresa denominada Sistemas Estratégicos S.A. de C.V.

Otros paquetes de auditoría son: Aditrack, Applaud, Cars y Panaudit.

[3] El Norte. Interfase. Incrementan productividad de sistemas. Lunes 22 de abril de 1996.

2.7. PROBLEMÁTICA ACTUAL DE LA AUDITORÍA EN INFORMÁTICA

Desde que las computadoras surgieron, su desarrollo como herramienta de trabajo ha sido increíblemente veloz y redituable. Contamos ahora con posibilidades de agilizar la elaboración de documentos, papeles de registro financiero y contable, planos arquitectónicos, diseños industriales, creaciones artísticas y desarrollos tecnológicos y científicos con el apoyo de recursos computacionales cada día mejor elaborados. También tenemos la posibilidad de contar con información localizada en otro lugar físico, como otro edificio, otra ciudad u otro país. Las telecomunicaciones han logrado que los datos ya no estén necesariamente en el mismo lugar donde se actualizan.

A estas dos grandes posibilidades de la computación se podrían agregar los avances en multimedia, que cada día parecen ser más una parte integral de toda computadora, los avances en servidores de alta velocidad, los desarrollos en la inteligencia artificial y la educación a distancia, que en general hacen del desarrollo computacional un fenómeno revolucionario e incontrolable en cuanto a su aplicación.

Como vimos en el primer capítulo, hacia finales del siglo XVI ya existían auditores en Inglaterra, por supuesto que distintos a los actuales, y los primeros registros de una contabilidad se pueden apuntar hacia la época de la Revolución Industrial. Las auditorías aún más formales se dan a finales del siglo XVII, siendo de carácter fiscal y contable.

Por otra parte la primera computadora fue desarrollada en 1940 (ENIAC), y sus características se alejan enormemente de las que ahora localizamos en una computadora comercial. El primer microprocesador se desarrolla a finales de la década de los 60's y su comercialización se da por 1975.

La intención de este comparativo es para hacer notar como la auditoría en materia contable-financiera ha tenido un tiempo mucho mas amplio para su desarrollo que la auditoría en informática. El corto tiempo en el que la informática ha evolucionado provocó que el desarrollo de controles en el manejo de los bienes relacionados a esta área, sea casi inexistente hasta hace algunos años. Actualmente el surgimiento de dichos controles se da mas por necesidad que por estándar y los problemas que solucionan sólo son de manera correctiva. Actualmente ya existen organizamos encargados de la reglamentación y estandarización del manejo de bienes informáticos en otros países.

En México son pocos los lugares donde la auditoría en informática se ha tomado en cuenta para su estudio y especialización y no es fácil encontrar institutos que brinden estándares en informática y muchísimo menos empresas que cuentan con una área definida para tal efecto. Hoy, sólo los grandes despachos contables dan el servicio de auditoría en informática y lo orientan a empresas también muy grandes que por sus recursos económicos pueden invertir en esto. La problemática que ha generado el vertiginoso avance de la actualización en cómputo contra la falta de revisiones a las inversiones, administración, control, registro y manipulación de bienes informáticos, se proyecta en dos caminos: la compra desmedida e injustificada de equipo y su mal uso, que provocará al final obsolescencia, improductividad y atentados contra la seguridad de la información.

La auditoría en informática atraviesa por algunos problemas, no se toma en cuenta, se trata como parte de una auditoría contable financiera y no se encuentran bases para llevarla acabo y en su caso respaldarla.

Para muchas empresas el uso y adquisición de equipo e implementos de cómputo, tiene sólo que ver con un especialista técnico en soluciones y el proveedor. Las más de las veces el requerimiento de equipo y sus características surgen de la moda, de el "no quedarse atrás", de la modernización y de razones que nunca han tenido que ver con un análisis de necesidades y de infraestructura corporativa. Cuando el equipo ya esta comprado, ¿a quién le importa como se use?, siempre y cuando los reportes se vean muy bonitos. Es por esto que decimos que la auditoría en informática no se toma en cuenta y nadie piensa que sea necesaria, unos por temor a ser cuestionados en el uso que le dan, otros por egoísmo cultural que no les permite aceptar que alguien les diga como hacer algo que supuestamente sólo ellos hacen y, otros más, por pensar que la computación es una solución espontánea, es decir que sólo con poner una computadora en un escritorio todo se solucionará.

Tampoco podemos descartar los intentos de empresas que preparan gente en materia técnico-informática para simular una auditoría. Sólo revisan registros contables del equipo, inventario, documentación en adquisiciones, desarrollo, objetivos, políticas y procedimientos en el área de informática. Como quedará claro en este trabajo, esto no es una verdadera auditoría en informática, falta la revisión de muchos controles relacionados a otras áreas y no sólo a los registros en papel.

Por fin, cuando una empresa preocupada por la aplicación de sus bienes informáticos y la rentabilidad que estos le dan, corre el riesgo de iniciar una revisión formal de sus controles, y de encontrarse con que no existe nada escandalizado (el por que de la falta de estándares no es cuestión de este trabajo), y la bibliografía sobre el tema es escasa. Es entonces cuando se basa en los principios de una auditoría común y trata de partir de cero para establecer su propio sistema de revisión. Esto puede llegar a provocar desviaciones en el enfoque de la auditoría y, en la mayoría de los casos, que se de el "aprender a hacer haciendo"

La realización de una auditoría en informática no es fácil de llevar, la diversidad de areas que abarca la computación y aun mas, la proliferación de versiones, tipos, modelos y marcas de los componentes de hardware y software, hacen de este tipo de revisión un reto para cualquier especialista en cómputo. La intención de este trabajo de investigación, es proporcionar una guía que permita conducir los caminos de una empresa que inicie una auditoría en informática y se encuentre con la falta de una metodología para su aplicación.

CAPÍTULO 3

Areas susceptibles de revisión

3.1. ELEMENTOS PARA EVALUAR UN ÁREA

La importancia de conocer con exactitud cuáles areas, relacionadas directa o indirectamente con informática requieren una auditoria, radica en que sus recursos suelen ser altos e importantes para el negocio. Una mala interpretación de las prioridades y necesidades de evaluación de cada una, podria tener un alto costo para el área de informática, sus usuarios y la alta dirección.

Es muy importante aclarar que en ningún momento se ha afirmado que las areas mencionadas sean todas las existentes en cualquier negocio, ni que serán las únicas que se podrán encontrar en las empresas los próximos años. Se han utilizado como referencia pues son las más comunes y homogéneas en empresas grandes, medianas y pequeñas, tanto de la iniciativa privada como del gobierno.

Componentes que se evaluarán por área de revision

Los componentes de las areas de revisión son aquellos que caracterizan a cada una de las areas que serán auditadas. La información mínima que ha de buscar el auditor en informática en cada componente comprende:

- Grado de formalización en el negocio
  - Forma en que se implantó el componente en el negocio
  - Definición de políticas y procedimientos (elaboración, autorización, difusión, entendimiento)
- Grado de cumplimiento
  - Según políticas y procedimientos
  - Manera de llevarlo a cabo (formal e informal)
  - Periodicidad de aplicación (diaria, esporadica, nunca)
  - Responsabilidades (quienes deben y quienes lo ejecutan)
- Grado de actualización
  - Adecuación a requerimientos actuales
  - Autorización de los cambios
  - Responsables de los cambios (quienes deben y quiénes lo hacen)
- Grado de acercamiento a estándares
  - Comparación con estándares nacionales o internacionales
  - Debilidad o inexistencia de estándares, políticas y procedimientos
  - Recomendación de estándares requeridos
  - Adaptación a caracteristicas del negocio

El auditor en informática tiene que verificar cada uno de los puntos mencionados en cada componente de las areas seleccionadas en la etapa de planeación. Esto es con el fin de contar con un panorama concreto y veraz del grado de satisfacción y cumplimiento que se da a la seguridad y control de informática en la organización.

En el momento de evaluar los componentes mediante entrevistas, visitas y cuestionarios, se van detectando las areas de oportunidad emanadas principalmente de las debilidades, carencias o incumplimiento de políticas, procedimientos, métodos y técnicas, entre otros puntos. Sin embargo, los objetivos principales del auditor son:

- Detectar dichas debilidades y carencias
- Encontrar las soluciones de cada una
- Consolidar en soluciones integrales y de valor agregado

Políticas y procedimientos por área de revisión

Las políticas y procedimientos de informática son los elementos o dispositivos que, al ser ejecutados formal y oportunamente, garantizan que las funciones y servicios relacionados con

informática, se lleven a cabo con eficiencia para el apoyo estratégico, táctico y operativo que requiere el negocio.

Dicho en otras palabras: a medida que la función de informática establezca políticas de seguridad y control para cada elemento de su función dentro de la organización y asegure su cumplimiento, mayor certeza y confianza tendrá en brindar continuidad a la operación de los recursos de informática, para el manejo permanente de la información requerida por los diferentes niveles del negocio.

Métodos y técnicas

El auditor debe especificar los métodos y técnicas requeridos para evaluar, de manera completa y eficiente, las áreas de informática seleccionadas.

Para efectos de una visión global de la revisión que debe hacer el auditor en informática de cada una de las áreas, se han unificado las diversas técnicas, métodos y herramientas, que pueden usarse, en doce conceptos. Cada uno encierra una variedad de formas de revisar, validar, probar y verificar que el funcionamiento de cada área sea el correcto.

En capítulos anteriores se han dejado claro las diversas técnicas aplicables a la auditoría desde distintos puntos de vista, en esta parte se unifican y se agregan técnicas de otras disciplinas como los son la metodología de investigación, los costos, el benchmarking y las propias de informática. Los doce conjuntos de técnicas, herramientas y métodos que proponemos son:

Metodología de desarrollo e implantación de sistemas

La metodología de desarrollo de sistemas, es lo que brinda la ingeniería de software al auditor para realizar sus revisiones, con ellas se debe evaluar lo relacionado a la utilización del software de una organización, la planeación que se hace del desarrollo de sistemas, la adquisición de paquetería o de sistemas externos hechos a la medida y de la seguridad y satisfacción que dan a los usuarios los sistemas instalados en la compañía.

Metodología de planeación

Aquí reunimos cualquier herramienta o técnica que permita evaluar, si en cada área se ha hecho una buena planeación, tanto en su desarrollo, creación, aplicación, instalación o desarrollo. Podemos encontrar filosofías como planeación por objetivos, planeación como parte del proceso administrativo, planeación de negocios, la misma planeación de un sistema informático y las técnicas de planeación de redes, su instalación y su crecimiento. Es un conjunto donde encontramos no sólo las primeras fases de una metodología de desarrollo de sistemas, sino la planeación de cualquier actividad que repercute en el área de informática de una compañía.

Cuestionarios

Esta es una de las técnicas que se toma de la metodología de la investigación y que se aplica al desarrollo de trabajos de investigación social, histórica, económica y de otras. En realidad es una herramienta muy importante para el auditor como lo veremos en el capítulo 5 del presente trabajo, en el cual, entre otros puntos, incluiremos los cuestionarios por área de revisión que proponemos para su aplicación en una auditoría en informática.

Un cuestionario es un conjunto de preguntas orientadas al rescate de información que tal vez un usuario no diría en una entrevista, además es un mecanismo de mayor cobertura en cuanto a su aplicación y permite apertar al contestador de hacerlo lo más cómodamente posible para él. Podrá notarse en los cuadros respectivos que todas las áreas necesitan de la aplicación de esta técnica de investigación, el tipo de cuestionario, con preguntas abiertas, cerradas o de opción múltiple, es consideración del auditor de acuerdo al tamaño del área a revisar, el número de usuarios, jefes y directivos, las características de la empresa y su recurso humano y de la profundidad con la cual se quiera indagar la información. En otro apartado de este mismo punto de desarrollo se retoma la importancia de esta técnica.

Entrevistas

Esta herramienta es muy importante para la evaluación de áreas íntimamente relacionadas con los usuarios. Permite además contar con parámetros de medición para una evaluación más profunda e identificada con la empresa. El auditor al revisar los cuestionarios aplicados, las pruebas de rendimiento y las pruebas de seguridad y validación, logra detectar los problemas relacionados con las fallas del personal, desarrolladores o directores. Pero el ¿porqué se dan estas fallas?, que llevarían a una opinión más profunda del estado de una compañía, sólo se conocería si logran aplicar encuestas bien preparadas a su personal clave.

Tal vez la mayor ventaja de la entrevista, es la sincendad con la que el entrevistado contesta frente a frente con el auditor; en el cuestionario, se pueden desviar las respuestas y hasta suplantarse por las de cualquier otra persona, en la entrevista se contesta en el instante y con los recursos con los que cuente en ese momento el personal. Esta técnica también permite dar confianza al personal de la empresa y modificar la idea clásica que se tiene del auditor como alguien déspota y enemigo.

La entrevista se aplica para todas las áreas y permite obtener, de manera muy fiable, la información necesaria para opinar sobre procedimientos, planeación y aceptación del servicio de informática que se da a los usuarios.

Observación

Es una técnica muy utilizada por los investigadores ya que les permite llevar una bitácora de sucesos relevantes, que ellos mismos seleccionan de su entorno. También se le llama observación directa y es aplicada a todas las áreas susceptibles de revisión. Es claro que con esta técnica se pueden verificar cuestionarios, entrevistas y, sobre todo, procedimientos.

Análisis y diseño

Aquí encontramos todas las herramientas de diseño y análisis para el estudio, interpretación y representación. Al igual que en otros, este conjunto no excluye las herramientas que aportan otras disciplinas, a parte de la informática. En análisis se englobaron todas aquellas técnicas y herramientas que permiten hacer una descomposición de algún proceso o problema relacionado con el área de informática. Tal vez el auditor decida siempre utilizar el proceso de análisis de alguna metodología de sistemas, esto es válido al igual que si decide tomar cualquier otro tipo de análisis, como el análisis de costos, el análisis financiero, el análisis de riesgos, etc.

Por lo que respecta al diseño, podemos encontrar aquí la aplicación del diseño orientado a objetos, el diseño propio del desarrollo de sistemas, donde se encuentra el diseño modular, diseño de diagramas como los diagramas de flujo de datos, diagramas entidad relación, diagramas cliente-proveedor y otros que se adapten a las necesidades del auditor.

Se podrá notar como sólo cuatro áreas no utilizan el análisis y diseño, el mantenimiento por que generalmente se da por externos y por que es un procedimiento claro y casi obvio. La investigación tecnológica por que depende demasiado de los intereses de la compañía y no tendría objeto analizar o diseñar algo que sólo consiste en realizar estudios y estar enterado de lo nuevo en tecnología. El área de usuarios de informática por que el auditor no puede diseñar como se comportaran éstos ante el desarrollo de la función informática, solo estudia su grado de satisfacción y no como realizan sus funciones. Por último el control interno no involucra el análisis y diseño por que se implanta como medida preventiva ante cualquier problema que se desarrolle en algún servicio de informática. El control interno, por el mismo, es ya una área que engloba el resultado del funcionamiento de las otras.

Trabajo en equipo

En esta parte resaltamos la importancia que tiene el trabajo en equipo para la obtención de información importante. Con técnicas de trabajo en conjunto como las mesas de discusión, tormenta de ideas y cualquier otra dinamica, se logran conclusiones relevantes y muchas veces más sustentadas. En la aplicación de estas técnicas en las áreas susceptibles de revisión, sólo

descartamos aquellas donde la función que realizan es hecha por terceros o, en su mayoría, el área que cuenta con factores donde intervienen agentes externos

Análisis costo beneficio

Por la importancia que tienen las inversiones en cómputo, en su mayoría cuantiosas y peligrosas, separamos esta técnica de la de análisis y diseño, explicada párrafos atrás. Un área de suma importancia para una organización es la de su gasto y presupuesto, hasta las organizaciones gubernamentales siempre buscan reducir costos o por lo menos cuidarlos, el auditor en informática es el indicado para opinar sobre las inversiones en tecnología, definir si son redituables o si serán inversiones muertas a largo plazo.

Documentación

Este apartado nos permite cuidar que exista una justificación para cualquier cambio en el área de informática. El soporte de las decisiones y acciones de los directivos sobre el futuro de la plataforma de cómputo de una empresa no puede ser tomado con palabras al aire, siempre se debe contar con algo que respalde y asegure que se hicieron las acciones más adecuadas según el momento en que se dieron. De igual manera se cuida que en caso de desastre, por una u otra causa, se cuente con lo necesario para restablecer un servicio y hacer las adaptaciones pertinentes. En general se trata de cuidar, en todas las áreas, que se cuente con respaldo documental de su creación, modificación, actualización y procedimiento de trabajo

Pruebas de auditoria

Aquí toma importancia lo que se expuso en el capítulo 2, en la parte cuatro, sobre las técnicas de auditoría en informática. Le queda al auditor la responsabilidad de escoger que técnicas aplicará a cada situación, en general las pruebas de auditoría son una gran fuente para los papeles de trabajo de los cuales surgen las observaciones de un informe

Control de proyectos

Se refiere a la administración de trabajos y proyectos que las áreas de informática desarrollan para los usuarios. En los cuadros se podrá notar como únicamente se indican con esta herramienta todas las áreas que involucrarían el desarrollo de proyectos para la realización de sus fines

Indices de producción (benchmarking)

Un benchmarking es una prueba de rendimiento que se aplica a una computadora, usando unidades de medición estándar se puede definir si un equipo está trabajando de la mejor manera, si ya es obsoleto o si debe ser reparado. El uso de índices de producción se extiende a los sistemas, donde también encontramos medidas para conocer su productividad. Actualmente con el impulso de las telecomunicaciones, las redes se unen a este enfoque que permite medir su rendimiento, determinando su velocidad de transmisión, peticiones simultáneas de usuarios, etc.

En el cuadro 3.1, se muestran algunas técnicas y herramientas por cada área susceptible de revisión. Estas técnicas y herramientas no son limitativas y el auditor en informática debe considerar aquellas que le sean de utilidad de acuerdo a la auditoría que se esté realizando

Cuestionarios por componentes

Los cuestionarios son una ayuda muy valiosa para el auditor en informática durante el desarrollo del proyecto, ya que son material elaborado, revisado, adaptado y documentado de manera previa.

Cuadro 3.1. Técnicas y herramientas para evaluar las áreas de informática

MÉTODOS, TÉCNICAS Y HERRAMIENTAS REQUERIDAS	ADMINISTRACIÓN DE INFORMÁTICA	DIRECCIÓN Y NIVELES EJECUTIVOS	USUARIOS DE INFORMÁTICA	CONTROL INTERNO
Metodología de desarrollo e implantación de sistemas	Sí	No	Sí	No
Metodología de planeación	Sí	Sí	Sí	No
Cuestionarios	Sí	Sí	Sí	Sí
Entrevistas	Sí	Sí	Sí	Sí
Observación	Sí	Sí	Sí	Sí
Análisis/diseño	Sí	Sí	No	No
Trabajo en equipo	Sí	Sí	Sí	Sí
Análisis costo/beneficio	Sí	Sí	Sí	No
Documentación	Sí	Sí	Sí	Sí
Pruebas de auditoría	No	No	No	Sí
Control de proyectos	Sí	Sí	Sí	No
Índices de producción (benchmarking)	Sí	No	No	No

(Continúa)

Cuadro 3.1. Técnicas y herramientas para evaluar las áreas de informática

MÉTODOS, TÉCNICAS Y HERRAMIENTAS REQUERIDAS	CICLO DE DESARROLLO E IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN	SISTEMAS DE INFORMACIÓN	MANTENIMIENTO	REDES LOCALES
Metodología de desarrollo e implantación de sistemas	SI	SI	SI	No
Metodología de planeación	SI	SI	SI	SI
Cuestionarios	SI	SI	SI	SI
Entrevistas	SI	SI	SI	SI
Observación	SI	SI	SI	SI
Análisis/diseño	SI	SI	No	SI
Trabajo en equipo	SI	SI	No	No
Análisis costo/beneficio	SI	SI	SI	No
Documentación	SI	SI	SI	SI
Pruebas de auditoría	SI	SI	No	SI
Control de proyectos	SI	SI	No	No
Índices de producción (benchmarking)	SI	No	No	SI

(Continúa)

Cuadro 3.1. Técnicas y herramientas para evaluar las áreas de informática

MÉTODOS, TÉCNICAS Y HERRAMIENTAS REQUERIDAS	COMUNICACIONES	HARDWARE	SOFTWARE	SEGURIDAD
Metodología de desarrollo e implantación de sistemas	No	No	Sí	Sí
Metodología de planeación	Sí	Sí	Sí	Sí
Cuestionarios	Sí	Sí	Sí	Sí
Entrevistas	Sí	Sí	Sí	Sí
Observación	Sí	Sí	Sí	Sí
Análisis/diseño	Sí	Sí	Sí	Sí
Trabajo en equipo	Sí	Sí	Sí	Sí
Análisis costo/beneficio	Sí	Sí	Sí	Sí
Documentación	Sí	Sí	Sí	Sí
Pruebas de auditoría	Sí	Sí	Sí	Sí
Control de proyectos	Sí	Sí	Sí	Sí
Índices de producción (benchmarking)	Sí	Sí	Sí	Sí

(Continúa)

Cuadro 3.1. Técnicas y herramientas para evaluar las áreas de informática

MÉTODOS, TÉCNICAS Y HERRAMIENTAS REQUERIDAS	PLANEACIÓN DE INFORMÁTICA	INVESTIGACIÓN TECNOLÓGICA
Metodología de desarrollo e implantación de sistemas	No	No
Metodología de planeación	Sí	Sí
Cuestionarios	Sí	Sí
Entrevistas	Sí	Sí
Observación	Sí	Sí
Análisis/diseño	Sí	No
Trabajo en equipo	Sí	No
Análisis costo/beneficio	Sí	Sí
Documentación	Sí	Sí
Pruebas de auditoría	Sí	Sí
Control de proyectos	Sí	No
Índices de producción (benchmarking)	Sí	No

Algunas ventajas son:

- Objetivos y alcances predefinidos
- Fáciles de aplicar, entender y contestar
- Orientados a que las respuestas sean fáciles de entender y analizar
- Preguntas adecuadas al perfil del personal que contestará
- Revisados y aprobados por el líder del proyecto
- Apegados a las políticas y procedimientos del negocio
- Relacionados con estándares recomendados por cada área
- Con objetivos predefinidos y una secuencia lógica en su aplicación

Los cuestionarios sugeridos para el desarrollo de la auditoría en informática son preguntas encaminadas a detectar el grado de cumplimiento y formalidad que se da a la función de informática en los negocios, de acuerdo con las políticas y procedimientos establecidos en este, así como de los estándares recomendados en el medio informático.

Se recomienda tomar en cuenta las siguientes consideraciones acerca de los cuestionarios:

- Son un punto de referencia que se complementa con entrevistas, visitas para observación directa, juntas, etc.
- Deben ser evaluados, depurados y actualizados conforme a características de las áreas de informática, con el fin de contemplar todos los aspectos de control y seguridad requeridos justo en el momento de la auditoría en informática.
- Las preguntas pueden llevarse en el orden que aparecen o bien en la secuencia y forma que el auditor en informática considere conveniente para el aseguramiento de los objetivos buscados.

Por la importancia que tienen estos cuestionarios hemos decidido proponer una serie de ellos que se detallarán en el capítulo 5, dedicado a la etapa de desarrollo de la auditoría. En ese capítulo se podrán encontrar las preguntas que se aplicarán en cada área susceptible de revisión.

3.2. ADMINISTRACIÓN DE INFORMÁTICA

Encontramos en esta área de revision la parte administrativa del área de informatica, se evaluarán los planes y politicas, su difusion y documentación. Es muy importante el compromiso y apoyo que exista de la alta dirección de la compañía hacia la función de informática

Esta área es la encargada de medir el desempeño de las demás funciones de informática y debe perseguir el logro de los objetivos y metas del negocio. La administración de los recursos informáticos en su conjunto es una de las labores más importantes en un centro de computo

Es un área pequeña pero de gran cuidado para su revisión ya que no faltan directivos que malinterpreten, de buena o mala fe, las verificaciones que hace el auditor. Además se debe dar un enfoque más administrativo que operativo a la revisión y buscar la manera de indagar que tanto apoyo y colaboración hay entre la alta dirección de la empresa y el área de computo

Objetivos de esta revisión

- Verificar que exista un uso eficiente de los recursos de informática (personal, tiempo, tecnología y dinero)
- Asegurar que la función de informática cubra los mayores riesgos y exposiciones existentes en el medio informático
- Asegurar que los recursos de informática (hardware, software, telecomunicaciones, servicios, personal, etc.) esten orientados hacia los objetivos y estrategias del negocio
- Confirmar que exista:
    - Elaboración y formalización de los planes de informática
    - Organización y control formal sobre los recursos de informática
    - Dirección, coordinación y control de los proyectos de informatica
- Comprobar la existencia de servicios de informática documentados y difundidos en el negocio
- Asegurar que existan parametros de medición para el desempeño de cada una de las funciones de informática
- Verificar que se lleve a cabo de manera formal la evaluación del desempeño
- Asegurar la existencia de un comité de informática, alta dirección y usuarios clave
- Confirmar la presencia de un apoyo formal a informática de parte de la alta dirección
- Asegurar que informática elabore, formalice, difunda y aplique sus politicas y procedimientos de manera permanente
- Verificar que existan metodologias, técnicas y herramientas para cada función
- Comprobar que haya un proceso formal de capacitacion y actualización del personal
- Detectar el grado de confianza, satisfacción y respaldo que brinda al negocio la función de informática
- Confirmar que los planes y politicas de informática sean difundidos y conocidos por la alta dirección
- Evaluar el grado de compromiso de la alta dirección con informática para establecer si el apoyo que le brinda es el adecuado

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoria
2. Concertar citas con el personal que se va a entrevistar
3. Revisar el formulario correspondiente y ver la conveniencia de actualización según necesidades especificas del negocio.
4. Ratificar y formalizar las fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este modulo
6. Elaborar un borrador con las principales conclusiones y recomendaciones
7. Revisarlo con el encargado de la función de auditoria en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.

9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de la revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución satisfactoria de sus actividades. Algunas acciones de apoyo serían

   - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimiento del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logrará mediante una capacitación teorico-práctica en los temas que se relacionan con la auditoría en informática

En el cuadro 3.2., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de administración de informática.

Cuadro 3.2. Políticas y procedimientos de control requeridos por área

ADMINISTRACIÓN DE INFORMÁTICA CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Difundir la misión, objetivos y planes de informática en todo el negocio	O	I
Debe existir un organigrama y una descripción de puestos	O	I
Debe haber un manual de políticas de la función de informática	O	I
Capacitación permanente del personal de la función de informática	R	I
Programas de calidad y productividad por puesto, función y servicio	R	I
Uso de metodologías, técnicas y herramientas estándares a nivel de función	R	I
Elaborar un documento que tenga los parametros de medicion por función	O	I
Evaluar permanentemente cada puesto de acuerdo con los parámetros de medición	O	I
Informática ha de participar en el proceso de planeación del negocio	O	AD/U
Involucrar activamente a la dirección en la planeación de informática	O	I
Elaborar un análisis costo/beneficio por cada proyecto de informática	O	I
Informática debe elaborar un informe de avance a la alta dirección	O	I
Tiene que existir un comité formal de informática, alta dirección y usuarios	O	AD/I/U

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.3. DIRECCIÓN Y NIVELES EJECUTIVOS

Como se explicó en el capítulo II, toda área de informática debe contar con una organización bien establecida, donde los niveles ejecutivos y de dirección sean los encargados de establecer la misión, los objetivos y los planes del área y, por otro lado, participar en los de la organización. La revisión que se haga de esta área, tendrá forzosamente que cuestionar estos temas, verificar la existencia de un comité en informática y requerir la documentación referente a los objetivos y metas, aunado todo esto al seguimiento de su divulgación.

Otra parte importante de la actividad de la dirección de informática es la elaboración y mantenimiento de políticas y procedimientos que cuiden el óptimo funcionamiento de los servicios informáticos para todos los usuarios.

Hasta aquí tenemos sólo una parte de la revisión ya que también se debe abarcar el nivel directivo de la organización, no sólo el de el área de informática. La alta dirección deberá revisarse con el debido cuidado y confidencialidad, se abarcarán aspectos como los ya mencionados: misión, objetivos y metas globales de la empresa u organización.

Objetivos de esta revisión

- Detectar el grado de confianza, satisfacción y respaldo que brinda la función de informática al negocio
- Verificar que las bondades y limitaciones de cada uno de los sistemas de información sean percibidos conceptualmente por la alta dirección y que este entendimiento sea congruente con la realidad
- Confirmar que exista una clasificación y entendimiento de los servicios de informática para la alta dirección
- Comprobar que la tecnología de informática (hardware, software, comunicaciones, etc.) se encuentre al alcance de los niveles directivos de una manera amigable y productiva
- Asegurar que la alta dirección tenga los sistemas de información, los servicios y la tecnología de informática que requiere para la toma de decisiones, el mejoramiento de las actividades de sus funciones, la obtención de un valor agregado por el uso de informática, etc.
- Verificar que exista un análisis costo/beneficio de la función de informática dentro del negocio
- Comprobar que los planes y políticas de informática sean difundidas y conocidos por la alta dirección
- Evaluar el grado de compromiso de la alta dirección con informática para establecer si el apoyo que le brinda es el adecuado o es limitado

Esto se comprueba con la alta dirección, los principales gerentes usuarios y el responsable de la función de informática (director, gerente, jefe o coordinador)

Principales actividades para auditar esta área

1. Comprobar proyectos con la planeación de auditoría.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio.
4. Ratificar y formalizar fechas de entrevistas y visitas.
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.
7. Revisarlo con el encargado de la función de auditoría en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por cada una de las áreas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.

11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de la revisión

1. Formalizar el apoyo por parte de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución satisfactoria de sus actividades. Algunas acciones de apoyo serían:

   - La alta dirección hace del conocimiento de las áreas por auditar que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimiento del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logrará mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática

En el cuadro 3.3 , se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de dirección y niveles ejecutivos

Cuadro 3.3. Políticas y procedimientos de control requeridos por área

DIRECCIÓN Y NIVELES EJECUTIVOS CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Misión, objetivos y planes formales del negocio	O	AD
Difusión y entendimiento de los organigramas y funciones del negocio	O	AD/U
Ubicación de la función informática en un nivel estratégico	R	AD
Involucramiento de la dirección en el proceso de planeación de informática	O	AD/I,U
Políticas y procedimientos de la alta dirección para la función de informática	R	AD/I
Comité formal de informática y alta dirección	R	AD,I
Calendario formal de reuniones del comité y resultados esperados	O	AD/I
Parámetros de medición de la función de informática	O	AD/E
Posición formal de la función de informática en la organización	O	AD/E
Funciones y alcances formales de las áreas de informática	O	I/E
Metas, objetivos y planes formales de informática	O	I/AD
Divulgación y aprobación de los planes de informática por la alta dirección	R	AD/I/U
Evaluación periódica del trabajo hecho por la función de informática	R	AD/U

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.4. USUARIOS DE INFORMÁTICA

Encontramos en ésta una de las areas mas impactantes en la opinión final sobre el área de informática de la organización. Se mide con ella el grado de satisfacción de los clientes de informática, es decir de los usuarios. De voz de los mismos operadores de los sistemas, captunistas y personal en general involucrado en el área, conocemos si se logran o no las metas y objetivos para los que esta destinada el área de servicio informático.

Tomar en cuenta la mayoría de las otras areas en ésta, revisando el nivel en el que se involucra a los usuarios en desarrollo de sistemas, mantenimiento, planeación, evaluación de paquetes y equipo, sistemas en operación y proyectos de actualización y capacitación.

En un caso óptimo el auditor en informatica lograría no sólo conocer que servicios informáticos están perdiendo su calidad, sino que también puede descubrir las areas de oportunidad en las cuales los usuarios podrían aprovechar la informatica para agilizar su trabajo.

Hay que especificar bien los límites del alcance de esta área para no perder el camino de una buena revisión.

Objetivos de esta revisión

- Detectar el grado de confianza, satisfacción y respaldo que perciben los usuarios de parte de la función de informatica
- Detectar el soporte real que brinda la función de informática a los diferentes departamentos usuarios del negocio
- Verificar que las bondades y limitaciones de cada uno de los sistemas de información sean percibidos claramente por los usuarios y que este entendimiento sea congruente con la realidad
- El auditor ha de definir la calidad, oportunidad y confiabilidad real de cada sistema de información, mismas que validarán los responsables de informática y los usuarios
- Estudiar el grado de involucramiento de los usuarios en proyectos específicos como desarrollo de sistemas, evaluación y adquisición de paquetes que serán utilizados por los mismos usuarios, etc.
- Confirmar si existen procedimientos formales para el seguimiento de la comunicación entre los usuarios e informática
- Comprobar si se cuenta con un comité formal integrado por representantes de informática y de los departamentos usuarios
- Detectar areas de oportunidad donde el usuario requiera el apoyo de la función de informática. Dicho apoyo puede ser por ejemplo la automatización de funciones manuales, implantación de una red, mejoras en el ambiente de telecomunicaciones, automatización de procesos, entre otros. La evaluación de la factibilidad de implantar esas areas de oportunidad corresponde a informatica y usuarios; el auditor sólo participará en la verificación del cumplimiento de las políticas relativas a este proceso de evaluación
- Confirmar la presencia de un analisis costo/beneficio de los diferentes productos y servicios que brinda informática a los usuarios
- Constatar que los planes y políticas de informatica sean difundidos y conocidos por las areas usuarias
- Evaluar el grado de compromiso de las areas usuarias hacia el comité de usuarios e informática (si existe)

El personal por entrevistar y visitar en esta revisión será gerentes, jefes y auxiliares de las areas usuarias que serán auditadas.

Principales actividades para auditar esta área

1. Comprobar proyectos con la planeación de auditoría.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio

4. Ratificar y formalizar fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.
7. Revisarlo con el encargado de la función de auditoria en informática
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final

Requerimiento para el éxito de la revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecucion de su trabajo. Algunas acciones de apoyo serian:

   - La alta dirección hace del conocimiento de las areas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoria en informática.

3.5. CONTROL INTERNO

En el capitulo I del presente trabajo se explicó que significa el control interno y su importancia. En esta parte no podemos hablar de controles especificos conjuntados en un área de revisión, hablaremos de todos los controles que deben existir en un área de servicio de informática.

Esta área es clave para la lista de observaciones de auditoria ya que es el conjunto de medidas que se toman para administrar las funciones de todas las areas, además se deben revisar las políticas y procedimientos que garanticen el buen funcionamiento de las demás areas.

Objetivos de esta revisión

- Detectar el grado de estandarización y seguimiento formal que existe en el medio informático.
- Evaluar la existencia de políticas y procedimientos requeridos para el desempeño eficiente de cada una de las funciones de informática:
    - Administración de la función de informática
    - Telecomunicaciones
    - Planeación de informática
    - Soporte a usuarios (capacitación, asesoria en hardware, software, aplicaciones, etc.)
    - Desarrollo e implantación de sistemas de información
    - Mantenimiento de sistemas de información
    - Operación de sistemas de información
    - Investigación de tecnología relacionada con informática
    - Automatización de oficinas
    - Seguridad
    - Auditoria en informática
    - Aseguramiento de calidad
    - Otras especificaciones del negocio
- Verificar y asegurar el cumplimiento oportuno y formal de las políticas y procedimientos relacionados con la función de informática.
- Confirmar la existencia de controles y procedimientos formales para el uso adecuado de los datos y recursos tecnológicos de informática.
- Comprobar y asegurar el cumplimiento oportuno y formal de las políticas y procedimientos relacionados con el manejo de los datos del negocio a través de sistemas de información y de recursos de la función de informática como equipos de cómputo y telecomunicaciones.
- Implantar y dar las recomendaciones necesarias para que se eliminen las debilidades y falta de controles detectados durante esta revisión.
- Asegurar que dichos controles y procedimientos cumplan con los objetivos, propósitos y sugerencias conocidos generalmente a través de institutos y asociaciones profesionales a nivel nacional e internacional.

Esta revisión se aplica a todos los involucrados en la administración y desarrollo de las funciones del área de informática.

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoria.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades especificas del negocio.
4. Ratificar y formalizar fechas de entrevistas y visitas.
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.

7. Revisarlo con el encargado de la función de auditoria en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta direccion al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

    - La alta dirección hace del conocimiento de las areas por auditar que algunas de sus funciones serán revisadas y se requiere su apoyo.
    - Proporcionar la información requenda por el auditor en informática
    - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática.

En el cuadro 3.4 , se mencionan algunas politicas y procedimientos sugeridos que deben existir como mínimo en el área de control interno.

Cuadro 3.4. Políticas y procedimientos de control requeridos por área

CONTROL INTERNO CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Procedimientos formales para el procesamiento de información	O	I/E
Funciones definidas formalmente para el área de informática y los usuarios	O	I/U.E.
Procedimientos formales de supervisión permanente de la ejecución de funciones	O	I/U.E
Procedimientos formales que aseguren la totalidad de la información	O	I/E
Procedimientos formales que aseguren la exactitud de la información	O	I/E
Procedimientos formales que aseguren la autorización de la información	O	I/E
Procedimientos formales que aseguren el mantenimiento de la información	O	I/E
Procedimientos formales que aseguren la actualización de la información	O	I/E
Procedimientos formales para el uso adecuado de hardware, software y aplicaciones	O	I/E
Políticas y procedimientos que regulen el uso de recursos externos a la compañía	O	I/U/AD
Políticas y procedimientos formales para la operación de la información	O	I/E
Procedimientos formales de evaluación y seguimiento de las funciones definidas	O	I/U
Procedimientos formales de evaluación del hardware, software y aplicaciones	O	I/E

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.6. CICLO DE DESARROLLO E IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN

"La participación de auditoria en el desarrollo de sistemas se refiere al control sobre la instalación y modificación de la plataforma informática de la empresa. Por ello, es importante que el auditor este involucrado desde la gestación del plan maestro de sistemas.

Los sistemas de información se deben desarrollar para servir al usuario, proporcionándole capacidades para el proceso de datos y reportes. Cada sistema de información tiene cuatro principales areas o fases sujetas a control durante el proceso del ciclo de vida del desarrollo de sistemas:

- Análisis y diseño
  - Requisición de servicios
  - Estudio de factibilidad
  - Diseño
  - Diseño general del sistema
  - Diseño detallado del sistema
- Desarrollo
  - Programación
  - Prueba modular y prueba del sistema integral
  - Desarrollo de manuales
  - Entrenamiento
- Implantación
  - Conversion
  - Revisión de la post-implantación
- Mantenimiento
  - Correctivo
  - Preventivo

El reconocer que hay un ciclo de vida para el desarrollo de un sistema es el primer paso para su control. El hecho de dividir el desarrollo en fases permite predecir el proyecto integro, analizar y evaluar cada parte con mayor concentración y monitorear continuamente la calidad y avance del trabajo.

La revisión del ciclo de vida del desarrollo de sistemas de información tiene el propósito de asegurar que la organización tenga y esté usando la metodologia adecuada de desarrollo. Adicionalmente el auditor de sistemas de información debe asegurar que el proceso de desarrollo se adhiera a los estándares establecidos por la metodologia.

La meta es verificar que se desarrollen sistemas útiles, seguros, auditables, mantenibles y controlables, lo cual produzca resultados consistentes para satisfacer los requerimientos del usuario.

La conciencia de la calidad, seguridad y control debe iniciarse en las areas de desarrollo, contemplando un balance adecuado con la productividad de los sistemas"[1].

Ademas se tiene que confirmar la estandarizacion que se lleva en los distintos procesos de desarrollo del sistema y la documentación referente a estos. Son muy importantes los controles implantados en cada etapa de crecimiento del sistema, de manera que el auditor pueda conocer en cualquier momento la situación y avance de cada etapa. "Los objetivos de control del proceso de planeación de sistemas son el asegurar que:

- Los proyectos de desarrollo de sistemas de información sean planeados con la suficiente anticipación
- Las necesidades y objetivos sean definidas adecuadamente

[1] Boletín del Instituto Mexicano de Auditores Internos, "Auditoría de Informática", C.P. Sara Isabel Ayala Rodiles. Mayo y Junio de 1994

- Se evalúen adecuadamente y suficientemente las desventajas, los aspectos económicos, técnicos, humanos, políticos y de operación
- Los sistemas sean planteados de acuerdo a estándares

Los objetivos de controlar el proceso del diseño de sistemas son el asegurar que el sistema satisfaga los requerimientos del usuario y los objetivos de control, así como que el diseño esté de acuerdo a los estándares Los objetivos de control del proceso de desarrollo de sistemas son asegurar que:

- Los programas sean construidos de acuerdo con las especificaciones aprobadas por el usuario en la etapa de diseño del sistema
- Los programas sean desarrollados en base a especificaciones detalladas por programas.
- Los sistemas sean verdaderamente probados y documentados
- Los usuarios sean adecuadamente entrenados
- El sistema esté de acuerdo a estándares

La participación del auditor de sistemas de información en el proceso de desarrollo se basa en la siguiente afirmación.

"La detección y corrección de controles inadecuados o incompletos durante la fase de diseño ahorrará tiempo y dinero cuando el sistema esté operando"[2]

Objetivos de esta revision

- Asegurar que exista un proceso metodológico para ejecutar el ciclo de vida de desarrollo e implantación de sistemas de información formal y estandarizado en la organización
- Verificar y asegurar que se utilice una metodología de desarrollo en cada proyecto de implantación de sistemas de información
- Confirmar que el personal de desarrollo de sistemas de información conozca dicha metodología, con el fin de que se asegure la calidad y productividad durante el desarrollo de estos
- Evaluar el nivel de estandarización que contiene dicha metodología con respecto a las comúnmente aceptadas en el mercado
- Exponer las recomendaciones pertinentes para que dicha metodología satisfaga las necesidades de desarrollo e implantación de sistemas de información
- Comprobar que exista un proceso formal de capacitación para el entendimiento y manejo satisfactorio de la metodología por todo el personal responsable de los proyectos de desarrollo e implantación de sistemas de información
- Verificar que exista un curso de orientación básica enfocado al personal involucrado en los proyectos que no pertenecen al área de desarrollo y que, sin embargo, desempeñan una función importante en este tipo de proyectos

Esta evaluación ha de aplicarse al responsable de informatica o a los responsables del desarrollo e implantación de sistemas

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio.
4. Ratificar y formalizar fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.

[2] Boletín del Instituto Mexicano de Auditores Internos, "Auditoría de Informática", C.P. Sara Isabel Ayala Rodiles Mayo y Junio de 1994

7. Revisarlo con el encargado de la función de auditoria en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta direccion al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

   - La alta dirección hace del conocimiento de las areas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoria en informática.

En el cuadro 3.5., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de ciclo de desarrollo e implantación de sistemas de información.

Cuadro 3.5. Políticas y procedimientos de control requeridos por área

CICLO DE DESARROLLO E IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Metodología formal para el desarrollo de sistemas de información	O	I/E
Técnicas formales para el desarrollo de sistemas de información	O	I/E
Herramientas formales para el desarrollo de sistemas de información	O	I/E
Definición formal de las etapas del desarrollo emanadas de la metodología	O	I/E
Tareas y actividades formales emanadas de la metodología	O	I/E
Funciones y responsabilidades formales originados de la metodología	O	I/E
Productos terminados formales de la metodología	O	I/E
Productos de revisión y aceptación de los productos terminados por etapa	O	I/E
Procedimientos formales para la capacitación en el uso de la metodología	R	I
Capacitar formalmente al personal involucrado en el desarrollo de sistemas	R	I
Procedimientos que aseguren la liga entre planeación y desarrollo	O	I/E
Evaluaciones periódicas de las metodologías de desarrollo	R	I/E
Actualización formal y oportuna de la metodología de desarrollo	R	I/E

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.7. SISTEMAS DE INFORMACIÓN

"La auditoría de sistemas de información, que se encuentran en operación, es de suma importancia pues no siempre el auditor participó durante las diferentes fases del desarrollo del mismo y además los controles tienden a convertirse en erráticos al paso del tiempo, por tanto no se cumplen. El objetivo principal de esta área de oportunidad de la auditoria en informática es que la información que producen los sistemas sea confiable, útil y oportuna cuando un sistema se encuentra en operación.

Un sistema de información o aplicación se define como un conjunto de procedimientos manuales y computarizados, interrelacionados y que constituyen un sistema que produce información relacionada con cierto tipo de operaciones o actividades

El auditor de sistemas de información necesita conocer y evaluar el control interno de los sistemas de información computarizados para determinar el alcance, la naturaleza y la oportunidad de sus procedimientos de auditoría.

También, debe conocer las diferentes técnicas de auditoría usando la computadora y elaborar la documentación que debe generarse como evidencia del trabajo realizado"[1]

Objetivos de esta revisión

Planeación y desarrollo

- Verificar que los sistemas de información desarrollados e implantados se deriven del proceso formal de planeación de sistemas
- Asegurar que los sistemas de información por desarrollar cuenten con el involucramiento y aprobación de la alta dirección y las áreas usuarias correspondientes
- Comprobar que existan y se lleven a cabo las funciones, estándares y procedimientos requeridos durante el desarrollo de un sistema de información
- Verificar y asegurar que se utilice una metodología de desarrollo en cada proyecto de implantación de sistemas de información
- Confirmar que el personal de desarrollo de sistemas de información ejecute de manera total la metodología, con el fin de que se asegure calidad y productividad durante el desarrollo de estos
- Evaluar el nivel de estandarización que se utiliza en el desarrollo de sistemas con respecto a la metodología de desarrollo, si no se cuenta con ella, comprobar el apego a los estándares aceptados
- Hacer las recomendaciones pertinentes para que dicho desarrollo satisfaga las necesidades de los requerimientos planteados en la planeación inicial del proyecto
- Verificar que el desarrollo de sistemas de información se elabore en condiciones de alta calidad y productividad

Operación

- Verificar la existencia de políticas y procedimientos formales relativos a la operación de los sistemas de información
- Comprobar que la liberación de los sistemas en operación haya sido aprobada por los usuarios de manera formal
- Obtener el siguiente conocimiento de los sistemas de información en operación:
    - Procedimientos y controles relativos a la operación
    - Datos y procesos (manuales y automatizados respectivamente)
    - Interfaces
    - Tecnología de soporte

[1] Boletín del Instituto Mexicano de Auditores Internos, "Auditoría de Informática", C.P. Sara Isabel Ayala Rodales Mayo y Junio de 1994

- Seguridad
- Asegurar que existan los controles y procedimientos requeridos para:
  - Entendimiento y uso eficiente de los sistemas de información en operación
  - Documentación
  - Capacitación previa a la operación inicial y capacitación a personal de nuevo ingreso que estará involucrado en la operación de los sistemas
  - Satisfacción de los requerimientos de usuarios
  - Procedimientos que aseguren la continuidad de la operación
  - Seguridad en la operación de los sistemas
  - Totalidad, mantenimiento, actualización, autorización, exactitud y registro de datos

Soluciones de mercado

- Asegurar que los sistemas de información que se adquieran de terceros contemplen el proceso metodológico de desarrollo de sistemas en la medida que lo requiera el proyecto
- Estudiar si en este tipo de proyectos se han evaluado diferentes productos y proveedores para asegurar la adquisición de soluciones de vanguardia que se orienten al cumplimiento de los objetivos del negocio y aporten como valor agregado una ventaja competitiva

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría
2. Concertar citas con el personal que se va a entrevistar
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio
4. Ratificar y formalizar fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo
6. Elaborar un borrador con las principales conclusiones y recomendaciones
7. Revisarlo con el encargado de la función de auditoría en informática
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros
9. Revisar el borrador con el responsable del proyecto por parte de las áreas evaluadas
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión
11. Anexar esta información al documento que definirá el informe final

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:
   - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor
2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática

En el cuadro 3.6., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de sistemas de información

Cuadro 3.6. Políticas y procedimientos de control requeridos por área

SISTEMAS DE INFORMACIÓN CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Uso formal del desarrollo de sistemas con una metodología estándar	O	I/E
Uso formal del desarrollo de sistemas con técnicas estándares	O	I/E
Uso formal del desarrollo de sistemas con herramientas estándares	O	I/E
Procedimiento formal para autorizar el desarrollo de cada sistema	O	I/U
Procedimiento que asegure que cada desarrollo tuvo una planeación	R	I
Técnicas de análisis y diseño estructurado	R	I/ E
Técnicas de programación estructurada para la construcción de sistemas	R	I /E
Técnicas y herramientas pa..a la instalacion de sistemas		
Técnicas y herramientas para la prueba de sistemas	R	I/E
Procedimiento formal de aceptacion de usuarios del sistema desarrollado	O	I/U
Procedimiento formal para la revision posterior a la instalación del sistema	R	I/E
Formalizar el uso de manuales técnicos, de operación y del usuario	O	U
Procedimientos de captura, validación, actualización y mantenimiento de datos	R	I/E
Procedimientos de evaluación y compra de sistemas hechos externamente	R	I/E

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.8. MANTENIMIENTO

Un servicio muy importante que debe mantener con calidad y continuidad el área de informática es el de mantenimiento. Se debe revisar la existencia de políticas y procedimientos formales para la ejecución del mantenimiento, tanto correctivo como preventivo.

Es muy importante revisar que exista documentación de estos procesos que se pueden realizar en software y hardware, un programa de mantenimiento bien planeado y una bitácora que contemple que equipo o sistema se revisó, fecha y responsable.

Se debe tener mucho cuidado para el caso de un mantenimiento contratado con externos. Se debe conocer bien quien los contacta y cual es el procedimiento para realizar su labor. Podemos encontrarnos con un gran peligro para la organización si no se verifica el termino de contrato con las personas de mantenimiento. Supongamos que en una compañía el contrato expiró y se presentan a realizar una verificación de algún equipo clientas personas que precisan ser de mantenimiento, por desconocimiento se les permite el acceso y roban infamación confidencial

También importante es la verificación del adecuado mantenimiento a los sistemas, no podemos vivir en un mundo de mantenimiento y "parches". El mantenimiento, al igual que los controles de seguridad no deben rebasar los costos de la compañía de manera que sea más barato adquirir otros equipos o hacer otros sistemas, que estar manteniéndolos "vivos".

Objetivos de esta revisión

- Comprobar la existencia de políticas y procedimientos formales relativos al mantenimiento preventivo y correctivo del hardware, software, sistemas de información y red de telecomunicaciones dentro de la organización
- Ver que el mantenimiento efectuado a los elementos mencionados garantice la continuidad de las operaciones principales del negocio
- Verificar que exista un proceso de planeación formal del mantenimiento para los diferentes elementos señalados
- Asegurar que el mantenimiento sea preventivo, mas que correctivo
- Confirmar que las áreas de informática y usuarias sean informadas con oportunidad de los calendarios de mantenimiento; si se trata de mantenimiento correctivo, proveer a las áreas afectadas de los elementos necesarios que les garantice la continuidad en el manejo de equipo, sistemas y software
- Verificar que existan funciones asignadas de manera formal para las tareas de:
  - Formulacion y difusión del plan de mantenimiento preventivo
  - Difusión del plan de mantenimiento preventivo
  - Medidas que garanticen la continuidad de las operaciones durante este proceso
  - Desarrollo de las actividades de mantenimiento preventivo
  - Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo
- Asegurar que se tengan funciones asignadas formalmente para las tareas de:
  - Formulación y documentación de acciones de mantenimiento correctivo
  - Difusión de las acciones correctivas a las areas afectadas por este proceso
  - Medidas que garanticen la continuidad de las operaciones durante este proceso
  - Desarrollo de las actividades de mantenimiento correctivo
  - Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento correctivo

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoria.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades especificas del negocio.
4. Ratificar y formalizar fechas de entrevistas y visitas.

5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.
7. Revisarlo con el encargado de la función de auditoría en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informatica con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

   - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo.
   - Proporcionar la información requerida por el auditor en informática.
   - Externar comentarios y sugerencias al auditor.

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo, esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática.

En el cuadro 3.7., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de mantenimiento.

Cuadro 3.7. Políticas y procedimientos de control requeridos por área

MANTENIMIENTO CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Registro de todo software, hardware, etc., en el negocio	O	I
Función responsable del control del inventario de informática	O	I
Programas de mantenimiento preventivo para los recursos de informática	O	I
Bitácoras de mantenimiento correctivo para hardware, software, sistemas, etc.	O	I
Políticas y procedimientos relativos al mantenimiento de la red instalada	O	I
Procedimientos que indiquen a los usuarios cómo dar mantenimiento preventivo formal	O	I
Evaluación del costo de un mantenimiento preventivo para su justificación ante los usuarios	R	I
Estadísticas de los costos o pérdidas por falta de mantenimiento preventivo	R	I
Estadísticas que muestren los elementos que requieren mas mantenimiento correctivo	R	I
Deslindar responsables directos para el seguimiento oportuno del mantenimiento	O	I
Aprobación formal del mantenimiento a sistemas de información	O	I
Lograr negociaciones con proveedores para que apoyen en el mantenimiento	R	I
Hacer que los costos de mantenimiento correctivo sean bajos y esporádicos	R	I

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.9. REDES LOCALES Y TELECOMUNICACIONES

La comunicación de datos se refiere a los medios y métodos para transferir datos entre lugares de procesamiento. Las telecomunicaciones no son algo novedoso; los teléfonos han existido durante más de 100 años, pero lo que si es relativamente reciente es la fusión de las tecnologías de computación y comunicaciones.

En esta área de revisión encontramos todo lo referente a las redes de área local, su planeación, diseño, instalación, mantenimiento y actualización. Además su conexión con redes MAN, WAN y GAN, como el caso de internet.

Por otro lado debemos tocar los temas de administración de la red, implementando pruebas sobre cualquier servidor existente en la compañía (servidores de respaldo, de web, de cuentas, de aplicaciones y, sumamente importante, el de bases de datos). Tenemos que revisar su control de cuentas, políticas de creación, permisos de usuarios y seguridad en la transmisión de información.

La comunicación por cualquier medio también esta comprendida en esta área, de manera que tendremos que revisar la comunicación vía módem, microondas, satélite o radiofrecuencia.

Objetivos de esta revisión

Redes locales

- Asegurar que exista una función formal de administración de la red local
- Asegurar la existencia de procedimientos y controles que orienten a la satisfacción de:
  - La administración de las redes locales
  - La instalación de las redes locales
  - La operación y seguridad de las redes locales
  - El mantenimiento de las redes locales
- Detectar el grado de confianza, satisfacción y desempeño que brindan al negocio las redes locales existentes
- Confirmar que existan parámetros de medición del desempeño de las redes
- Evaluar el grado de soporte que se brinda a los usuarios de la red en el uso de sistemas y software al que tienen acceso en la misma
- Determinar si existen los suficientes controles y procedimientos de seguridad para la red de la empresa
- Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes de las redes locales
- Asegurar que sólo se encuentre instalado software legalizado en las redes locales
- Comprobar si se cuenta con algun software que apoye el monitoreo y la auditoría de los diferentes elementos que componen una red local

Telecomunicaciones

- Asegurar que exista una función formal de administración de la red de comunicaciones
- Asegurar la existencia de procedimientos y controles que orientan a la satisfacción de:
  - La administración de la red de telecomunicaciones
  - La instalación de la red de telecomunicaciones
  - La operación y segundad de la red de telecomunicaciones
  - El mantenimiento de la red de telecomunicaciones
- Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio la red de comunicaciones existente
- Verificar que existan parámetros de medición del desempeño de la red de comunicaciones
- Evaluar el grado de soporte que se brinda a los usuarios de la red de comunicaciones en el uso de sistemas y software al que tienen acceso en la misma
- Determinar si existen los suficientes controles y procedimientos de seguridad para la red de comunicaciones de la empresa

- **Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes de la red de comunicaciones**
- **Asegurar que sólo se encuentre instalado software legalizado en la red de comunicaciones**
- **Verificar si se cuenta con algún software que apoye el monitoreo y la auditoría de los diferentes elementos que componen la red de comunicaciones**

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio
4. Ratificar y formalizar fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo
6. Elaborar un borrador con las principales conclusiones y recomendaciones
7. Revisarlo con el encargado de la función de auditoría en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las áreas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

    - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
    - Proporcionar la información requerida por el auditor en informática
    - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática

En el cuadro 3.8, se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de redes locales y telecomunicaciones.

Cuadro 3.8. Políticas y procedimientos de control requeridos por área

REDES LOCALES Y TELECOMUNICACIONES CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Justificación formal de la instalación de una red	O	I
Planeación formal de las etapas de implantación de la red	O	I
Documento que indique como administrar y operar la red	O	I
Existencia de un responsable directo de la administración de la red	O	I
Existencia de elementos que justifiquen el software y sistemas que habrá en la red	O	I
Instalación exclusiva de software original en la red	O	I
Habrá una definición formal de usuarios que tendrán acceso a la red	O	I
Procedimientos que no permitan acceso a la red a personas no autorizadas	O	I
Procedimientos de respaldo de la información manejada en la red	O	I
Procedimiento de respaldo del hardware de la red	O	I
Políticas que limiten el uso de la red por el perfil de usuarios	O	I
Procedimientos de uso de la red	O	I/U
Procedimientos de seguridad al conectarse con otras redes	O	I
Debe haber datos que justifiquen la integración de un equipo a la red	O	I
Se integrarán a la red solo equipos autorizados por el administrador	O	I
Políticas de seguridad para los datos manejados en la red	O	I/E
Políticas que apoyen el mantenimiento y reemplazo de la red	O	I/E

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.10. HARDWARE

Al igual que el área de revisión en software, en este apartado se debe poner dedicación en evaluar los controles para adquisición, instalación, uso y administración del hardware existente en una organización. Se debe revisar la existencia de políticas y procedimientos relacionados a la operación de los equipos, desde las PC's aisladas del centro de procesamiento hasta las computadoras que contienen las aplicaciones de alto riesgo de la empresa.

Se debe contar con una clara documentación sobre el proceso de adquisición del equipo y de su instalación y manejo. Tan simple sería que por no contar con documentación para el uso de un Primary Domain Controler de Windows NT, se perdieran las bases de datos de cuentas para todo un dominio, trayendo a consecuencia la caída del servicio por algunas horas.

Muy importante sería contar con un inventario de toda la plataforma instalada de equipo, desde PC's y Mainframes hasta impresoras.

Objetivos de esta revisión

- Asegurar que exista una función formal de administración del hardware
- Asegurar la presencia de procedimientos y controles para:
  - La administración del hardware
  - La instalación del hardware
  - La operación y seguridad del hardware
  - El mantenimiento del hardware
- Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio el hardware existente
- Comprobar que existan parámetros de medición del desempeño del equipo
- Evaluar el grado de soporte que se brinda a los usuarios del equipo en el uso de sistemas y software al que tienen acceso
- Determinar si existen los suficientes controles y procedimientos de seguridad para el hardware de la empresa
- Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes del hardware
- Asegurar que sólo se encuentre instalado software legalizado
- Verificar si se cuenta con algún software que apoye el monitoreo y auditoría de los diferentes elementos que componen el hardware del negocio
- Evaluar el grado de compatibilidad e integridad entre microcomputadoras, minicomputadoras, mainframes y supercomputadoras de la empresa

Esta revisión se aplica a los administradores del hardware o usuarios responsables del mismo.

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio.
4. Ratificar y formalizar fechas de entrevistas y visitas.
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.
7. Revisarlo con el encargado de la función de auditoría en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las áreas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.

11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

   - La alta dirección hace del conocimiento de las areas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática.

En el cuadro 3.9., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de hardware.

Cuadro 3.9. Políticas y procedimientos de control requeridos por área

HARDWARE CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Plan de evaluación, compra e instalación de hardware	O	I
Análisis costo/beneficio del hardware antes de su compra	O	I/U
Aprobación formal de la adquisición del hardware	O	AD/U
Contrato legal de la compra de hardware	O	I
Inventario formal de todo el hardware	R	I
Un registro del mantenimiento preventivo y correctivo	R	I
Orientación del hardware comprado para integración con otra tecnología	R	I
Políticas y procedimientos de reemplazo de equipo (justificación)	O	I/U
Políticas y procedimientos de seguridad relacionados con el hardware	O	I
Capacitación y actualización del personal en el uso del hardware	O	I/U
Función responsable de la administración del hardware	O	I
Registro de usuarios responsables del hardware	O	I/U
Registro de ubicación del hardware y los cambios del mismo	R	I

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.11. SOFTWARE

Cuando una organización crece en su plataforma informática, de manera que por cualquier lugar encontramos equipos destinados a dar servicios a usuarios con diversas necesidades, el auditor tendrá que abocarse a la revisión del control que se ejerce sobre el software. Se deben revisar aspectos como:

- Administración en el uso de software
- Instalación
- Seguridad que brindan las aplicaciones instaladas para la toma de decisiones
- Actualización que se hace del software existente

Todos estos aspectos son para conocer el grado de satisfacción de los usuarios de informática y cuidar la continuidad en el servicio prestado por el área.

Un aspecto que tiene atención aparte, por su gran importancia, es la legalización de todo software adquirido para uso de la empresa. La piratería no es sólo un tema controversial motivo de platica, cuando las empresas lanzan demandas a otras por robo o fraude en aspectos de desarrollos de paquetes y sistemas comerciales, se convierte en un verdadero gasto para la compañía el mantener esta situación. Aunque en nuestro país la cultura informática de la mayoría esta desviada en su entendimiento y muy atrasada para nuestros días, es necesario luchar por que lo referente al uso ilegal de software se entienda como un daño al derecho de autor de las empresas desarrolladoras. Ligado a esto tenemos el proceso de adquisición de nuevo software, su evaluación, prueba y costo, todo con su respectiva documentación comprobatoria.

La ultima parte a evaluar en esta área es lo referente a la capacitación sobre el software actualizado de la organización, como se planea este proceso y si es satisfactorio para los usuarios.

Objetivos de esta revisión

- Asegurar que exista una función formal de administración del software
- Asegurar la presencia de procedimientos y controles para:
    - La administración del software
    - La instalación del software
    - La operación y seguridad del software
    - El mantenimiento del software
- Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio el software existente
- Investigar si hay políticas que aseguren un proceso formal de:
    - Evaluación y selección del software por comprar
    - Contratos que aseguren la legalización, instalación, capacitación y actualización oportuna del software adquirido por la empresa
    - Seguimiento a las normas de utilización del software legal, no de copias
    - Evaluación permanente del software existente en el mercado
    - Evaluación permanente de nuevos requerimientos de software en el negocio
- Evaluar el grado de soporte que se brinda a los usuarios en el uso del software al que tienen acceso en los equipos de la empresa
- Determinar si existen los suficientes controles y procedimientos de seguridad para el software de la empresa
- Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes del software
- Asegurar que sólo se encuentre instalado software legalizado
- Verificar si se cuenta con algún sistema o paquete computacional que apoye el monitoreo y auditoria de los diferentes elementos que componen el software instalado en los equipos del negocio
- Evaluar el grado de compatibilidad e integridad entre los diferentes tipos de software instalado en las computadoras del negocio

Esta revisión se aplica a los administradores del software y a los usuarios responsables del mismo.

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el inventario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio.
4. Ratificar y formalizar fechas de entrevistas y visitas.
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.
7. Revisarlo con el encargado de la función de auditoría en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las áreas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:
   - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo.
   - Proporcionar la información requerida por el auditor en informática.
   - Externar comentarios y sugerencias al auditor.
2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática.

En el cuadro 3.10., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de software.

Cuadro 3.10. Políticas y procedimientos de control requeridos por área

SOFTWARE CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Plan de evaluación, compra e instalación del software	O	I
Análisis costo/beneficio del software antes de su compra	O	I/U
Aprobación formal de la adquisición del software	O	AD/U
Contrato legal de la compra del software	O	I
Inventario formal de todo el software	R	I
Procedimiento de actualización del software y su registro	R	I
Orientación del software comprado para integración con otra tecnología	R	I
Políticas y procedimientos de reemplazo de software (justificación)	O	I/U
Políticas y procedimientos de seguridad relacionados con el software	O	I
Capacitación y actualización del personal en el uso del software	O	I/U
Políticas que verifiquen la originalidad del software instalado	O	I
Función responsable de la administración del software	O	I/U
Clasificación del software y su uso en el negocio	R	I

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.12. SEGURIDAD

En este trabajo de investigación dedicamos un apartado completo en el capítulo I, a la seguridad en informática. Ahora podemos agregar que esta área susceptible de revisión es una de las más importantes en el desarrollo de la función de informática, sin un cuidado contundente de ella se puede interrumpir el servicio a los usuarios, desde unas horas hasta por algunos meses, aspecto que imputaría demasiado en costos a la empresa y costos de recuperación al estado original de la información.

El auditor debe revisar aspectos relacionados a respaldos de información, sistemas y aplicaciones de alto riesgo. Además, planes de contingencia en caso de pérdidas materiales de equipos y sistemas de información, su difusión y simulacro.

Esta área abarca también la existencia y aprobación de un plan de seguridad total para los recursos informáticos, la evaluación periódica del nivel de seguridad con que se cuenta y las respectivas políticas y procedimientos para asegurar la efectividad de las medidas de seguridad implantadas.

Por último, al evaluar esta área, el auditor no debe perder de vista que los costos por implantar y mantener un óptimo nivel de seguridad en informática, no serán superiores al de los recursos protegidos.

Objetivos de esta revisión

- Verificar que existan los planes, políticas y procedimientos relativos a la seguridad dentro de la organización.
- Confirmar que exista un análisis costo/beneficio de los controles y procedimientos de seguridad antes de ser implantados.
- Comprobar que los planes y políticas de seguridad y de recuperación sean difundidos y conocidos por la alta dirección.
- Evaluar el grado de compromiso por parte de la alta dirección, los departamentos usuarios y el personal de informática con el cumplimiento satisfactorio de los planes, políticas y procedimientos relativos a la seguridad.
- Asegurar la disponibilidad y continuidad del equipo de cómputo el tiempo que requieran los usuarios para el procesamiento oportuno de sus aplicaciones.
- Asegurar que las políticas y procedimientos brinden confidencialidad a la información manejada en el medio de desarrollo, implantación, operación y mantenimiento.
- Verificar que exista la seguridad requerida para el aseguramiento de la integridad de la información procesada en cuanto a totalidad y exactitud.
- Constatar que se brinde la seguridad necesaria a los diferentes equipos de cómputo que existen en la organización.
- Comprobar que existan los contratos de seguro necesarios para el hardware y software de la empresa.
- Confirmar la presencia de una función responsable de la administración de la seguridad en:
    - Recursos humanos, materiales y financieros relacionados con la tecnología de informática.
    - Recursos tecnológicos de informática.

Esto debe verificarse con los responsables de la seguridad de informática del centro de cómputo, de comunicaciones y usuarios que el auditor considere pertinentes.

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría.
2. Concertar citas con el personal que se va a entrevistar.
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades específicas del negocio.

4. Ratificar y formalizar fechas de entrevistas y visitas.
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones.
7. Revisarlo con el encargado de la función de auditoría en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las áreas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

   - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática

En el cuadro 3.11., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de seguridad.

Cuadro 3.11. Políticas y procedimientos de control requeridos por área

SEGURIDAD CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Plan de seguridad total relativo a informática	O	I
El plan ha de ser aprobado por la alta dirección, usuarios e informática	O	I/AD/U
Debe contemplar un plan de contingencias y un plan de reinicio de operaciones	O	I
El plan de contingencias será difundido formalmente	O	I/U
Los aspectos de seguridad se deben orientar a todos los recursos	O	I
Políticas de la alta dirección que impulsen la seguridad	O	AD
Debe involucrar a todo el negocio en la implantación de la seguridad	O	I/AD/U
Se ha de proteger la seguridad de datos, equipo, tecnología y usuarios	O	I
Las políticas y procedimientos se actualizan de manera oportuna	O	I
Concientización permanente de la necesidad de aplicar la seguridad	R	I/AD/U
Evaluación periódica del nivel de cumplimiento de seguridad	O	I/E
El costo de la seguridad no será superior al de los recursos protegidos	R	I
Apoyarse en estándares de seguridad nacionales e internacionales	R	I/E

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.13. PLANEACIÓN DE INFORMÁTICA

Esta área está dedicada al desarrollo formal de planes, procedimientos y estrategias para el desarrollo de la infraestructura informática de la organización. Se evalúa en ella la adopción de métodos, técnicas y herramientas de planeación y el procedimiento que se sigue en la formulación y aceptación de proyectos, así como su respectiva documentación.

Un apartado de esta revisión esta dedicado al comité de usuarios de informática, en caso de que exista, y si no a su propuesta. El buen funcionamiento de esta planeación impacta en demasía en el logro de los objetivos planteados para el área de informática, como cualquier dirección o gerencia en una empresa. Sin una buena planeación no se puede llegar a la satisfacción de los objetivos del negocio.

Objetivos de la revisión

- Detectar la existencia, formalización y conocimiento de la planeación de informática en las areas claves del negocio
- Verificar que la planeación de informática haya sido evaluada y aprobada por la alta dirección
- Comprobar que la planeación de informatica se enfoque al soporte de los objetivos, planes, políticas y estrategias de la empresa
- Evaluar el grado de compromiso por parte de la alta dirección con informatica para determinar si el apoyo que brinda a la planeación de informática es el adecuado
- Confirmar la existencia de una metodologia en informática
- Investigar si existen tecnicas y herramientas de productividad para el desarrollo del plan general de informática
- Comprobar que exista un proceso formal de capacitación para el entendimiento y manejo satisfactorio de la metodologia de planeación en informatica
- Evaluar el grado de cumplimiento de la metodologia, tecnicas y herramientas en el proceso de planeación de informática
- Comprobar si la alta dirección, los responsables de las areas usuarias y los responsables de informática, se han involucrado en el proceso de planeación de informática
- Verificar si se da cumplimiento a los proyectos surgidos del plan de informática
- Evaluar el grado de dominio que tiene el personal de informática sobre la metodología, técnicas y herramientas de productividad que utilizan para el desarrollo del plan de informatica
- Valorar el nivel de estandarización que tiene la metodologia de planeación de informática con respecto a las aceptadas comunmente en el mercado

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoria
2. Concertar citas con el personal que se va a entrevistar
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades especificas del negocio
4. Ratificar y formalizar fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este módulo.
6. Elaborar un borrador con las principales conclusiones y recomendaciones
7. Revisarlo con el encargado de la función de auditoria en informática.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión.
11. Anexar esta información al documento que definirá el informe final.

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:

   - La alta dirección hace del conocimiento de las áreas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
   - Proporcionar la información requerida por el auditor en informática
   - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática.

En el cuadro 3.12., se mencionan algunas políticas y procedimientos sugeridos que deben existir como mínimo en el área de planeación de informática

Cuadro 3.12. Políticas y procedimientos de control requeridos por área

PLANEACIÓN DE INFORMÁTICA CONCEPTO	RECOMENDADA (R) OBLIGATORIA (O)	FUNCIÓN RESPONSABLE DEL SEGUIMIENTO
Comité formal de usuarios e informática	R	I/U
Proceso formal de planeación del negocio	O	U/E
Metodología formal de planeación de informática	O	I/E
Proceso formal de desarrollo de la planeación de informática	O	I/U/E
Análisis costo/beneficio de cada proyecto emanado de la planeación	O	I/E
Aceptación formal de cada proyecto por área involucrada	O	U
Técnicas y herramientas formales para el proceso de planeación	O	I/E
Documentación formal del plan de informática	O	I/E
Difusión formal del plan de informática dentro del negocio	R	I
Administración y control formal de los proyectos del plan de informática	O	I
Procedimientos que aseguren la actualización de los proyectos	R	I
Involucramiento formal y permanente del comité en los procesos de planeación	O	I/U

I = Informática
U = Usuario
AD = Alta Dirección
E = Externo (Auditoría Externa, Compañías de Servicios, etc.)

3.14. INVESTIGACIÓN TECNOLÓGICA

Esta área se basa principalmente en la adopcion de proyectos que permitan dar actualización al área de informática en hardware, software, redes, telecomunicaciones y seguridad. Se debe revisar el seguimiento que se da a los proyectos, su aprobación, justificación y documentación. Se darán muchos casos en los que no exista un área dedicada a esto en la organización y por tanto el auditor tendrá que proponer si se debe o no adoptar esta actividad

Por último se revisará que tanto impacto a tenido la investigación tecnológica para la organización y el logro de sus objetivos.

Objetivos de la revisión:

- Verificar si existe una función formal de investigacion tecnológica dentro del area de informática
- Detectar el grado de confianza, satisfacción y respaldo que brinda al negocio la función de investigación tecnológica
- Verificar que exista una clasificación y entendimiento de los servicios y productos que proporciona al negocio la función de investigación tecnológica
- Determinar las acciones emprendidas por la función de investigación tecnológica para que la tecnología de informática se encuentre al alcance de las diferentes areas de la empresa que así lo requieran
- Comprobar que exista un análisis costo/beneficio de los proyectos propuestos por la función de investigación tecnológica que justifiquen su aprobación antes de ser implantados
- Constatar que los proyectos de investigacion tecnológica sean resultado del pan de informática
- Evaluar el grado de compromiso de la alta dirección con los proyectos de investigación que informatica considera estratégicos para el negocio

Principales actividades para auditar esta area

1. Comparar proyectos con la planeacion de auditoria
2. Concertar citas con el personal que se va a entrevistar
3. Revisar el formulario correspondiente y ver la conveniencia de actualizarlo según necesidades especificas del negocio
4. Ratificar y formalizar fechas de entrevistas y visitas
5. Efectuar las entrevistas y visitas necesarias para cubrir los puntos de este modulo
6. Elaborar un borrador con las principales conclusiones y recomendaciones
7. Revisarlo con el encargado de la función de auditoria en informatica.
8. Clasificar y almacenar la información de soporte en dispositivos de almacenamiento seguros.
9. Revisar el borrador con el responsable del proyecto por parte de las areas evaluadas.
10. Elaborar y documentar formalmente las conclusiones y recomendaciones finales de esta revisión
11. Anexar esta información al documento que definirá el informe final

Requerimientos para el éxito de esta revisión

1. Formalizar el apoyo de la alta dirección al auditor en informatica con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serian:

    - La alta dirección hace del conocimiento de las areas por auditar, que algunas de sus funciones serán revisadas y se requiere su apoyo
    - Proporcionar la información requerida por el auditor en informatica
    - Externar comentarios y sugerencias al auditor

2. Conocimientos del auditor acerca de los aspectos que se evaluarán en este módulo; esto básicamente se logra mediante una capacitación teórico-práctica en los temas que se relacionan con la auditoría en informática.

CAPÍTULO 4

Metodología para el desarrollo de la Auditoría en Informática

4.1 ANTECEDENTES

Al igual que otras funciones de las empresas, la auditoría en informática se debe efectuar mediante un proceso metodológico, ya que no se debe fomentar la dependencia de la auditoría en informática sólo en la experiencia, habilidad, criterios y conocimientos del auditor.

El desarrollo de las actividades de la función de auditoría en informática debe estar basado en un método de trabajo formal, que sea entendido por todos los auditores en informática y complementado con técnicas y herramientas propias de la función.

Cabe señalar que el uso de la metodología no garantiza por si sola el éxito de los proyectos de auditoría en informática, además se requiere un amplio dominio y uso constante de los siguientes aspectos:

- Técnicas
- Herramientas de productividad
- Habilidades personales
- Conocimientos técnicos y administrativos
- Experiencia en los campos de auditoría e informática
- Conocimiento de los factores del negocio y del medio externo al mismo
- Actualización permanente
- Involucramiento y comunicación constante con asociaciones nacionales e internacionales relacionadas con el campo
- Otras[1]

Además, el no cumplir con las siguientes condiciones, puede llevar a la función de auditoría en informática a que sus proyectos no cumplan con los tiempos, costos o resultados esperados:

- Aprobación de la metodología por la alta dirección
- Adecuación de la metodología a los requerimientos específicos de la organización
- Documentación o actualización de la metodología
- Capacitación formal en el uso de la metodología (de acuerdo con el perfil y nivel de participación de cada individuo por capacitar)
- Elaboración de los planes de auditoría en informática según la metodología
- Verificación del uso formal de la metodología en cada proyecto
- Capacitación formal para el personal de nuevo ingreso o cuando se hagan actualizaciones relevantes a la metodología
- Otros observados por las mismas empresas en sus proyectos[2]

Debido a la dificultad para encontrar información acerca de la metodología de auditoría en informática y para poder proponer nuestra propia metodología, tomamos como referencias la metodología utilizada para realizar un trabajo de investigación documental expuesta por la Dra. Guillermina Baena Paz, la metodología de investigación en organización y métodos de la Secretaría de la Presidencia, la metodología general del desarrollo e implantación de un sistema de procesamiento de datos y la información sobre la auditoría en informática expuesta en las obras del L.I. Enrique Hernandez Hernández y el M.A. José Antonio Echenique García, además de nuestros conocimientos adquiridos como auditores en informática en Auditoría Interna de la UNAM.

En el cuadro 4.1, se muestran de manera general, las metodologías propuestas por cada autor y la utilizada en Auditoría Interna de la UNAM. Como se puede observar en el cuadro 4.1, tanto la propuesta del M.A. José Antonio Echenique García y la metodología utilizada en Auditoría Interna de la UNAM, presentan como etapas, a las áreas susceptibles de revisión; como por ejemplo: evaluación de la función de informática, evaluación de los sistemas en operación, evaluación del desarrollo de sistemas, evaluación de la seguridad, revisión de controles generales, etc. Desde nuestro punto de vista, el concepto de las etapas de una metodología (en este caso

[1] Hernández Hernández, Enrique. Auditoría en Informática, un enfoque metodológico. pag. 73
[2] Hernández Hernández, Enrique. Auditoría en Informática, un enfoque metodológico. pág. 74

Metodología de auditoría en informática L.I. Enrique Hdez. Hdez.		Metodología de auditoría en informática M.A. José Antonio Echenique García		Metodología de auditoría en informática Auditoría interna de la UNAM	
Etapa	**Especificaciones**	**Etapa**	**Especificaciones**	**Etapa**	**Especificaciones**
Preliminar	Diagnóstico del negocio Diagnóstico de informática	Planeación	Investigación preliminar Personal participante	Revisión de controles generales	Adquisición de bienes informáticos Sistema operativo Seguridad física
Justificación	Matriz de Riesgos Plan de auditoría en informática	Auditoría de la función de informática	Información organizacional Evaluación estructura orgánica Evaluación recursos humanos Entrevistas al personal de informática Situación presupuestal y financiera		Seguridad lógica Plan de contingencias
Adecuación	Plan y metodología de acuerdo con el cliente Plan detallado			Revisión de la administración de la función de informática	Previsión Planeación Organización Integración Dirección Control
Formalización	Plan aprobado Compromiso ejecutivo	Evaluación de los sistemas	Evaluación de sistemas Evaluación del análisis Evaluación del diseño lógico Evaluación del desarrollo Control de proyectos Control de diseño de sistemas Instructivos de operación Forma de implantación Equipo y facilidades de programación Entrevistas a usuarios	Microcomputadoras Independientes	
Desarrollo	Auditar áreas seleccionadas Informe de auditoría en informática			Desarrollo de sistemas	Planeación Análisis y diseño Desarrollo Implantación
Implantación	Recomendaciones y acciones terminadas Aprobación final			Sistemas de Información en operación	Antecedentes Conocimiento de los procedimientos manuales Conocimiento de los procedimientos computarizados Evaluación del ambiente de control Registro de debilidades de control Programas de pruebas de cumplimiento Pruebas de auditoría Informe de auditoría
		Evaluación del proceso de datos y de los equipos de computo	Controles Orden en el centro de cómputo Evaluación de la configuración del sistema de cómputo Productividad		
		Evaluación de la seguridad	Seguridad lógica y confidencialidad Seguridad en el personal Seguridad física Seguros Seguridad en el uso del equipo Procedimientos en caso de desastre Soporte a otras instituciones		

(Continúa)

Cuadro 4.1. Metodologías tomadas como referencia para la elaboración de una propuesta para la elaboración de una metodologíade auditoría en informática

Metodología investigación documental Dra. Guillermina Baena Paz	Metodología investigación documental Secretaría de la Presidencia	Metodología general de la implantación de un sistema de procesamiento de datos
Plan de trabajo	Planificación del estudio	Planeación
Recopilación del material	Recopilación de datos	Análisis
Análisis y ordenación de las datos	Análisis de los datos	Diseño
Exposición de los datos	Formulación de recomendaciones	Desarrollo
	Implantación	Implantación
	Evaluación	

Cuadro 4.1. Metodologías tomadas como referencia para la elaboración de una propuesta para la elaboración de una metodología de auditoría en informática

de la metodología de auditoría en informática) es más general y corresponden a períodos o fases generales donde se realizan cierto tipo de actividades que pueden o no, hacer referencia a una o varias de las áreas susceptibles de revisión expuestas en el capítulo 3.

En nuestra metodología proponemos etapas que se asemejan "teóricamente" a las etapas de una metodología de investigación documental, de una metodología de investigación en organización y métodos o de una metodología general para el desarrollo e implantación de un sistema de procesamiento de datos. De esta manera, tomamos los elementos más importantes de las propuestas de cada uno de los autores mencionados anteriormente y, junto con nuestras aportaciones, proponemos una metodología aun mas completa, a la cual le añadimos y quitamos los aspectos que así consideramos pertinentes.

En el cuadro 4.2, se muestra de manera practica la propuesta que hacemos sobre la metodología de auditoría en informatica y, en seguida, se explican cada una de las etapas por las que está compuesta nuestra metodología, describiendo cada una de las actividades del auditor en informática y los documentos que se vayan generando durante el proyecto.

ETAPA	TAREAS	PRODUCTOS	RESPONSABLE	INVOLUCRADOS
Preliminar	1 Solicitud	1 1 Solicitud de elaboración de la auditoría en informática	AD	AD
	2 Elaborar un contrato	3 1 Contrato de auditoría en informática	RAI	AD
Diagnóstico	1 Hacer un diagnóstico de la empresa o institución	1 1 Misión, objetivos y organización de la institución	CAI/RAI	AD
		1 2 Grado de apoyo a la institución	CAI/RAI	AD/PU
	2 Hacer un diagnóstico del área de informática	2 1 Organización y objetivos del área de informática	CAI/RAI	RI
		2 2 Control	CAI/RAI	RI/PI
		2 3 Productos y servicios	CAI/RAI	RI
	3 Detectar posibles áreas de oportunidad	3 1 Áreas de oportunidad para mejoras inmediatas	CAI/RAI	AD/PU/RI
Planeación	1 Hacer la matriz de riesgos	1 1 Matriz de riesgos	CAI/AI	RAI
	2 Hacer un plan general de auditoría en informática	2 1 Plan general de auditoría en informática	CAI	RAI/AI
	3 Aprobación del plan	3 1 Plan aprobado	CAI	RAI/AD/RI/PU
	4 Definir objetivos del proyecto	4 1 Objetivos y alcances del proyecto	CAI	RAI
	5 Actualizar el plan general	5 1 Plan actualizado	AI/RAI	RAI
	6 Hacer un plan detallado de auditoría en informática	6 1 Etapas y tareas	AI/RAI	RAI
		6 2 Responsables e involucrados	AI	CAI
		6 3 Productos terminados	AI	CAI
		6 4 Revisiones (formales e informales)	AI	CAI
	7 Definir los elementos por auditar por cada área de revisión	7 1 Aspectos o elementos a evaluar por cada área de revisión	AI	CAI
	8 Establecer técnicas y herramientas por cada área de revisión	8 1 Técnicas	AI	CAI
		8 2 Software	AI	CAI
		8 3 Equipo de cómputo	AI	CAI
		8 4 Otros	AI	CAI
	9 Definición o actualización de políticas por área de revisión	9 1 Políticas o procedimientos por verificar de acuerdo con cada área que será auditada	AI	CAI
		9 2 Políticas complementarias	AI	CAI
	10 Elaboración o actualización de cuestionarios por área de revisión	10 1 Cuestionarios por cada área que será auditada	AI	CAI
		10 2 Cuestionarios adicionales	AI	CAI
Formalización	1 Verificar prioridades y cursos de acción	1 1 Prioridades clasificadas	CAI	RAI
		1 2 Áreas por auditar verificadas	AI/CAI	RAI
	2 Verificar plan y actividades	2 1 Etapas y tareas	AI	CAI
	3 Presentar formalmente el proyecto	3 1 Propuesta de servicios	RAI	AD
		3 2 Plan detallado final	AI	CAI
		3 3 Proyecto revisado de la auditoría en informática	RAI	AD/PU/RI

(Continúa)

Nomenclatura: AD = alta dirección, PU = personal usuario, RI = responsable del área de informática, PI = personal de informática, RAI = responsable del área de auditoría en informática, CAI = coordinador de auditoría en informática, AI = auditor en informática

Cuadro 4.2. Enfoque práctico del proceso metodológico de la Auditoría en Informática

ETAPA	TAREAS	PRODUCTOS	RESPONSABLE	INVOLUCRADOS
Formalización	4 Aprobación formal del proyecto de auditoría en informática	4 1 Aprobación del proyecto	AD/PU RI	RAI/CAI
		4 2 Compromiso ejecutivo	AD	RAI/RI/PU
		4 3 Addendum del contrato de auditoría en informática	AD	RAI
		4 4 Inicio formal del proyecto	CAI	AD/PU/PI
	5 Compromiso de las áreas involucradas	5 1 Entendimiento del proyecto	RI	CAI/AI
		5 2 Aceptación del proyecto	PI/PU	CAI/AI
		5 3 Compromiso de cada una de las áreas involucradas	PI/PU	CAI AI
	6 Definir las áreas por visitar	6 1 Fechas de entrevistas	CAI	PI/PU
		6 2 Fechas de visitas	CAI	PI/PU
		6 3 Fechas para aplicación de cuestionarios	CAI	PI/PU
Desarrollo	1 Concertar citas	1 1 Fechas aprobadas o actualizadas	AI	PI/PU
	2. Verificar tareas, involucrados, etc	2 1 Tareas, involucrados, etc. revisados	AI	PI/PU
	3 Clasificar técnicas, cuestionarios y herramientas por usar	3 1 Técnicas, cuestionarios y herramientas clasificadas	AI	CAI
	4 Efectuar entrevistas	4 1 Entrevistas realizadas	AI	PI/PU
		4 2 Entrevistas documentadas	AI	AI
		4 3 Análisis de entrevistas	CAI/AI	RAI
	5 Aplicar cuestionarios	5 1 Cuestionarios aplicados	AI	PI/PU
		5 2 Cuestionarios documentados	AI	AI
		5 3 Análisis de cuestionarios	CAI/AI	RAI
	6 Efectuar visitas de verificación	6 1 Visitas realizadas	AI	RI/PI/PU
		6 2 Comentarios documentados	AI	AI
		6 3 Análisis de documentos	CAI/AI	RAI
	7 Elaborar informe preliminar acerca de las áreas auditadas	7 1 Observaciones (acerca de debilidades o carencia de controles)	AI	CAI
		7 2 Áreas de oportunidad	AI	CAI
		7 3 Alternativas por cada área de oportunidad detectada	AI	CAI
		7 4 Recomendaciones (acciones específicas) por alternativa	AI	CAI
		7 5 Responsables de ejecutar cada acción	AI	CAI
		7 6 Plazos de ejecución por acción	AI	CAI
		7 7 Áreas auditadas clasificadas	AI	CAI
		7 8 Informe documentado, almacenado y clasificado	AI	AI
	8 Revisar el informe preliminar por área	8 1 Borrador de auditoría en informática revisado	CAI	RAI/AI
	9 Autorizar el borrador del informe preliminar	9 1 Informe preliminar revisado	CAI	PI/PU/AI
		9 2 Informe preliminar corregido	AI	CAI

(Continúa)

Nomenclatura: AD = alta dirección, PU = personal usuario, RI = responsable del área de informática, PI = personal de informática, RAI = responsable del área de auditoría en informática, CAI = coordinador de auditoría en informática, AI = auditor en informática

Cuadro 4.2. Enfoque práctico del proceso metodológico de la Auditoría en informática

ETAPA	TAREAS	PRODUCTOS	RESPONSABLE	INVOLUCRADOS
Desarrollo		9 3 Informe preliminar entregado	CAI	CAI
		9 4 Informe preliminar autorizado	AD/RI/PU	AD/RI/PU
	10 Efectuar entrevistas, cuestionarios y visitas complementarias	10 1 Entrevistas, cuestionarios y visitas pendientes realizados	CAI/AI	PI/PU
		10 2 Informe actualizado con observaciones, acciones, etc	AI	CAI
	11 Elaborar informe final	11 1 Informe final revisado con información de todas las áreas auditadas	AI	CAI
		11 2 Informe con visto bueno del responsable de la función de auditoría en informática	RAI	CAI/AI
		11 3 Informe final almacenado en medios magnéticos (respaldo)	AI	AI
		11 4 Documentación del informe para la alta dirección	CAI/AI	RAI
		11 5 Documentación del informe para responsables de los usuarios y del personal del área de informática	AI	CAI
	12 Elaborar un plan de implantación general de acciones sugeridas	12 1 Acciones clasificadas por plazos sugeridos	CAI/AI	RAI
		12 2 Costo/beneficio del plan	CAI/AI	RAI
	13 Aprobar informe y plan de implantación	13 1 Informe de auditoría en informática y plan aprobados	AD/RI/PU	RAI/CAI
	14 Presentación del informe de auditoría en informática y del plan de implantación	14 1 Informe final y plan presentados a la dirección	RAI	AD/RI/CAI
		14 2 Informe final y plan presentados a personal usuario y de informática	CAI/AI	PI/PU
	15 Aprobar informe final	15 1 Revisión del informe de auditoría en informática	AD/RI/PU	RAI/CAI/PI
		15 2 Aprobación del informe de auditoría en informática	AD/RI	RAI/CAI/PU
		15 3 Compromiso ejecutivo	AD/RI	RAI/PU
Implantación y Seguimiento	1 Definir requerimientos para el éxito del plan de implantación	1 1 Recursos requeridos para el éxito de la implantación sugerida por auditoría en informática	RI/PU	CAI
		1 2 Recursos aprobados	AD	RI/PU/CAI
		1 3 Equipo de trabajo para la implantación	RI/PU	CAI
		1 4 Equipo de trabajo aprobado	AD	RI/PU/CAI
		1 5 Funciones y responsabilidades	RI/PU	CAI
		1 6 Fechas de revisión	RI/PU	CAI
		1 7 Productos terminados	RI/PU	CAI
		1 9 Costo/beneficio revisado	RI/PU	CAI
		1 9 Costo/beneficio aprobado	AD	RI/PU/CAI
		1 10 Inicio de la implantación	RI/PU	CAI
	2 Desarrollar el plan de implantación delineado	2 1 Plan de implantación revisado según los resultados de la primera tarea	RI/PU	CAI/AI

Nomenclatura: AD = alta dirección, PU = personal usuario, RI = responsable del área de informática, PI = personal de informática, RAI = responsable del área de auditoría en informática, CAI = coordinador de auditoría en informática, AI = auditor en informática

(Continúa)

Cuadro 4.2. Enfoque práctico del proceso metodológico de la Auditoría en Informática

ETAPA	TAREAS	PRODUCTOS	RESPONSABLE	INVOLUCRADOS
Implantación y Seguimiento		2.2 Plan de implantación corregido y actualizado	PI	AI/PU
		2.3 Documentar plan final	RI	AI/PU
		2.4 Plan final aprobado	AD	PI/PU/CAI
	3. Efectuar implantación sugerida por auditoría en informática	3.1 Inicio del proyecto	PI/PU	RI
		3.2 Tareas terminadas	PI/PU	RI
		3.3 Pendientes justificados	PI/PU	AD/RI
		3.4 Pendientes implantados	PI/PU	RI
		3.5 Presentación de implantación	RI	AD/RAI/CAI
		3.6 Implementacion aprobada	AD/PI/PU	RI/RAI/CAI
	4. Seguimiento a la implantación del plan recomendado por la auditoría	4.1 Acciones de seguimiento	CAI	RAI/AI
		4.2 Seguimiento de la implantación	CAI	AI
		4.3 Revisiones informales	CAI	AI
		4.4 Revisiones formales	CAI	RAI
		4.5 Aseguramiento de calidad	CAI	RAI
		4.6 Pendientes revisados	CAI	RAI
		4.7 Pendientes aprobados	CAI	RAI
		4.8 Seguimiento de pendientes	CAI	RAI
		4.9 Implantación exitosa final	CAI	RAI
		4.10 Implantación aprobada	RAI	RAI

Nomenclatura: AD = alta dirección, PU = personal usuario, RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática, CAI = coordinador de auditoría en informática, AI = auditor en informática

(Continúa)

Cuadro 4.2. Enfoque práctico del proceso metodológico de la Auditoría en Informática

4.2. ETAPA PRELIMINAR

Como se mencionó en la introducción, nuestra propuesta pretende servir de guía tanto para auditores en informática internos como para auditores en informática externos. De ésta manera, las fases de esta primera etapa dependen del tipo de auditoría en informática que se realice, ya sea interna o externa, ya que la solicitud y el contrato de auditoría en informática dependen en gran medida de ésta circunstancia.

Solicitud

Dependiendo del tipo de auditoría que se realice, la solicitud puede ser de dos formas; para la auditoría en informática interna, la solicitud debe ser por escrito de parte del jefe del área de informática al jefe del área de auditoría interna. Un ejemplo del contenido general de los aspectos que debe contener dicha solicitud lo podemos ver en la figura 4.1., para la auditoría en informática externa, la solicitud puede ser por escrito, por vía telefónica o por medio de una entrevista.
Nota: Cabe destacar que hacemos referencia a los jefes de las áreas de informática y de auditoría interna con esa denominación, sin embargo, dichos títulos pueden variar de acuerdo al organismo que se esté auditando.

Contrato

El contrato de auditoría en informática se divide en dos partes. La primera parte consta de las etapas de diagnóstico, planeación y formalización. La segunda parte, está contemplada en un addendum que puede o no llegar a formar parte del contrato y contiene las etapas de desarrollo, implantación y seguimiento. Lo anterior se debe a que en ocasiones, el cliente no esta conforme con lo que se está desarrollando y da por terminado el contrato, dando como resultado grandes pérdidas de tiempo y dinero y muy probablemente una difusión de información sin fundamentos, que desprestigia a nuestra compañía de auditoría en informática. De ésta manera, con la primera parte se realiza un diagnóstico de la empresa u organismo, se detectan las áreas de mayor riesgo, se elabora un plan de acción detallado y se presenta una propuesta de servicios. Si ésta es aceptada por el cliente, se continúa con la segunda parte, en caso contrario, se da por terminado el contrato sin tener problemas por los honorarios o por la presentación de resultados, ya que así quedó formalmente establecido.

En la figura 4.2., se muestra un formato donde se pueden observar los elementos que debe contener el contrato de auditoría en informática y la parte complementaria, se presenta en la etapa de formalización.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO

C.P. MARCELA FERNÁNDEZ IZAGUIRRE
AUDITOR INTERNO DE LA UNAM

P R E S E N T E

Por medio de la presente, comunico a usted que debido a los requerimientos del area y para proporcionar el servicio a los usuarios, es indispensable realizar una auditoria en informatica en la dependencia a mi cargo

Sin mas por el momento y en espera de su respuesta le envio un cordial saludo

A T E N T A M E N T E
"Por mi raza hablara el espíritu"
Ciudad Universitaria, 3 de mayo de 1997.

L.I. CECILIA CALDERÓN ORTEGA
DIRECTOR GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO

Figura 4.1. Ejemplo de solicitud de auditoria en informática dentro del mismo organismo.

CONTRATO DE AUDITORÍA EN INFORMÁTICA

Contrato de prestación de servicios profesionales de auditoría en informática que celebran por una parte _____ representado por _____ en su carácter de _____, y que en lo sucesivo se denominará el cliente, por otra parte _____ representada por _____, a quien se denominará el auditor, de conformidad con las declaraciones y cláusulas siguientes

D E C L A R A C I O N E S

I El cliente declara

a) Que es una _____
b) Que está representada para este acto por _____ y que tiene como su domicilio _____

c) Que requiere obtener servicios de auditoría en informática, por lo que ha decidido contratar los servicios del auditor.

II Declara el auditor

a) Que es una sociedad anónima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales está el de prestar auditoría en informática _____

b) Que está constituida legalmente según escritura número _____ de fecha _____ ante el notario público número _____ del _____ Lic. _____
c) Que señala como su domicilio _____

III Declaran ambas partes

a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que se contiene en las siguientes

C L Á U S U L A S

PRIMERA. OBJETO

El auditor se obliga a prestar al cliente los servicios de auditoría en informática para llevar a cabo las etapas de diagnóstico, planeación y formalización en el área de informática del cliente

SEGUNDA. ALCANCE DEL TRABAJO

El alcance de los trabajos que llevará a cabo el auditor dentro de este contrato son
a) Etapa de Diagnóstico
1 Hacer un diagnóstico de la empresa o institución
1.1 Misión, objetivos y organización de la institución
1.2 Grado de apoyo a la institución
2 Hacer un diagnóstico del área de informática
2.1 Organización y objetivos del área de informática
2.2 Control
2.3 Productos y servicios
3 Detectar posibles áreas de oportunidad para mejoras inmediatas
b) Etapa de Planeación
1 Hacer la matriz de riesgos
2 Hacer un plan general de auditoría en informática
3 Definir objetivos y alcances del proyecto
4 Hacer un plan detallado de auditoría en informática
4.1 Etapas y tareas
4.2 Responsables e involucrados

Figura 4.2. Ejemplo de contrato de auditoría en informática **(Continúa)**

4.3 Productos terminados
4.4 Revisiones (formales e informales)
5. Definir los elementos por auditar por cada área de revisión
6. Establecer técnicas y herramientas por cada área de revisión
6.1 Técnicas
6.2 Software
6.3 Equipo de cómputo
6.4 Otros
7. Definición de políticas o procedimientos por cada área que será auditada
8. Elaboración o actualización de cuestionarios por área de revisión
8.1 Cuestionarios por cada área que será auditada
8.2 Cuestionarios adicionales

c) Etapa de Formalización:
1. Presentar formalmente el proyecto
1.1 Propuesta de servicios
1.2 Plan detallado final
1.3 Proyecto revisado de la auditoría en informática

TERCERA. PROGRAMA DE TRABAJO

El cliente y el auditor convienen en desarrollar en forma conjunta un programa de trabajo en el que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realización

CUARTA. SUPERVISIÓN

El cliente o quien designe tendrá derecho a supervisar los trabajos que le han encomendado al auditor dentro de este contrato y a dar por escrito las instrucciones que estime convenientes

QUINTA. COORDINACIÓN DE LOS TRABAJOS

El cliente designará por parte de la organización a un coordinador del proyecto quien será el responsable de coordinar la recopilación de la información que solicite el auditor y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas

SÉXTA. HORARIO DE TRABAJO

El personal del auditor dedicará el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes y gozará de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estarán sujetos a horarios y jornadas determinadas

SÉPTIMA. PERSONAL ASIGNADO

El auditor designará para el desarrollo de los trabajos objeto de este contrato a socios del despacho quienes, cuando considere necesario incorporarán personal técnico capacitado de que disponde la firma, en el número que se requieran de acuerdo a los trabajos a realizar

OCTAVA. RELACIÓN LABORAL

El personal del auditor no tendrá ninguna relación laboral con el cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el auditor en ningun momento se considera intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre el y su personal, y exime al cliente de cualquier responsabilidad que a este respecto existiere

NOVENA . PLAZO DE TRABAJO

El auditor se obliga a terminar los trabajos señalados en la cláusula segunda de este contrato en _____ días hábiles después de la fecha en que se firme el contrato y se ha cobrado el anticipo correspondiente. El tiempo estimado para la terminación de los trabajos está en relación a la oportunidad en que el cliente entregue los documentos requeridos por el auditor y por el cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin prejuicio alguno para el auditor

DÉCIMA. HONORARIOS

El cliente pagará al auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de

Figura 4.2. Ejemplo de contrato de auditoría en informática (Continúa)

_____ más el impuesto al valor agregado correspondiente. La forma de pago será la siguiente:

a) _____% a la firma del contrato
b) _____% a los _____ días hábiles después de iniciados los trabajos
c) _____% a la terminación de los trabajos

DECIMOPRIMERA. ALCANCE DE LOS HONORARIOS

El importe señalado en la cláusula décima compensará al auditor por sueldos, honorarios, organización y dirección técnica propia de los servicios de auditoría, prestaciones sociales y laborales de su personal.

DECIMOSEGUNDA. INCREMENTO DE HONORARIOS

En caso de que se tenga un retraso debido a la falta de entrega de información, demora o cancelación de las reuniones, o cualquier otra causa imputable al cliente, este contrato se incrementará en forma proporcional al retraso y se señalará el incremento de común acuerdo.

DECIMOTERCERA. PARTE COMPLEMENTARIA

El cliente conviene con el auditor que de ser aceptada la propuesta de servicios y el plan detallado final, se continuará con la parte complementaria de este contrato, misma que será definida por acuerdo entre ambas partes.

DECIMOCUARTA. TRABAJOS ADICIONALES

De ser necesaria alguna adición a los alcances o productos del presente contrato, las partes celebrarán por separado un addendum que formará parte integrante de este instrumento y en forma conjunta se acordará el nuevo costo.

DECIMOQUINTA. VIÁTICOS Y PASAJES

El importe de los viáticos y pasajes en que incurra el auditor en el traslado, hospedaje y alimentación que requieran durante su permanencia en la ciudad de _____, como consecuencia de los trabajos objeto de este contrato, será por cuenta del cliente.

DECIMOSEXTA. GASTOS GENERALES

Los gastos de fotocopiado y dibujo que se produzcan con motivo de este contrato correrán por cuenta del cliente.

DECIMOSÉPTIMA. CAUSAS DE RESCISIÓN

Serán causas de rescisión del presente contrato la violación o incumplimiento de cualquiera de las cláusulas de este contrato.

DECIMOCTAVA. JURISDICCIÓN

Todo lo no previsto en este contrato se regirá por las disposiciones relativas, contenidas en el código civil del _____ y, en caso de controversia para su interpretación y cumplimiento, las partes se someten a la jurisdicción de los tribunales federales renunciando al fuero que les pueda corresponder en razón de su domicilio presente o futuro.

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad en original y tres copias, en la ciudad de _____, el día _____.

_____ _____
EL CLIENTE EL AUDITOR

Figura 4.2. Ejemplo de contrato de auditoría en informática

4.3. ETAPA DE DIAGNÓSTICO

Diagnóstico de la Empresa o Institución

Esta etapa es el primer paso práctico del auditor en informática dentro de las empresas o instituciones al efectuar un proyecto de auditoría en informática. Se busca la opinion de la alta dirección para estimar el grado de satisfacción y confianza que tiene sobre los productos y servicios que brinda el área de informática, así como sus aciertos y debilidades.

Un punto importante que debe quedar plasmado en esta etapa son las areas de oportunidad que tiene informática para hacer más competitiva y rentable a la empresa.

A esta etapa no se debe considerar como un conjunto de tareas que requiere muchos recursos o un tiempo considerable, es simplemente un aspecto necesario y generalizado para conocer la empresa o institución y los puntos debiles y fuertes de la función de informática desde el punto de vista de los usuarios clave y la alta dirección.

Los aspectos por evaluar en esta etapa se mencionan a continuación. Ahora bien, si el auditor considera que la complejidad del negocio, la fusión o compra de la empresa, la informalidad evidente en el área de informática o alguna consideración especifica para el coordinador de la auditoria en informática o a petición de la alta dirección, requieren más puntos por considerar y un tiempo más prolongado, conviene que los integre en esta fase, ya que aquí se detectan los primeros síntomas de informática que, posteriormente, pueden ser los mas importantes

Misión, objetivos y organización de la institución

El auditor en informática debe conocer el tipo de organización, la misión, estrategias, planes, organización, el nivel jerárquico de la función de informática, los procesos básicos de la empresa, así como las entidades externas que se relacionan con cada area de la empresa.

Los elementos relevantes que ha de solicitar el auditor en informática para su análisis preliminar son los manuales de organizacion y procedimientos donde conocerá

- Misión de la empresa
- Objetivos de la empresa
- Organización de la empresa
- Relación existente entre las diversas areas o departamentos
- Relación de la empresa con entidades externas
- Politicas y normas de la empresa
- Procedimientos de la empresa
- Otros de interés para el auditor en informática

Grado de apoyo a la institución

El auditor en informática debe obtener una idea global del grado de apoyo y satisfacción que existe en la empresa de los servicios de informática y estimar hacia dónde se orientan.

- Apoyo a la alta dirección
- Apoyo a las gerencias
- Apoyo a los niveles operativos

Debe conocer de manera general los siguientes aspectos.

- Participación de la función de informática en los proyectos clave de la empresa
- Difusión de las politicas y planes de informática en los niveles estratégico, táctico y operativo
- Imagen de informática ante la alta direccion y los responsables de cada área del negocio
- Grado de satisfacción que existe por cada servicio prestado por la función de informática
- Expectativas que tiene la empresa referentes a informática

- Fortalezas y debilidades de informática
- Areas de oportunidad propuestas por la alta dirección, usuarios, personal de informática
- Otros de interés para el auditor en informática

Diagnóstico del área de informática

En esta parte, el auditor en informática se coordina directamente con el responsable del área de informática.

Organización y objetivos del área de informatica

El auditor conocerá:

- Objetivos del área de informática
- Organización del área de informática
- Relación del área de informatica con las otras areas de la empresa
- Politicas y normas del área de informática
- Procedimientos del área de informática
- Planes del area de informática
- Estrategias del área de informática
- La tecnologia de software y hardware con la que cuenta el área de informática

Se busca también la información relacionada con algunos aspectos indagados entre los usuarios y la alta direccion con objeto de encontrar la congruencia o discrepancia entre una opinión y la otra.

Las entrevistas deben efectuarse con el responsable del area de informática y ocasionalmente con los encargados directos de las funciones clave de esta área. Es indispensable hacerles entender la importancia de su apoyo en este tipo de proyectos y brindarles la seguridad de que al final todo será para beneficio de todos.

Control

Otra actividad de la etapa del diagnostico es evaluar el grado de formalidad y cumplimiento que se da a politicas, controles y procedimientos relativos a cada area de informática.

Una manera de obtener dicha información es a través de la entrevista que concede el responsable de informatica al lider del proyecto, pero el camino mas directo es entrevistar al encargado de cada área que conforma la función de informática, evitando caer en el detalle y ocupar mucho tiempo en las entrevistas.

Algunos aspectos que se deben considerar son los siguientes:

- Politicas y procedimientos de organizacion de la funcion de informática
- Descripción de puestos y funciones
- Evaluacion de desempeño
- Politicas y procedimientos para el desarrollo e implantacion de sistemas
- Politicas y procedimientos de evaluacion de hardware y software
- Politicas y procedimientos de seguridad
- Politicas y procedimientos de mantenimiento (preventivo y correctivo)
- Plan de contingencias
- Otros de interés para el auditor en informática

Productos y servicios

Un aspecto clave que se tiene que considerar en la etapa de diagnostico es la evaluación general de los servicios que presta el área de informática a las otras areas de la empresa.

El auditor en informática ya puede formarse un juicio inicial de la congruencia entre las áreas usuarias y el responsable de informática; aquí se detecta por lo general qué servicios ya son aceptados en la empresa y cuáles sólo son operativos o necesarios para llevar a cabo tareas que no producen valor agregado.

El responsable del área de informática no debe ser su propio juez, pero al menos puede brindar su opinión personal de lo que considera que es su grado de apoyo a la empresa y comprobarlo o manifestarlo mediante minutas, memorandos, reconocimientos, etc., de los usuarios y de la alta dirección.

El objetivo de conocer su opinión al respecto, es encontrar la congruencia entre su función y lo que dice la alta dirección que debe ser. No se busca crear controversias ni encontrar fallas personales.

El auditor en informática tiene la responsabilidad moral de dar un sentido crítico y práctico a todas las áreas de la empresa para encontrar un mejor modo de hacer las cosas desde el punto de vista profesional en el campo de informática y, de ser posible, en las áreas de la empresa involucradas en este tipo de proyectos. Los servicios que brinda generalmente informática son:

- Implantación de soluciones de información
  - Desarrollo de sistemas de información
  - Compra y adecuación de aplicaciones hechas por expertos
  - Bases de datos
- Evaluación, adquisición instalación y reemplazo de
  - Equipo de cómputo
  - Paquetes de software
  - Equipos de telecomunicaciones
  - Lenguajes de programación
- Mantenimiento
  - Sistemas de información
  - Bases de datos
  - Equipos de cómputo
  - Equipo de telecomunicaciones
  - Redes locales
- Soporte a usuarios
  - Capacitación
  - Asesoría
- Investigación
  - Tecnológica (equipos de cómputo, comunicaciones, CASE, etc.)
  - Aplicaciones en el mercado
- Planeación de informática
- Auditoría en informática
- Soporte a la alta dirección
- Otros de acuerdo con el tipo de empresa

Los servicios pueden ser ejecutados por externos y coordinados por el área de informática. El auditor en informática ha de encontrar las causas o los efectos que esto causa en la empresa.

Es muy recomendable que en esta tarea el auditor en informática documente todas las observaciones relevantes expuestas por el responsable del área de informática en relación con los servicios que proporciona, con la finalidad de cruzarlas con las hechas por la alta dirección y los principales usuarios de la organización.

Áreas de oportunidad

Aquí se detectan todas las circunstancias que facilitarán la puesta en marcha de soluciones brindadas por informática y que tendrán un impacto relevante en alguna función o gerencia de la empresa; de igual manera, cabe proponer acciones inmediatas o a corto plazo que redunden en

beneficios directos para la alta dirección, dichas acciones pueden encaminarse a aprovechar por ejemplo a alguna de las siguientes areas de oportunidad

- Capacitación o actualización profesional del personal de informática
- Creación y difusión de nuevos servicios de informatica en la empresa
- Reubicación de la función del área de informatica en la estructura organizacional
- Capacitación a los niveles ejecutivos y a los usuarios clave acerca de las aplicaciones instaladas
- Actualización tecnológica
- Sistematización de algunas areas de la empresa
- Creación de algún comité de informática
- Formalización y divulgación de políticas y planes de informatica en la empresa

Las areas de oportunidad pueden emanar de la alta direccion, de los usuarios, del responsable del area de informatica o del mismo auditor en informática; sin embargo, todas las propuestas deben ser analizadas y documentadas antes de ponerlas en práctica

Existen muchas razones para que el auditor en informatica tome en cuenta las areas de oportunidad expresadas por la alta dirección, los usuarios clave y el responsable de informatica. La principal es que todas esas personas viven y dedican gran parte de su tiempo a la empresa, por lo que conocen mejor que nadie sus fortalezas, debilidades y tipo de soluciones

No significa que el auditor en informática se comprometa a efectuar todas las tareas y actividades sugeridas por ellos. La deduccion y objetividad empiezan a ser un factor clave en este momento; se revisarán o auditarán sólo las funciones o areas relacionadas con informática que se enfoquen en la misión del auditor en informática, esto es, nada más se pondrán en el plan tareas orientadas a dar un valor agregado a la empresa e incumban directamente a la función de auditoria en informática (seguridad, calidad y control)

Algunos proyectos enfocados al aprovechamiento y logro de areas de oportunidad, requieren que los responsables directos de su planeación, desarrollo e implantación pertenezcan al personal del área de informática o de auditoria financiera u operativa, no al equipo del auditor en informática. En este caso, se debe tener cuidado de encauzar las areas de oportunidad a quienes correspondan y ofrecer el apoyo de auditoria en informática sólo en el caso en que se necesite

El criterio de un auditor en informática puede incrementar o reducir el alcance de la etapa de diagnóstico dependiendo de las caracteristicas de la empresa, así como de las restricciones o facilidades en factores criticos del proyecto (como tiempo, presupuesto o los objetivos buscados por la alta dirección o el responsable de la auditoria en informática)

Con base en lo anterior es recomendable acompañar los aspectos complementarios con cuestionarios o preguntas específicas para tal fin

A continuación se proporcionan los cuestionarios detallados que apoyaran al auditor en informática para obtener la información mencionada, esto es, los diagnósticos de la empresa y del área de informática (tablas 4.1 a 4.11). El cumplimiento total y secuencial de los cuestionarios es recomendable, sin embargo, el criterio del coordinador de auditoria en informatica y las circunstancias particulares del proyecto pueden variar el grado de uso del mismo

Tabla 4.1. Cuestionario de Diagnóstico de la Organización
Aspectos generales

Empresa: Fecha de elaboración:
Líder de proyecto:

CONCEPTO	DESCRIPCIÓN	COMENTARIOS
Giro y misión de la organización (solicitar organigrama)		
Áreas de la organización		
Macroproyectos de la organización		
Objetivos de la organización		
Políticas referentes a la función de informática		
Áreas de oportunidad que se derivan de informática		

Tabla 4.2. Cuestionario de Diagnóstico de la Organización
Soluciones de informática

Empresa: Fecha de elaboración:
Líder de proyecto:

¿CUÁL DE LAS SIGUIENTES SOLUCIONES LE HAN SIDO PROPORCIONADAS POR INFORMÁTICA Y CÓMO LAS CALIFICA?	E	B	R	D
• Soluciones de consultoría – Asesoría y soporte en la definición, evaluación y selección de estrategias para la obtención de soluciones de negocio	( )	( )	( )	( )
• Soluciones de sistematización de procesos – Instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	( )	( )	( )	( )
• Soluciones de desarrollo tecnológico – Evaluación y selección de tecnología de vanguardia, definición de nuevos enlaces con otras empresas vía telecomunicaciones, automatización de oficinas, etc.	( )	( )	( )	( )
• Servicios técnicos – Instalación de equipo de cómputo y telecomunicaciones	( )	( )	( )	( )
– Capacitación en el uso de la tecnología	( )	( )	( )	( )
– Atención a fallas de software y aplicaciones	( )	( )	( )	( )
– Atención a fallas en equipos de cómputo y comunicaciones	( )	( )	( )	( )

E= Excelente B= Buena R= Regular D= Deficiente

Tabla 4.3. Cuestionario de Diagnóstico de la Organización
Aspectos administrativos del área de informática

Empresa: Fecha de elaboración:
Líder de proyecto:

CONCEPTO	DESCRIPCIÓN	COMENTARIOS
Misión del area de informática (solicitar organigrama)		
Funciones del area de informatica		
Macroproyectos del area de informatica		
Objetivos de la funcion del area de informática		
Políticas referentes a cada función del área de informatica		
Areas de oportunidad que se derivan del área de informática		

Tabla 4.4. Cuestionario de Diagnóstico del Área de Informática
Paquetes de software instalados

Empresa: Fecha de elaboración:

NOMBRES	ORIGINAL (SI/NO)	NÚMERO DE INSTALACIONES
Sistema Operativo	( )	
Sistema Operativo de Red	( )	
Interfase gráfica	( )	
Procesador de palabras	( )	
Hojas de cálculo	( )	
Graficadores	( )	
Lenguajes de programación	( )	
Manejadores de bases de datos	( )	
Correo electrónico	( )	
Para servicios de internet	( )	
De conectividad	( )	
Multimedia	( )	
Herramientas CASE y software de inteligencia artificial	( )	
Utilerías y otros	( )	

Tabla 4.5. Cuestionario de Diagnóstico del Área de Informática
Sistemas de información instalados

Empresa **Fecha de elaboración**

NOMBRES	SI	NO	NÚMERO
Sistemas estratégicos de información	( )	( )	
Sistemas tácticos de información	( )	( )	
Sistemas operativos de informacion	( )	( )	

* Los sistemas estratégicos de informacion apoyan directamente a la alta direccion en la toma de decisiones.
* Los sistemas tacticos apoyan al nivel gerencial en el desempeño de sus funciones administrativas y de toma de decision
* Los sistemas operativos de información apoyan las actividades operativas diarias de la organizacion

Tabla 4.6. Cuestionario de Diagnóstico del Área de Informatica
Capacitación y actualización en software

Empresa: Fecha de elaboracion:

NOMBRES	E	B	R	D
Sistema Operativo	( )	( )	( )	( )
Sistema Operativo de Red	( )	( )	( )	( )
Interfase grafica	( )	( )	( )	( )
Procesador de palabras	( )	( )	( )	( )
Hojas de calculo	( )	( )	( )	( )
Graficadores	( )	( )	( )	( )
Lenguajes de programacion	( )	( )	( )	( )
Manejadores de bases de datos	( )	( )	( )	( )
Correo electrónico	( )	( )	( )	( )
Para servicios de Internet	( )	( )	( )	( )
De conectividad	( )	( )	( )	( )
Multimedia	( )	( )	( )	( )
Herramientas CASE y software de inteligencia artificial	( )	( )	( )	( )
Utilerias y otros	( )	( )	( )	( )

E= Excelente
B= Buena
R= Regular
D= Deficiente

Tabla 4.7. Cuestionario de Diagnóstico del Area de Informática
Utilización del software

Empresa: Fecha de elaboración

NOMBRES	A	B	C	D
Sistema Operativo	( )	( )	( )	( )
Sistema Operativo de Red	( )	( )	( )	( )
Interfase grafica	( )	( )	( )	( )
Procesador de palabras	( )	( )	( )	( )
Hojas de cálculo	( )	( )	( )	( )
Graficadores	( )	( )	( )	( )
Lenguajes de programación	( )	( )	( )	( )
Manejadores de bases de datos	( )	( )	( )	( )
Correo electrónico	( )	( )	( )	( )
Para servicios de internet	( )	( )	( )	( )
De conectividad	( )	( )	( )	( )
Multimedia	( )	( )	( )	( )
Herramientas CASE y software de inteligencia artificial	( )	( )	( )	( )
Utilerías y otros	( )	( )	( )	( )

A = Usado por la dirección
B = Usado por las gerencias
C = Usado por las jefaturas
D = Usado por el nivel operativo

Tabla 4.8. Cuestionario de Diagnóstico del Área de Informatica
Utilización del hardware

Empresa: Fecha de elaboración:

NOMBRES	A	B	C	D
Microcomputadoras	( )	( )	( )	( )
Computadoras portátiles	( )	( )	( )	( )
Minicomputadoras	( )	( )	( )	( )
Mainframes	( )	( )	( )	( )
Supercomputadoras	( )	( )	( )	( )
Redes locales	( )	( )	( )	( )
Redes de área amplia, metropolitanas y globales	( )	( )	( )	( )
Transmision por satelite	( )	( )	( )	( )
Transmisión por microondas	( )	( )	( )	( )
Transmisión telefónica	( )	( )	( )	( )
Máquinas impresoras	( )	( )	( )	( )
Hardware de multimedia	( )	( )	( )	( )
Varios (scanners, plotters)	( )	( )	( )	( )

A = Usado por la direccion B = Usado por las gerencias C = Usado por las jefaturas D = Usado por el nivel operativo

Tabla 4.9. Cuestionario de Diagnóstico del Área de Informatica
Capacitación y actualizacion en los sistemas

Empresa: Fecha de elaboración:

NOMBRES	E	B	R	D
Sistemas estrategicos de información	( )	( )	( )	( )
Sistemas tacticos de informacion	( )	( )	( )	( )
Sistemas operativos de informacion	( )	( )	( )	( )

* Los sistemas estrategicos de información apoyan directamente a la alta direccion en la toma de decisiones
* Los sistemas tacticos apoyan al nivel gerencial en el desempeño de sus funciones administrativas y de toma de decision
* Los sistemas operativos de información apoyan las actividades operativas diarias de la organizacion

Tabla 4.10. Cuestionario de Diagnóstico del Área de Informática
Inventario de manuales y documentos

INVENTARIO DE MANUALES Y DOCUMENTOS

Empresa: Fecha:

Hoja 1/

Tipo de Documento	Título del Documento	Cantidad	Editorial
Utilerías			
Procesadores de Texto			
Aditamentos para Hardware			
Monitores			
Impresoras			
Redes			
Equipos			
Aplicaciones			
Sistemas Operativos			
Multimedia			
Lenguajes de programación			
Bases de datos			
Drivers y Otros			
Gráficos			
Hojas de Cálculo			

Tabla 4.11. Cuestionario de Diagnóstico del Área de Informática

Inventario de software

INVENTARIO DE SOFTWARE

Empresa:

Fecha:

Hoja 1/

Tipo de Software	Nombre	¿Ver.	Copias	No. Disk.	Almacenamiento	Fabricante
Elaborado por la dependencia						
Bases de Datos						
Drivers y Otros						
Gráficos						
Hojas de Cálculo						
Lenguajes de programación						
Redes						
Sistemas Operativos						
Utilerías						
Multimedia						
Aplicaciones						

4.4. ETAPA DE PLANEACIÓN

Una vez que se ha concluido la etapa de diagnóstico, se procede a continuar con la etapa de planeación, la cual se explica a continuación.

Cuando se han analizado, evaluado y determinado las áreas de oportunidad específicas de auditoría en informática, deben traducirse en el plan de auditoría en informática, en tareas y productos terminados. Las tareas y actividades que se reflejan en este momento se contemplarán con la matriz de riesgos.

Matriz de riesgos. Justificación por área de revisión

La siguiente tarea del auditor en informática es elaborar la matriz de riesgos, cuyo objetivo principal es detectar las áreas de mayor riesgo en relación con el área de informática y que requieren una revisión formal y oportuna. En el cuadro 4.3, se muestra el contenido final que debe tener la matriz de riesgos. Algunas consideraciones que se deben tener al elaborar la matriz de riesgos son:

- Es importante identificar el nivel de riesgo de cada uno de los elementos que integran la función de informática en la empresa a través del diagnóstico de la situación actual del área de informática
- Las áreas que serán diagnosticadas pueden variar según el tamaño y estructura de la empresa, originando en ocasiones que el auditor en informática tenga que evaluar productos y servicios de informática con un enfoque centralizado o descentralizado, según sea el caso
- El auditor debe utilizar todos los parámetros de medición y evaluación posibles sin caer en un análisis detallado, ya que solo se trata de detectar la problemática principal de cada área (puede apoyarse en especialistas de informática, auditoría financiera, asesores o consultores externos)
- Si emanan anomalías de considerable importancia de algún elemento evaluado, se deben tomar opciones inmediatas orientadas a eliminarlas o minimizarlas (en el plan de auditoría en informática se plantearán como acciones inmediatas)
- Determinar el nivel de riesgo que existe en cada área de la función de informática, cada área, producto o servicio de informática es susceptible de evaluación y control para asegurar que se desarrolle de acuerdo con los estándares, políticas y procedimientos específicos que le han sido asignados de acuerdo con su función)
- Los parámetros para medir el nivel de riesgos pueden variar de acuerdo con factores como la experiencia y conocimiento en la auditoría y de las áreas que conforman informática o el grado de profundidad y análisis que desee darle el auditor en informática
- Algunos hechos pueden indicar directamente al auditor en informática la existencia de riesgos relevantes
- Revisar la matriz de riesgos con el responsable de auditoría en informática
- Asegurarse de tener el soporte que requieran las debilidades o anomalías detectadas (entrevistas, visitas y cuestionarios analizados, revisados y documentados)
- Clasificar cada área y sus componentes por nivel de riesgo, lo que puede ser determinado por el coordinador de la auditoría en informática, los usuarios clave o el responsable de informática
- Dar prioridades a cada área de revisión de acuerdo con el nivel de riesgo o por factores específicos mencionados por la alta dirección o el responsable de informática
- Justificar cada una de las áreas seleccionadas para auditar. La justificación debe basarse en el nivel de riesgo que representa, de acuerdo con las prioridades establecidas por los involucrados, de alto nivel o solicitud expresa de la alta dirección o del responsable de informática

Cuadro 4.3. Matriz de riesgos

Empresa: Fecha de elaboración:

Representante del área de informática:

ÁREAS SUSCEPTIBLES DE AUDITAR		ASPECTOS O COMPONENTES POR EVALUAR	RIESGO POR COMPONENTE	TOTAL DEL RIESGO POR ÁREA	NÚMERO DE ÁREA SEGÚN CLASIFICACIÓN
Administración de informática	1	Misión y objetivos	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Organización	%		
	3	Servicios	%		
	4	Parámetros de medición	%		
Dirección y niveles ejecutivos	1	Seguimiento a la función de informática por la dirección	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Comunicación e integración	%		
	3	Apoyo a toma de decisiones	%		
Usuarios de informática	1	Comunicación e integración	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Proyectos conjuntos	%		
	3	Administración de recursos de informática	%		
	4	Grado de satisfacción	%		
Control interno	1	Políticas y procedimientos	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
Ciclo de desarrollo e implantación de sistemas de información	1	Metodología	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Técnicas	%		
	3	Herramientas	%		
	4	Capacitación/actualización	%		
Sistemas de información	1	Planeación	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Desarrollo	%		
	3	Operación	%		
	4	Soluciones de mercado	%		
Mantenimiento	1	Hardware	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Software	%		
	3	Sistemas de información	%		
	4	Red de comunicaciones	%		
Redes locales	1.	Administración	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2.	Instalación	%		
	3	Operación/seguridad	%		
Telecomunicaciones	1	Administración	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2	Instalación	%		
	3	Operación/seguridad	%		
Hardware	1.	Administración	%	%	Número sugerido para auditar cada componente y área según el nivel de riesgo estimado
	2.	Instalación	%		
	3.	Operación/seguridad	%		

(Continúa)

Cuadro 4.3. Matriz de riesgos

Empresa: Fecha de elaboración:
Representante del área de informática:

ÁREAS SUSCEPTIBLES DE AUDITAR		ASPECTOS O COMPONENTES POR EVALUAR	RIESGO POR COMPONENTE	TOTAL DEL RIESGO POR ÁREA	NÚMERO DE ÁREA SEGÚN CLASIFICACIÓN
Software	1	Administración	%	%	*Número sugerido para auditar cada componente y área según el nivel de riesgo estimado*
	2	Legalización	%		
	3	Operación/seguridad	%		
	4	Capacitación	%		
Seguridad	1.	Hardware	%	%	*Número sugerido para auditar cada componente y área según el nivel de riesgo estimado*
	2	Software/aplicaciones	%		
	3.	Plan de contingencias y de recuperación	%		
Planeación de informática	1	Metodología	%	%	*Número sugerido para auditar cada componente y área según el nivel de riesgo estimado*
	3	Plan de contingencias y de recuperación	%		
	2	Técnicas	%		
	3	Herramientas	%		
	4	Capacitación/actualización	%		
Investigación tecnológica	1.	Consideraciones generales	%	%	*Número sugerido para auditar cada componente y área según el nivel de riesgo estimado*

Plan general de la auditoria en informática

Una vez elaboradas, revisadas y documentadas la matriz de riesgos y las areas de oportunidad, se procede a la formulación del plan general de informática el cual consiste básicamente en plantear las tareas más importantes que se ejecutarán durante cierto periodo al efectuar la auditoría en informática. El cuadro 4.4, puede servir de guía para la elaboración del plan general.

Los principales aspectos a considerar sobre el plan general de auditoria en informática son:

- Tomar como referencia los datos recomendados en el proceso metodológico para encontrar responsables e involucrados en esta tarea
- El plan general de auditoria en informática se deriva de los siguientes elementos:
  - Areas de oportunidad
  - Matriz de riesgos
  - Prioridades de la alta direccion, de auditoria, de informática o de la misma función de auditoria en informática
- El plan elaborado en esta etapa es general, ya que sólo busca plantear los datos básicos para que la alta dirección los analice y apruebe
- El plan detallado se lleva a cabo posteriormente
- Es muy importante la retroalimentación constante entre el lider del proyecto y los demás involucrados

Las actividades principales del auditor en informática o del lider del proyecto para la elaboración del plan general son al menos las siguientes:

- Estimar el tiempo necesario para auditar cada area determinada en la matriz de riesgos y en las tareas de apoyo a fin de lograr las areas de oportunidad planteadas
- Analizar y definir los aspectos o componentes más relevantes que se evaluarán, tomando como referencia las caracteristicas propias de la empresa
- De ser necesario verificará la importancia y validez de los puntos anteriores con los involucrados sin consumir mucho tiempo ni aplicar tecnicismos en las entrevistas (puede ser via telefónica, fax o personalmente)
- Asignar prioridades a cada area por evaluar o revisarlas con los principales involucrados en el proyecto
- Definir fechas estimadas de inicio y terminación por area de revision no por componente
- Establecer fechas de revision formales (firmas aprobaciones) e informales (avances)
- Definir responsables e involucrados directos por etapas del proyecto
- Otras de interes para el auditor en informática segun las caracteristicas del proyecto y la empresa

Aprobación del plan de auditoria en informática

El objetivo principal de esta parte es obtener el visto bueno (aprobacion) inicial de parte de la alta dirección, usuarios clave y del responsable del área de informática para continuar con el proyecto de auditoria en informática.

Los aspectos fundamentales para lograr el compromiso ejecutivo a fin de continuar con el proyecto de auditoria en informática son los siguientes:

- Presentación del plan con toda la información de soporte requerida bien documentada y validada con los principales involucrados
  - Resumen del diagnóstico actual
  - Areas de oportunidad

Cuadro 4.4. Plan General de la Auditoría

Empresa | Gerencia | Fecha de elaboración
Representante usuario | Representante de informática | Líder de proyecto

ÁREA POR AUDITAR	ASPECTOS O COMPONENTES DEL ÁREA POR AUDITAR	PRIORIDAD	CLASIFICACIÓN DEL RIESGO POR ÁREA (TOTAL)	FECHA DE INICIO	FECHA DE FIN
Área seleccionada	Componentes seleccionados del área	Número asignado	%	dd/mm/aa	dd/mm/aa
Área seleccionada	Componentes seleccionados del área	Número asignado	%	dd/mm/aa	dd/mm/aa

- Matriz de riesgos
- Prioridades
- Otros comentarios de apoyo

- Se debe ser objetivo y claro al exponer el plan general
- Justificar cada una de las areas por auditar con datos concretos y bien documentados
- Lograr que la alta dirección tome conciencia del compromiso requerido de su parte para la culminación exitosa del proyecto
- Recibir una aprobación formal del plan general (firma)
- El coordinador de auditoría en informática debe indicar fechas de inicio y terminación estimadas

Las principales actividades del auditor en informática o del coordinador de auditoría en informática para la elaboración del plan general son al menos las siguientes:

- Revisar el plan general
- Considerar fecha posible de reunión con los involucrados en esta tarea
- Documentar y resumir el diagnóstico actual
- Verificar y documentar áreas de oportunidad y matriz de riesgos
- Justificar cada área de revisión con la información obtenida anteriormente
- Recomendar o negociar fecha de revisión y aprobación del plan con los involucrados
- Efectuar reunión
- Exponer y justificar el plan de auditoría en informática
- Obtener aprobación formal del plan general
- Establecer fechas de inicio del proyecto
- Obtener el compromiso ejecutivo en todo el transcurso del proyecto
- Otros que el auditor en informática considere pertinentes

En la figura 4.3 se muestra un formato que contiene los elementos generales que se deben considerar al obtener la aprobación formal del plan general.

Definición de objetivos del proyecto de auditoría en informática por área de revisión

Los objetivos de cada etapa y tarea, deben ser elaborados entre el coordinador de auditoría en informática y los auditores en informática, validándolos con el responsable de la función de informática en la empresa.

Cada área de revisión debe contemplar de manera clara, para el auditor en informática, sus objetivos (cuantitativos o cualitativos) para poder medir si se han logrado con el paso del tiempo o no.

Los objetivos de cada área que será auditada, se especificaron en el capítulo 3 junto con los aspectos por evaluar (componentes o elementos), políticas y procedimientos recomendados y técnicas y herramientas requeridas.

Actualización del plan general

Conforme se avanza en el proyecto surgen cancelaciones, prioridades, requerimientos, expectativas, nuevos involucrados, etc., que obligan a actualizar el plan general de auditoría en informática.

Dicha actualización debe justificarse, debido a que se hizo un compromiso inicial acerca de las áreas que serían auditadas, fechas, prioridades, etc.

Se debe evitar caer en el ciclo de actualización-terminación-actualización; se recomienda poner en práctica todos los cambios pertinentes para proseguir con la elaboración del plan detallado de auditoría en informática.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO

APROBACION DEL PLAN GENERAL

México, D.F., a 18 de mayo de 1997.

POR MEDIO DEL PRESENTE DOCUMENTO SE HACE CONSTAR QUE EN REUNIÓN PACTADA EL DÍA 18 DE MAYO DE 1997 A LA CUAL ASISTIERON LAS PERSONAS QUE POSTERIORMENTE SE ENUNCIARAN, SE DECIDIÓ QUE ES FACTIBLE Y CONVENIENTE PARA LA DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO CONTINUAR CON EL PROYECTO DE AUDITORIA EN INFORMÁTICA Y SE APRUEBA EL PLAN GENERAL

L.I. CECILIA CALDERÓN ORTEGA
DIRECTOR GENERAL

L.A. EMILIANO RICO NIETO
JEFE DE UNIDAD ADMINISTRATIVA

L.I. ALEJANDRO ORTEGA ZARATE
USUARIO CLAVE

L.I. MIRIAM PRECIADO VIDALS
RESPONSABLE DEL ÁREA DE INFORMÁTICA

L.C. DEYANIRA FLORES FLORES
RESPONSABLE DE AUDITORIA EN INFORMÁTICA

L.I. MIGUEL GARCÍA URBANO
COORD. DE AUDITORÍA EN INFORMÁTICA

Figura 4.3 Formato que contiene los elementos generales considerados en la aprobación del plan general.

Conviene llevar una bitácora de cambios al plan general que contemple:

- **Cambio**
- **Motivo de cambio**
- **Responsable de solicitar el cambio**
- **Tareas o fechas que afecta**
- **Areas por evaluar afectadas por el cambio**
- **Responsable de aprobar el cambio**
- **Fecha del cambio**
- **Plan actualizado**
- **Otros que el auditor en informática considere necesarios**

Plan detallado de la auditoria en informática

Es una de las tareas más importantes de la etapa de planeación, ya que en ella se define todo el detalle de los elementos del proyecto, se especifican tareas, productos terminados, responsables, fechas, etc., que serán validados y aprobados en la etapa de formalización para arrancar el proyecto

Se pueden realizar dos planes: en uno se da seguimiento interno a las tareas y responsabilidades de los auditores en informática y en el otro se especifica el detalle emanado del plan general de auditoría en informática, mismo que involucra a la alta dirección, usuarios e informática. En los cuadros 4.5 y 4.6 se muestran los aspectos generales que deben contener los planes interno y detallado. A continuación se explican brevemente

Plan interno

Le corresponde al coordinador de la auditoria en informática y su propósito principal es verificar el cumplimiento del proceso metodológico por parte de los auditores en informática a lo largo del proyecto. Algunas razones importantes de contar con un plan de este tipo son:

- Elaborar compromisos con base en tareas, productos terminados y los responsables
- Asignar funciones y responsabilidades a los usuarios en informática involucrados en el proyecto
- El coordinador de la auditoria en informática da seguimiento a los auditores en informática con base en dicho plan
- Utilizar el grado de cumplimiento del plan en futuras evaluaciones del personal

Plan detallado de auditoria en informática

Detalla la información relacionada con:

- El desarrollo de la auditoria en informática, que corresponde a las áreas seleccionadas en la matriz de riesgos
- Documentación, revisión y aprobación del informe de auditoria en informática
- Implantación de las acciones recomendadas

Los datos mencionados en el plan detallado de informática se enfocan en ser la guía del proyecto de auditoria en informática desde el punto de vista del cliente, ya que describen tareas, productos terminados, responsables, involucrados, fechas de revisión, etc.

Aspectos relevantes del plan detallado de auditoria en informática:

- Especifica responsables e involucrados en cada área por auditar
- Es el detalle final del plan
- Ya fue adaptado y actualizado según características específicas del proyecto

- Con base en dicho plan se dará seguimiento por parte de la alta dirección, los responsables de los usuarios de informática, del personal del área de informática y de auditoría en informática.
- Con el plan detallado terminado y aprobado en la etapa de formalización, puede darse inicio a la auditoría en informática (evaluación de las áreas de informática seleccionadas).

Aspectos por evaluar en cada área de revisión

Estos aspectos o componentes fueron mencionados en la matriz de riesgos, lo que procede es confirmar si son las requeridas y si los objetivos de cada área son válidos y completos.

Es recomendable que las áreas susceptibles de auditar y los componentes de cada área que sean agregados por el auditor en informática en el momento en que un proyecto lo requiera, cuenten con los cuestionarios correspondientes, y de ser posible, con el formato y secuencia de tareas para no perder continuidad.

Definición de técnicas y herramientas por área de revisión

Aquí se especifican las técnicas y herramientas recomendadas que debe conocer amplia y satisfactoriamente el auditor en informática para la revisión de las áreas contempladas en el plan detallado.

La experiencia profesional que se haya obtenido en cada una de las áreas susceptibles de revisión, hace más viable tanto la auditoría como la definición eficiente de soluciones.

No es un punto negativo no haber trabajado en las áreas que se auditarán, simplemente el grado de investigación y actualización en los temas o aspectos que se evaluaran debe ser más profundo.

Es casi imposible que todos los auditores en informática dominen todas las áreas de informática que se pueden auditar, sin embargo, el especialista en el campo ha de actualizarse en la medida de lo posible en las áreas que considere críticas o en los requerimientos que van surgiendo a lo largo del trabajo.

En el capítulo 3 se mencionaron las técnicas y herramientas que ha de utilizar el auditor en informática.

Definición o actualización de estándares, políticas y procedimientos por área de revisión

Todas las acciones operativas y administrativas de las organizaciones se deben orientar con base en lineamientos, políticas y procedimientos, con el objetivo principal de que los individuos que en ella laboran, lo hagan en forma metódica (sin entender esto como un trabajo mecánico y robotizado), con estándares o con normas de calidad y productividad comúnmente aceptadas en negocios similares al giro de la empresa.

Las normas y habilidades personales no serán afectadas por políticas rígidas y obsoletas de algunas empresas; deberá haber compatibilidad y congruencia entre lo que determina la empresa como reglas de trabajo y las aspiraciones y habilidades del personal.

En lo que se refiere a estándares, políticas y procedimientos, se aclara que las actividades y elementos que se relacionan con informática suelen operar bajo estándares aceptados en el medio de dicho campo.

Las funciones de desarrollo e implantación de sistemas de información, al igual que las de planeación de informática o de telecomunicaciones e investigación, se encuentran en un marco nacional e internacional donde existen estándares, metodologías, técnicas y herramientas de trabajo recomendadas para un desempeño eficiente de cada una de las actividades inherentes a sus tareas.

Al igual que para las funciones de planeación, telecomunicaciones, investigación, etc., en el campo de la auditoría en informática, existen asociaciones integradas por profesionales de gran experiencia y conocimiento en el campo. Estas asociaciones se enfocan en establecer, formalizar,

Cuadro 4.5. Plan Interno de la Auditoría
(Para uso exclusivo del líder de proyecto)

Empresa:
Líder de proyecto:

Fecha de elaboración:

ETAPA	TAREAS	PRODUCTOS	INVOLUCRADOS	RESPONSABLE	REVISIONES	DURACIÓN
Preliminar						
Justificación						
Adecuación						
Formalización						
Desarrollo						
Implantación						

Cuadro 4.6. Plan Detallado de la Auditoría

Empresa
Líder de proyecto

Fecha de elaboración

TAREA		ACTIVIDADES		PRODUCTOS	RESPONSABLE	INVOLUCRADOS	FECHA DE INICIO	FECHA DE TÉRMINO	FECHA DE REVISIÓN
Verificación de datos	1	Revisar datos del proyecto	1	Prioridades y matriz de riesgos aprobados	Líder de proyecto Auditores en informática	Alta dirección Usuarios Informática			
	2	Documentar							
Evaluación de las áreas por auditar	1	Concertar citas	•	Compromiso formal	Auditores en informática	Usuarios Informática			
	2	Realizar entrevistas	•	Datos Documentos de soporte Otros	Auditores en informática	Responsables de las áreas por visitar			
	3	Efectuar visitas	•	Datos Documentos de soporte	Auditores en informática	Usuarios Informática			
	4	Aplicar cuestionarios	•	Datos Documentos de soporte	Auditores en informática	Usuarios Informática			
	5	Análisis de información	•	Observaciones iniciales Conclusiones iniciales Acciones recomendadas	Auditores en informática	Usuarios Informática			
	6	Elaboración del informe preliminar	a) Antecedentes b) Situación actual. • Fortalezas • Debilidades (observaciones) • Áreas de oportunidad c) Situación propuesta • Acciones de mejora • Plazos • Responsables		Líder de proyecto Auditores en informática	Usuarios Informática			
	7	Clasificar y documentar el informe preliminar	•	Datos Documentos de soporte	Auditores en informática	Usuarios Informática			
	8	Revisión del informe preliminar	•	Informe preliminar revisado Pendientes	Auditores en informática	Usuarios Informática			
	9	Ejecutar pendientes	•	Pendientes terminados	Auditores en informática	Usuarios Informática			
	10	Actualizar el informe preliminar	•	Informe preliminar actualizado	Auditores en informática	Usuarios Informática			
	11	Revisar el informe preliminar actualizado	•	Informe preliminar actualizado, revisado y aprobado	Líder de proyecto	Usuarios Informática			

(Continúa)

Cuadro 4.6. Plan Detallado de la Auditoría

Empresa:
Líder de proyecto:

Fecha de elaboración:

TAREA		ACTIVIDADES	PRODUCTOS	RESPONSABLE	INVOLUCRADOS	FECHA DE INICIO	FECHA DE TÉRMINO	FECHA DE REVISIÓN
Documentar el informe final del proyecto	1.	Elaborar el informe de la alta dirección	• Informe de la alta dirección	Líder de proyecto	Usuarios Informática			
	2	Elaborar el informe detallado	• Informe detallado (para usuarios e informática)	Auditores en informática				
Revisión del informe final de la auditoría	1	Presentar los informes de la alta dirección actualizados, revisados y detallados	• Informes revisados • Informes aprobados formalmente	Responsable de la función de auditoría	Alta dirección Usuarios clave			
	2	Aprobación de los informes	• Compromiso ejecutivo para realizar las acciones sugeridas	Líder de proyecto	Responsable de la función de informática			
	3.	Compromiso ejecutivo						

difundir y recomendar la aplicación de los estándares, políticas y procedimientos más convenientes a las necesidades actuales y futuras del área de auditoría en informática.

Los estándares, políticas y procedimientos de informática referentes a técnicas de análisis y diseño de sistemas de información, los diferentes tipos de base de datos, las tipologías y protocolos en comunicaciones, y los lineamientos de control interno emanan de dichas asociaciones, sin embargo, las empresas pueden crear, formalizar y difundir sus propias políticas y procedimientos, aunque su alcance y cumplimiento será interno y, en ocasiones, con sus clientes o proveedores.

Los estándares o normas no son dogma de empresa alguna, sin embargo, se orientan a lo que su nombre se refiere: a uniformar métodos de trabajo, tecnologías, parámetros de desempeño, costos, cualidades, facilidades, etc. En esto reside la ventaja de seguir lo que dictan los estándares de mercado propuestos por las asociaciones profesionales e independientes, al menos sobre trabajos de investigación.

Ahora bien, el auditor en informática no dependerá de lo que dictan a nivel nacional o internacional los estándares; éstos sólo son puntos de referencia. Su criterio y experiencia profesional, aunados a las características de la empresa donde ejerce, le dictarán la necesidad de actualizar estándares, políticas y procedimientos conforme den a la empresa las soluciones requeridas.

Hay que estar atento a lo que los especialistas propongan como estándares, políticas y procedimientos (incluyendo la auditoría en informática) a través de suscripciones a revistas especializadas, bases de datos vía telecomunicaciones, inscripciones a asociaciones, asistencia a seminarios, actualización profesional como maestrías o cursos de posgrado, estudio constante de la empresa, entre otros.

Es conveniente atender los estándares propuestos por los especialistas independientes del campo, llámense consultores o asociaciones, reconocidos a nivel local, nacional o internacional, los cuales se pueden enriquecer si intervienen proveedores líderes en el mercado del campo de la informática que se encuentre en estudio.

Las asociaciones no son las únicas que pueden establecer estándares, políticas y procedimientos de auditoría en informática aún cuando estas agrupan el mayor número de personas expertas en la auditoría e informática dedicadas a estudiar y sugerir los elementos tecnológicos o administrativos relacionados con informática (incluyendo auditoría) que se encuentran en el mercado o que se pueden introducir al mismo y que brinden soluciones a las empresas de una manera más eficiente y segura.

En ocasiones (sucede continuamente con los equipos de cómputo o el software) las ventas que logra un proveedor a nivel mundial, establecen un nuevo estándar o al contrario, la caída estrepitosa o los problemas legales afectan a tal grado la imagen de algún proveedor líder en el mercado, que sus productos tecnológicos definidos como estándares, salen del mercado para convertirse en obstáculos o sinónimos de obsolencia en las empresas.

Cabe señalar que existen consultores independientes y bajo nómina tanto en empresas privadas como gubernamentales que pueden establecer estándares, políticas y procedimientos internos. Las características que han de cumplir para tomarse como tales en las empresas son las siguientes:

- Referir exigencias externas relativas al control y la seguridad
- Justificar la necesidad de su existencia ante la empresa
- Probados, difundidos y autorizados por el responsable directo donde se ejercerán o llevarán a la práctica
- Elaborados y descritos formalmente en documentos (hojas, archivos, etc.)
- Aprobados por la alta dirección
- Difundidos amplia y formalmente por los involucrados en su cumplimiento
- Cumplidos formalmente
- Actualizarlos con oportunidad (evitar su obsolescencia)

Hay que recalcar que las asociaciones profesionales tienen un reconocimiento oficial que no poseen los paradigmas establecidos por los consultores independientes o el personal interno de una empresa (a menos que el liderazgo o impacto de ellas trascienda a las demás empresas y se convierta en estándar de mercado).

Las ventajas de las asociaciones nacionales e internacionales al respecto son:

- Los estándares recomendados son reconocidos a nivel nacional e internacional
- Agrupan personal de gran experiencia en el campo
- Existen programas de actualización e iniciación en la auditoría en informática para apoyar a las empresas con oportunidad y eficiencia en aspectos de seguridad y control
- Cursos y seminarios continuos
- Se pueden intercambiar experiencias con miembros de diferentes empresas y países

En el capítulo 3 se mencionaron las políticas y procedimientos que se deben seguir en las diferentes áreas del departamento de informática.

Elaboración o actualización de cuestionarios por área de revisión

Cada entrevista, visita o verificación de la etapa de desarrollo de la auditoría en informática, será apoyada con preguntas específicas y definidas con anterioridad.

Los cuestionarios que corresponden a cada área que será auditada tendrán carácter formal y estarán orientados a detectar las debilidades o inexistencias relativas al control y seguridad de informática que competen a cada área.

Los cuestionarios pueden aplicarse en una entrevista personal con los involucrados en el proyecto (usuarios o personal de informática), por medio de visitas de verificación física (evaluación de equipos y materiales de informática de interés para el proyecto) o mediante listas de verificación (listado de preguntas breves y concretas) orientadas al personal que requiere de una atención breve por sus múltiples aplicaciones o simplemente porque lo que se busca de él es una participación mínima en el trabajo del proyecto.

Las características básicas de los cuestionarios son: actualización, orientados a los aspectos evaluados, sintéticos, técnicos si se requiere y basados en estándares nacionales e internacionales.

En el capítulo 5 se mencionarán los cuestionarios mínimos sugeridos para cada uno de los componentes de las áreas susceptibles de auditarse, mismos que deben ser actualizados y validados cada vez que las características de las áreas de revisión sufran modificaciones relevantes por efecto del medio tecnológico o de la empresa misma.

4.5. ETAPA DE FORMALIZACIÓN

Las fases anteriores fueron de introducción e investigación de la empresa y sus diversas funciones; en ellas se detectaron las debilidades y fortalezas más relevantes; se definió la planeación y proyección de las áreas que requieren ser auditadas, y se documentaron las adecuaciones o agregados requeridos. En la presente etapa (formalización) corresponde a la alta dirección dar su aprobación y apoyo formal para el desarrollo del proyecto de auditoria presentado por el coordinador de auditoria en informática y el responsable de la función de auditoria en informática.

La participación real de la alta dirección es basica lo mismo que la del responsable de la función de informática en la empresa. Los usuarios clave también deben estar presentes durante el proceso de formalización del proyecto.

El objetivo primario de esta etapa es claro: justificar el desarrollo del proyecto con base en todos los argumentos y detalles encontrados, analizados y clasificados en las bases anteriores.

La duración de la etapa no debe ser muy prolongada, ya que se obtuvo el visto bueno de los usuarios clave y del personal de informática en la etapa de planeación.

Verificación de prioridades, restricciones y alcances del proyecto

La verificación, validación, clasificación y documentación de las prioridades, restricciones y alcances del proyecto son de alto valor para el auditor en informática, ya que mediante su realización se clarifica el rumbo, límites y cobertura que tendrá el proyecto.

Las actividades requeridas en la presente tarea son una serie de pequeñas entrevistas personales o reuniones de varios involucrados con un enfoque muy objetivo y práctico.

Se recomienda que el auditor en informática (o el coordinador de auditoria en informática) documenten lo expuesto en las reuniones o entrevistas que se efectúen mediante una minuta o resumen (tablas, gráficas, narrativa, etc.), donde se mencionen los puntos tratados y las conclusiones. Lo anterior tiene más validez si aparecen las firmas de conformidad de cada participante.

Prioridades. Son las acciones que deben llevarse a cabo antes que las demás sugeridas para el proyecto. Esto se justifica al menos por las siguientes circunstancias:

- Urgencia de mejorar algún hecho que perjudica en alto grado a la empresa
- Un requerimiento específico de la alta dirección
- Implantación de algún proceso previamente justificado
- Otros

Restricciones. Son los hechos o circunstancias identificables que están ocurriendo o que pueden ocurrir en el transcurso de la auditoria y que van a afectar directa o indirectamente al proyecto. Por lo general son limitaciones o carencias que no se podrán resolver de inmediato a lo largo del proyecto, por ejemplo:

- Falta de experiencia de los auditores en informática
- Bajo presupuesto para asignar recursos al proyecto
- Escepticismo de la alta dirección o de los usuarios respecto de este tipo de proyectos
- Otros

Alcance. Aquí se define la cobertura específica que tendrá el proyecto, se aclara qué se hará en éste (tareas y etapas) y los resultados (productos terminados).

Lo que no se mencione aquí (excepto que se justifique la omisión) no se obtendrá durante el proyecto. Es muy importante valorar estos aspectos al menos una vez antes de que arranque el proyecto; después sería ir en contra del proceso metodológico y de los recursos y tiempos dedicados hasta este punto.

Verificación y actualización del plan de auditoría en informática

Se ha hablado de cómo actualizar un plan; lo importante en este momento es asegurarse de que los pocos (pero significativos) cambios que se hayan suscitado después de realizar la tarea anterior, se reflejen en el plan detallado de auditoría en informática que se presentará a la alta dirección para su aprobación final y formal.

Presentación formal del proyecto de auditoría en informática

La presente tarea es la más importante para el coordinador de auditoría en informatica y el responsable de la auditoría en informática, ya que en ésta se justificará la continuación del proyecto. Las actividades primordiales del responsable de esta tarea son:

- Asegurarse de contar con toda la información en un formato de presentación resumida e inteligible, ya que su principal audiencia será la alta dirección, los usuarios clave y el responsable de informática.
- Revisarla y verificarla con este último.
- Concertar la cita en una fecha y lugar apropiados.
- Ser fluido, claro y contundente en la presentación de la información.
- Asegurar el entendimiento de la audiencia de los datos presentados.

Las consideraciones clave son:

- Contar con todo el soporte documentado de lo que será presentado.
- No asistir a la junta sin aclarar las dudas o pendientes de tareas anteriores.
- Lograr que la alta dirección tome conciencia de la importancia de su apoyo al proyecto.
- Hacer que todos los presentes comprendan que forman un equipo de trabajo.
- Apoyarse en los usuarios clave o en el responsable de informática, de ser necesario.

Dentro de ésta tarea se presentan dos documentos a la alta dirección: la propuesta de servicios de auditoría en informática y el plan detallado final; la alta dirección junto con un representante del personal usuario y el responsable del área de informática, evaluarán dichos documentos y en ese momento se decidirá si se continua el proyecto o no.

La propuesta de servicios contiene los antecedentes, objetivo, alcances, tiempos y costos del proyecto de la auditoría en informática. Un ejemplo del contenido general de los aspectos que debe contener la propuesta de servicios de auditoría en informática lo podemos ver en la figura 4.4.

El plan detallado final incluye las tareas, actividades, productos terminados, responsables, involucrados, fechas de inicio y termino y las fechas de revisión del proyecto de auditoría en informática. Un ejemplo del contenido general de los aspectos que debe contener el plan detallado final lo pudimos ver en el cuadro 4.6 de la etapa de planeación.

PROPUESTA DE SERVICIOS DE AUDITORÍA EN INFORMÁTICA.

I. ANTECEDENTES

Anotar los antecedentes específicos del proyecto de auditoría

II. OBJETIVO DE LA AUDITORÍA EN INFORMÁTICA

Anotar el objetivo de la auditoría

III. ALCANCES DEL PROYECTO

El alcance del proyecto comprende

1. Evaluación de la administración de informática en lo que corresponde a:
   - Misión y funciones de la informática
   - Organización
   - Servicios
   - Parámetros de medición
2. Evaluación de la dirección y niveles ejecutivos en lo que corresponde a
   - Seguimiento a la función de informática por la dirección
   - Comunicación e integración
   - Apoyo a toma de decisiones
3. Evaluación de los usuarios de informática en lo que corresponde a:
   - Comunicación e integración
   - Proyectos conjuntos
   - Administración de recursos de informática
   - Grado de satisfacción
4. Evaluación del control interno en lo que corresponde a
   - Políticas y procedimientos
5. Evaluación del ciclo de desarrollo e implantación de sistemas de información en lo que corresponde a
   - Metodología
   - Técnicas
   - Herramientas
   - Capacitación/actualización
6. Evaluación de sistemas de información en lo que corresponde a:
   - Planeación
   - Desarrollo
   - Operación
   - Soluciones de mercado
7. Evaluación del mantenimiento en lo que corresponde a
   - Hardware
   - Software
   - Sistemas de información
   - Red de comunicaciones
8. Evaluación de redes locales en lo que corresponde a
   - Administración
   - Instalación
   - Operación/seguridad
9. Evaluación de telecomunicaciones en lo que corresponde a
   - Administración
   - Instalación
   - Operación/seguridad
10. Evaluación del hardware en lo que corresponde a:
    - Administración
    - Instalación

Figura 4.4. Ejemplo de propuesta de servicios de auditoría en informática (Continúa)

- Operación/seguridad

11. Evaluación del software (paquetes de uso general, lenguajes de programación, sistemas operativos, paquetes de uso específico) en lo que corresponde a:
    - Administración
    - Legalización
    - Operación/seguridad
    - Capacitación
12. Evaluación de la seguridad en informática en lo que corresponde a
    - Hardware
    - Software/aplicaciones
    - Plan de contingencias y de recuperación
13. Evaluación de la planeación de informática en lo que corresponde a:
    - Metodología
    - Técnicas
    - Herramientas
    - Capacitación/actualización
14. Evaluación de investigación tecnológica (CASE, EDI, Multimedia, etc.) en lo que corresponde a.
    - Consideraciones generales
15. Otros de interés específico para el auditor en informática.

IV. TIEMPO Y COSTO

Poner el tiempo en que se llevará a cabo el proyecto, de preferencia indicando el tiempo de cada una de las etapas, costo del proyecto y forma de pago.

Figura 4.4. Ejemplo de propuesta de servicios de auditoría en informática

Aprobación formal del proyecto de auditoría en informática

Se puede decir que es la tarea más breve y una de las más importantes, ya que de ella surge la aprobación formal del proyecto. Una vez logrado el visto bueno de todos los involucrados, la responsabilidad de la función de auditoría en informática es más clara y evidente: terminar con éxito el proyecto, pues uno de los dilemas a que se enfrentan muchos proyectos ha sido superado, el obstáculo de continuar con la etapa siguiente (en gran número de empresas muchos proyectos viven entre lo que llaman comúnmente proyectos en proceso de justificación, en espera o cancelados). Aquí ha pasado a la autorización para su desarrollo y terminación, según el plan de auditoría en informática. Consideraciones clave que aseguran la terminación satisfactoria de esta tarea:

- Presentar un resumen de la matriz de riesgos, áreas de oportunidad, plan detallado de auditoría en informática, prioridades, restricciones, etc. (en términos claros)
- Entendimiento del proyecto (la información tiene el mismo significado para todos)
- No surgen adecuaciones al proyecto (nuevas prioridades, áreas por revisar, etc.)
- Se aprueba formalmente el proyecto (firma de conformidad de los involucrados)
- Se autorizan las fechas de inicio del proyecto

La alta dirección no siempre autoriza todo lo planeado; en ocasiones, la falta de una buena venta del proyecto en la presentación o la falta de compromiso por alguno de los involucrados puede retrasar su aprobación formal, sin embargo, el coordinador de la auditoría en informática o el responsable de auditoría en informática tienen que continuar justificando y documentando el proyecto hasta lograr la aprobación de todos.

En la figura 4.5 se muestra un formato que contiene los elementos generales que se deben considerar al obtener la aprobación formal del proyecto de auditoría en informática y, en la figura 4.6, se muestra el addendum del contrato de auditoría en informática expuesto en la etapa preliminar.

Compromiso de las áreas involucradas

El siguiente paso es lograr que la alta dirección, los usuarios clave, el responsable en informática y el responsable de la auditoría en informática se comprometan a lo largo del proyecto, desde ese momento hasta lo que es el desarrollo e implantación de las acciones recomendadas por auditoría en informática en su informe final. El apoyo requerido por los involucrados se traduce en los siguientes aspectos:

- Difusión de los objetivos y alcance del proyecto con los usuarios y personal de informática que serán entrevistados y visitados por los auditores en informática
- Proporcionar la información requerida por auditoría en informática
- Asignación de recursos como:
    - Equipo de cómputo, espacio físico para trabajar si se requiere estar por tiempo prolongado en las áreas de informática o usuarias y tiempo
- Cumplimiento de su función dentro del proyecto de manera oportuna
- Revisión y aprobación del informe (el cual debe ser justificado)
- Implantación de las acciones recomendadas al final del proyecto

La función de auditoría se compromete a:

- Utilizar un proceso metodológico y adecuado a la empresa
- Trabajar con ética y profesionalismo
- Dar soluciones factibles y de valor agregado
- Apoyar a informática y áreas usuarias en la implantación de soluciones recomendadas en el proyecto
- Guardar de manera confidencial la información manejada en el proyecto

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO

APROBACION FORMAL DEL PROYECTO DE AUDITORIA EN INFORMATICA

México, D.F., a 28 de mayo de 1997.

POR MEDIO DE LA PRESENTE, SE DA VALIDEZ AL SEGUIMIENTO DEL PROYECTO DE AUDITORÍA EN INFORMÁTICA EN LA DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO, FIRMANDO DE COMÚN ACUERDO LAS PERSONAS QUE A CONTINUACIÓN SE ENUNCIAN

L.I. CECILIA CALDERÓN ORTEGA
DIRECTOR GENERAL

L.A. EMILIANO RICO NIETO
JEFE DE UNIDAD ADMINISTRATIVA

L.I. ALEJANDRO ORTEGA ZARATE
USUARIO CLAVE

L.I. MIRIAM PRECIADO VIDALS
RESPONSABLE DEL ÁREA DE INFORMÁTICA

L.C. DEYANIRA FLORES FLORES
RESPONSABLE DE AUDITORIA EN INFORMÁTICA

L.I. MIGUEL GARCÍA URBANO
COORD. DE AUDITORÍA EN INFORMÁTICA

Figura 4.5. Formato que contiene los elementos generales considerados en la aprobación formal del proyecto de auditoría en informática.

ADDENDUM RELATIVO AL CONTRATO DE AUDITORÍA EN INFORMÁTICA

Addendum relativo al contrato de prestación de servicios profesionales de auditoría en informática, que tiene celebrado _____, representada por _____, en su carácter de _____, a quien en lo sucesivo se denominará el cliente, y por la otra parte, _____, representada por _____, en su carácter de _____, a quien en lo sucesivo se denominará el auditor, al tenor de las siguientes declaraciones y cláusulas

D E C L A R A C I O N E S

I Declaran las partes

a) Que el día _____ de _____ de 19_____ celebraron un contrato de prestación de servicios profesionales de auditoría en informática

b) Que en relación al referido instrumento jurídico que se menciona en la declaración anterior, las partes pactaron en la cláusula decimotercera, que de ser aceptada la propuesta de servicios y el plan detallado final, se continuaría con la parte complementaria del instrumento jurídico mencionado en la declaración anterior, la cual sería definida por acuerdo entre ambas partes, por lo que es materia de este instrumento la definición de la parte complementaria del contrato de prestación de servicios profesionales de auditoría en informática.

c) Que con el objeto de adecuar el contrato de prestación de servicios profesionales de auditoría en informática celebrado entre las partes, y atento a las necesidades y posibilidades de las mismas, manifiestan su conformidad de celebrar el presente addendum de acuerdo con las siguientes

C L Á U S U L A S

PRIMERA

Convienen las partes de común acuerdo modificar el texto de la cláusula primera del contrato que se menciona en la declaración I de este documento, de acuerdo a los siguientes términos
El auditor se obliga a prestar a el cliente los servicios de auditoría en informática para llevar a cabo las etapas de diagnóstico, planeación, formalización, desarrollo, implantación y seguimiento en el área de informática del cliente

SEGUNDA

Acuerdan las partes dejar sin efecto lo señalado en la cláusula primera del contrato de prestación de servicios profesionales de auditoría en informática mencionado en la declaración I del presente addendum, respecto a las etapas de la auditoría en informática

TERCERA

Convienen las partes de común acuerdo modificar el texto de la cláusula segunda del contrato que se menciona en la declaración I de este documento, de acuerdo a los siguientes términos:
El alcance de los trabajos que llevara a cabo el auditor dentro de este contrato son

a) Etapa de Diagnóstico:
1. Hacer un diagnóstico de la empresa o institución
   1.1 Mision, objetivos y organizacion de la institucion
   1.2 Grado de apoyo a la institución
2. Hacer un diagnóstico del área de informática
   2.1 Organización y objetivos del área de informatica
   2.2 Control
   2.3 Productos y servicios
3. Detectar posibles áreas de oportunidad para mejoras inmediatas

b) Etapa de Planeación
1. Hacer la matriz de riesgos
2. Hacer un plan general de auditoría en informática
3. Definir objetivos y alcances del proyecto
4. Hacer un plan detallado de auditoría en informática

Figura 4.6. Ejemplo de addendum del contrato de auditoría en informática (Continúa)

4.1 Etapas y tareas
4.2 Responsables e involucrados
4.3 Productos terminados
4.4 Revisiones (formales e informales)
5. Definir los elementos por auditar por cada área de revisión
6. Establecer técnicas y herramientas por cada área de revisión
6.1 Técnicas
6.2 Software
6.3 Equipo de computo
6.4 Otros
7. Definición de políticas o procedimientos por cada area que será auditada
8. Elaboración o actualización de cuestionarios por área de revisión
8.1 Cuestionarios por cada área que será auditada
8.2 Cuestionarios adicionales

c) Etapa de Formalización

1. Presentar formalmente el proyecto
1.1 Propuesta de servicios
1.2 Plan detallado final
1.3 Proyecto revisado de la auditoría en informática
2.- Obtener la aprobación formal del proyecto de auditoría en informática
2.1 Aprobación del proyecto
2.2 Compromiso ejecutivo
2.3 Inicio formal del proyecto
3. Obtener el compromiso de las áreas involucradas
3.1 Entendimiento del proyecto
3.2 Aceptación del proyecto
3.3 Compromiso de cada una de las áreas involucradas
4. Definir las áreas por visitar
4.1 Fechas de entrevistas
4.2 Fechas de visitas
4.3 Fechas para aplicación de cuestionarios

d) Etapa de Desarrollo

1. Concertar citas
2. Verificar tareas, involucrados, etc
3. Clasificar técnicas, cuestionarios y herramientas por usar
4. Efectuar entrevistas
4.1 Entrevistas realizadas
4.2 Entrevistas documentadas
4.3 Análisis de entrevistas
5. Aplicar cuestionarios
5.1 Cuestionarios aplicados
5.2 Cuestionarios documentados
5.3 Análisis de cuestionarios
6. Efectuar visitas de verificación
6.1 Visitas realizadas
6.2 Comentarios documentados
6.3 Análisis de documentos
7. Elaborar informe preliminar acerca de las áreas auditadas
7.1 Observaciones (acerca de debilidades o carencia de controles)
7.2 Areas de oportunidad
7.3 Alternativas por cada área de oportunidad detectada
7.4 Recomendaciones (acciones específicas) por alternativa
7.5 Responsables de ejecutar cada acción
7.6 Plazos de ejecucion por acción
7.7 Areas auditadas clasificadas
7.8 Informe documentado, almacenado y clasificado
8. Revisar el informe preliminar por área
8.1 Borrador de auditoría en informática revisado
9. Autorizar el borrador del informe preliminar
9.1 Informe preliminar revisado
9.2 Informe preliminar corregido
9.3 Informe preliminar entregado
9.4 Informe preliminar autorizado
10. Efectuar entrevistas, cuestionarios y visitas complementarias

Figura 4.8. Ejemplo de addendum del contrato de auditoría en informática (Continúa)

10.1 Entrevistas, cuestionarios y visitas pendientes
10.2 Informe actualizado con observaciones, acciones, etc
11 Elaborar informe final
11.1 Informe final revisado con información de todas las áreas auditadas
11.2 Informe con visto bueno del responsable de la función de auditoría en informática
11.3 Informe final almacenado en medios magnéticos (respaldo)
11.4 Documentación del informe para la alta dirección
11.5 Documentación del informe para responsables de los usuarios y del personal del área de informática
12 Elaborar un plan de implantación general de acciones sugeridas
12.1 Acciones clasificadas por plazos sugeridos
12.2 Costo/beneficio del plan
13 Aprobar informe y plan de implantación
13.1 Informe de auditoría en informática y plan aprobados
14 Presentación del informe de auditoría en informática y del plan de implantación
14.1 Informe final y plan presentados a la dirección
14.2 Informe final y plan presentados a personal usuario y de informática
15 Aprobar informe final
15.1 Revisión del informe de auditoría en informática
15.2 Aprobación del informe de auditoría en informática
15.3 Compromiso ejecutivo

e) Implantación y Seguimiento

1 Definir requerimientos para el éxito del plan de implantación
1.1 Recursos requeridos para el éxito de la implantación sugerida por auditoría en informática
1.2 Recursos aprobados
1.3 Equipo de trabajo para la implantación
1.4 Equipo de trabajo aprobado
1.5 Funciones y responsabilidades
1.6 Fechas de revisión
1.7 Productos terminados
1.8 Costo/beneficio revisado
1.9 Costo/beneficio aprobado
1.10 Inicio de la implantación
2 Desarrollar el plan de implantación detallado
2.1 Plan de implantación revisado según los resultados de la primera tarea
2.2 Plan de implantación corregido y actualizado
2.3 Documentar plan final
2.4 Plan final aprobado
3 Efectuar implantación sugerida por auditoría en informática
3.1 Inicio del proyecto
3.2 Tareas terminadas
3.3 Pendientes justificados
3.4 Pendientes implantados
3.5 Presentación de implantación
3.6 Implantación aprobada
4 Seguimiento a la implantación del plan recomendado por la auditoría
4.1 Acciones de seguimiento
4.2 Seguimiento de la implantación
4.3 Revisiones informales
4.4 Revisiones formales
4.5 Aseguramiento de calidad
4.6 Pendientes revisados
4.7 Pendientes aprobados
4.8 Seguimiento de pendientes
4.9 Implantación exitosa final
4.10 Implantación aprobada

CUARTA

Acuerdan las partes dejar sin efecto lo señalado en la cláusula segunda del contrato de prestación de servicios profesionales de auditoría en informática mencionado en la declaración I del presente addendum, respecto al alcance de la auditoría en informática

QUINTA

Convienen las partes de común acuerdo modificar el texto de la cláusula novena del contrato que se menciona

Figura 4.6. Ejemplo de addendum del contrato de auditoría en informática (Continua)

en la declaración I de este documento, de acuerdo a los siguientes términos

El auditor se obliga a terminar los trabajos señalados en la clausula segunda de este contrato en _____ días hábiles después de la fecha en que se firme el contrato y se ha cobrado el anticipo correspondiente. El tiempo estimado para la terminación de los trabajos está en relación a la oportunidad en que el cliente entregue los documentos requeridos por el auditor y por el cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin prejuicio alguno para el auditor

SEXTA

Acuerdan las partes dejar sin efecto lo señalado en la clausula novena del contrato de prestación de servicios profesionales de auditoría en informática mencionado en la declaración I del presente addendum, respecto al plazo de trabajo

SÉPTIMA

Convienen las partes de común acuerdo modificar el texto de la clausula décima del contrato que se menciona en la declaración I de este documento, de acuerdo a los siguientes términos

El cliente pagará al auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de _____ más el impuesto al valor agregado correspondiente. La forma de pago será la siguiente

a) _____% a la firma del contrato
b) _____% a los _____ días hábiles después de iniciados los trabajos
c) _____% a la terminación de los trabajos

OCTAVA

Acuerdan las partes dejar sin efecto lo señalado en la cláusula décima del contrato de prestación de servicios profesionales de auditoría en informática mencionado en la declaración I del presente addendum, respecto a los honorarios por los servicios profesionales de auditoría en informática

NOVENA

Las partes contratantes manifiestan que el presente documento no constituye novación alguna a lo estipulado en el instrumento jurídico descrito en la declaración I de este documento, salvo lo señalado en estricto en las cláusulas primera, tercera, quinta y septima del presente addendum

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad en original y tres copias, en la ciudad de _____, el día _____

_____ _____
EL CLIENTE EL AUDITOR

Figura 4.6. Ejemplo de addendum del contrato de auditoría en informática

4.6. ETAPA DE DESARROLLO

Por la importancia que tiene esta etapa y por ser el tema central de nuestra investigación, se decidió tratarla en el capítulo siguiente. En dicho capítulo se explicarán cada una de las tareas de ésta etapa, se mencionarán las actividades más importantes que llevará a cabo el auditor en informática y los productos terminados mínimos que se deben obtener al finalizar cada una de ellas y se incluirán los programas de trabajo por cada área susceptible de revisión.

4.7. ETAPA DE IMPLANTACIÓN Y SEGUIMIENTO

Esta fase abarca:

1. Definición de requerimientos para el éxito de la etapa de implantación
2. Desarrollo del plan de implantación.
3. Implantación de las acciones sugeridas por la auditoría en informática
4. Seguimiento de la implantación

La presente etapa es la más importante para todos los involucrados en el proyecto de auditoría en informática que, por decirlo de alguna manera, termina para los auditores y empieza para los responsables de las áreas usuarias y de informática, ya que ellos ejecutarán las acciones recomendadas en los informes de la alta dirección y detallado aprobados en la etapa anterior. La función del auditor en informática pasa a ser de seguimiento y apoyo.

Cada tarea de la etapa de implantación se explicará a continuación de una manera uniforme para hacerlas mas prácticas, asimismo, se mencionaran las actividades más importantes que llevará a cabo el auditor en informática y los productos terminados mínimos que se deben obtener al finalizar cada una.

Definición de requerimientos para el éxito de la etapa de implantación y desarrollo del plan de implantación

Estas tareas son ejecutadas por el responsable de informática; de ser necesario involucra a los usuarios y auditores en informática

Actividades principales:

- Analizar qué recursos humanos (asesores internos o externos), materiales (tecnología), financieros (inversiones), etc., se necesitan para ejecutar las acciones recomendadas en los plazos determinados por auditoría en informática
- Documentar dichos requerimientos y, de ser necesario, pedir la aprobación de la alta dirección
- Verificar que se cuente con los recursos estimados en la tarea anterior
- Consultar los informes para verificar acciones y tiempos de terminación
- Elaborar un plan de implantación que tenga al menos
    - Tareas
    - Productos terminados
    - Responsables
    - Involucrados
    - Fechas de inicio y término
    - Fechas de revisión

Productos terminados:

- Requerimientos de implantación documentados
- Requerimientos aprobados por la alta dirección
- Plan de implantación documentado

En la cuadro 4.7 se muestra un formato del plan de implantación, mismo que puede ser modificado según las necesidades del auditor y de la empresa que se esté auditando.

Cuadro 4.7. Plan detallado de implantación

TAREAS	PRODUCTOS TERMINADOS	RESPONSABLES	INVOLUCRADOS	FECHAS DE INICIO	FECHA DE TÉRMINO	FECHAS DE REVISIÓN

En la figura 4.7 se muestra un formato que contiene los elementos generales que se deben considerar al obtener la aprobación formal del plan de implantación sugerido por auditoría en informática.

Implantación de las acciones sugeridas por la auditoría en informática

La lleva a cabo el responsable de informática, aunque puede involucrar a los usuarios y auditores en informática.

Actividades principales:

- Verificar tareas, productos terminados, etc., del plan de implantación
- Ejecutar cada una de las tareas de acuerdo con el plan de implantación

Productos terminados:

- Plan de implantación ejecutado

Seguimiento de la implantación

Esta tarea corresponde al auditor en informática.

Actividades principales:

- Solicitar el plan de implantación para revisar su congruencia con los informes de la auditoría en informática
- Comprobar el cumplimiento formal de las tareas en los tiempos y formas que considere convenientes para asegurar los resultados esperados por él y la alta dirección
- Documentar debilidades y anomalías relevantes en la implantación
- Sugerir acciones para el cumplimiento de la implantación al nivel que considere pertinente

Productos terminados:

- Seguimiento del plan de implantación
- Anomalías y debilidades de implantación registradas y comentadas con el responsable de informática o la alta dirección
- Implantación de las acciones recomendadas por la función de auditoría en informática

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE SERVICIOS DE CÓMPUTO ACADÉMICO

APROBACIÓN DEL PLAN DE IMPLANTACIÓN SUGERIDO POR AUDITORIA EN INFORMATICA

México, D.F., **a 15 de junio de 1997.**

POR MEDIO DEL PRESENTE DOCUMENTO SE HACE CONSTAR QUE EN REUNION PACTADA EL DIA 15 **DE JUNIO DE 1997** A LA CUAL ASISTIERON LAS PERSONAS QUE POSTERIORMENTE **SE ENUNCIARAN, SE** DECIDIO QUE ES FACTIBLE Y CONVENIENTE PARA LA DIRECCIÓN GENERAL DE **SERVICIOS DE CÓMPUTO ACADEMICO**, LA APROBACIÓN DEL PLAN DE IMPLANTACION SUGERIDO **POR AUDITORÍA EN** INFORMÁTICA

L.I. CECILIA CALDERÓN ORTEGA
DIRECTOR GENERAL

L.A. EMILIANO RICO NIETO
JEFE DE UNIDAD ADMINISTRATIVA

L.I. **ALEJANDRO** ORTEGA ZARATE
USUARIO CLAVE

L.I. MIRIAM PRECIADO VIDALS
RESPONSABLE DEL ÁREA DE INFORMÁTICA

L.C. **DEYANIRA** FLORES FLORES
RESPONSABLE DE AUDITORÍA EN INFORMÁTICA

L.I. MIGUEL GARCÍA URBANO
COORD. DE AUDITORÍA EN INFORMÁTICA

Figura 4.7. Formato que contiene los elementos generales considerados en la aprobación formal del plan de implantación sugerido por auditoría en informática

La participación del responsable de informática es más directa, pues tendrá la responsabilidad de coordinar a su personal, a los usuarios y quizás a los asesores externos para una implantación exitosa. Sus objetivos principales serán:

- Asegurar que las recomendaciones y plazos de terminación surgidos de los informes de auditoría en informática y aprobados por la alta dirección se lleven a cabo de manera formal y oportuna
- Utilizar los recursos necesarios para lograr una implantación exitosa
- Respetar y cumplir las políticas y procedimientos de seguridad y control emanados de los informes de auditoría en informática
- Otros que el responsable de informática considere oportunos y convenientes para una implantación eficiente

El auditor en informática tendrá una participación más discreta e indirecta en la etapa de implantación; sin embargo, es fundamental, ya que debe garantizar que se pongan en práctica las acciones de mejoramiento que ha sugerido y en los plazos definidos

CAPÍTULO 5

Etapa de Desarrollo de la Auditoría en Informática

5.1. ETAPA DE DESARROLLO DE LA AUDITORÍA EN INFORMÁTICA

5.2. PROGRAMAS DE TRABAJO DE AUDITORÍA EN INFORMÁTICA

5.1. ETAPA DE DESARROLLO DE LA AUDITORÍA EN INFORMÁTICA

Es la etapa más importante para el auditor en informática porque ejerce su función de manera práctica y empieza a ejecutar las tareas de su trabajo de acuerdo con el plan aprobado en la etapa de formalización

Esta fase comprende

a) Concertacion de fechas de entrevistas, visitas y aplicación de cuestionarios
b) Verificación de tareas, involucrados y productos terminados
c) Clasificación de técnicas, herramientas, cuestionarios y entrevistas
d) Aplicación de entrevistas y cuestionarios
e) Visitas de verificación
f) Elaboración del informe preliminar correspondiente a los componentes por área auditada
g) Revisión del informe preliminar
h) Clasificación y documentación del informe preliminar
i) Finalización de tareas o productos terminados pendientes
j) Elaboración del informe final de la auditoría en informática
k) Presentación a la alta dirección y participantes clave
l) Aprobación del proyecto y compromiso ejecutivo

Es importante señalar que a partir de la primera tarea que corresponde a la presente etapa, el auditor en informática debe conjuntar todo lo recomendado en los capítulos anteriores:

- Profesionalismo
- Ética personal
- Virtudes y habilidades personales
- Metodología de trabajo
- Técnicas
- Herramientas de productividad:
    - Microcomputadoras portátiles, procesadores de palabras, graficadores, bases de datos, software de auditoria, entre otros
- Experiencia profesional
- Otras propias de cualquier auditor en informática

La asimilación y puesta en practica de los aspectos anteriores tiene los siguientes objetivos en los proyectos:

- Proyectar seguridad y confianza en todos los involucrados del proyecto
- Verificar y dar seguimiento a las funciones de cada involucrado
- Detectar las áreas de oportunidad no visualizadas con anterioridad
- Verificar debilidades e inexistencias relativas al control y seguridad
- Impulsar la motivación y cumplimiento de políticas y procedimientos relativos al control y seguridad en informática de manera permanente
- Otros originados por el desarrollo profesional de la auditoría en informática

Las actividades más importantes del auditor en informática en la etapa de desarrollo son las siguientes:

- Ejecutar las tareas de acuerdo con la secuencia establecida en el plan detallado de auditoría en informática
- Respetar el proceso metodológico
- Coordinar los recursos humanos con eficiencia para el cumplimiento oportuno del proyecto

- Orientar los recursos humanos, tecnológicos y financieros hacia resultados que brinden soluciones factibles y de valor agregado
- Otros considerados por el coordinador de auditoría en informática conforme las características de la empresa y la función de informática
- Documentar los datos relevantes de cada entrevista, visita o cuestionario relativos a debilidades o falta de políticas y procedimientos de control y seguridad inherentes a cada área de revisión y sus componentes
- Elaborar informes de alta calidad con la documentación requerida
- Otros que crea pertinentes la función de auditoría en informática de acuerdo con la empresa y las características propias de informática

A fin de tener un producto final de calidad y beneficios tangibles para la empresa al final de la etapa de desarrollo, al momento de revisar las áreas requeridas el auditor en informática deberá realizar las siguientes acciones:

- Basarse en el plan de auditoría en informática elaborado y aprobado en las etapas anteriores para la secuencia y duración de su trabajo en la presente etapa
- No interrumpir la continuidad de las operaciones de la empresa
- Utilizar técnicas y herramientas según lo demande cada tarea de la etapa actual
- Apoyar su trabajo con políticas y estándares comúnmente aceptados
- Involucrar a los usuarios y personal de informática según lo amerite cada tarea
- Usar los cuestionarios para cada área auditada
- Hacer entrevistas de manera profesional y adecuarlas al perfil de cada entrevistado
- Cuando se visiten los centros de cómputo y áreas de trabajo de los usuarios, se debe ser respetuoso de las políticas que imperan en ese medio
- Analizar con objetividad los escenarios emanados de la aplicación de cuestionarios, entrevistas y visitas realizados

Elaborar informes preliminares con la siguiente información:

- Áreas de oportunidad para mejorar de inmediato procesos de negocio apoyados en informática
- Observaciones (debilidades, carencias) de los aspectos de informática auditados
- Recomendaciones preliminares para cada una de las observaciones encontradas
- Responsables
- Actualización del plan de auditoría en informática
- Revisión detallada de los aspectos que tengan un impacto considerable en la operación del negocio o que soporten alguna estrategia de la empresa
- Comunicación abierta con los usuarios y el personal de informática involucrados
- Presentar un plan de implantación de auditoría en informática factible y realista que contemple los siguientes elementos:

  a) Debilidades o carencias de control, su problemática y causas que la originan
  b) Acciones inmediatas de corto y mediano plazo
  c) Responsables e involucrados en la implantación de estándares, políticas y procedimientos en cada componente de informática que así lo requiera
  d) Costo/beneficio del proyecto de implantación
  e) Aprobación formal de los directivos usuarios y del responsable de informática

Durante la etapa de desarrollo el auditor revisará áreas típicas de informática en algunos casos y en otros tendrá que enfrentarse a componentes más complejos y nuevos en el negocio; sin embargo, el seguimiento de la metodología, el uso de buenas técnicas, el respeto a los estándares comúnmente aceptados y el apoyo de la empresa lo llevarán al éxito.

Existen funciones o areas de informática tradicionalmente auditadas, debido al tiempo y arraigo que tienen en las empresas. Algunas de las areas más comunes son:

- Sistemas de información
- Planeación
- Desarrollo
- Operación o mantenimiento
- Metodología de desarrollo e implantación de sistemas de información
- Técnicas
- Herramientas
- Seguridad
- Planes de contingencia
- Planes de recuperación en casos de desastre
- Administración de la función de informática
- Planeación de informática
- Organización de informática
- Políticas y procedimientos de informática

Cada una de las tareas de la etapa de desarrollo se explica de manera uniforme para hacerla más práctica e inteligible en el cuadro 5.1.; se mencionan las actividades más importantes del auditor en informática y los productos terminados mínimos que se deben obtener al finalizar cada una de ellas.

Cuadro 5.1. Etapa de Desarrollo

TAREA	ACTIVIDADES PRINCIPALES	PRODUCTOS TERMINADOS
Concertar fechas tanto de entrevistas y visitas como de aplicación de cuestionarios Nota: las visitas se hacen con el objetivo de validar el uso de políticas y procedimientos de seguridad y control como el registro de acceso a centros de computo y areas donde existe documentación o tecnología importante para la empresa, existencia de extinguidores, detectores de humo, etc.; respaldos de información en cintotecas, equipos en buen estado, avisos de seguridad, etc	• Solicitar al responsable de informatica una lista con todos los nombres, puestos y departamentos del personal de informatica y de las areas usuarias involucradas en el proyecto • Hablar personal o telefónicamente con los involucrados para concertar citas	• Lista del personal de informatica y de usuarios • Fecha y hora formal de cada entrevista
Verificar tareas, involucrados y productos terminados	• Verificar si la tarea anterior altero el orden de las tareas mencionadas en el plan detallado • Asegurar que los cambios sean minimos y de bajo impacto en el plan • Documentar los cambios necesarios y justificarlos	• Cambios justificados • Cambios documentados
Clasificar tecnicas, herramientas, cuestionarios, entrevistas y otros	• Verificar la lista de metodos, tecnicas y herramientas sugeridas por area que será auditada • Verificar cuestionarios sugeridos a fin de asegurar que sean los requeridos para cada area que se auditara • Actualizar cuestionarios, de ser necesario • Documentar los cambios • Elaborar entrevistas con base en la experiencia, cuestionarios y necesidades del proyecto • Clasificar y documentar segun el proyecto	• Lista de metodos, tecnicas y herramientas clasificadas por área de revision • Cuestionarios actualizados y documentados de cada area • Entrevistas documentadas al personal de informatica y usuarios
Aplicacion de entrevistas y cuestionarios	• Efectuar cada una de las entrevistas en las fechas y horas planeadas • Aplicar cada uno de los cuestionarios en las fechas planeadas • Documentar las entrevistas y cuestionarios • Obtener el apoyo requerido (reportes, copias, documentos fuente, entre otros) • Registrar entrevistas y cuestionarios pendientes	• Entrevistas aplicadas y documentadas • Cuestionarios aplicados y documentados • Cancelaciones y causas documentadas • Documentacion de comentarios de apoyo relevantes para el proyecto
Efectuar visitas de verificación	• Validar objetivos e información buscada en cada visita • Efectuar las visitas a centros de computo o a los departamentos usuarios o de informatica • Notificar la visita a los responsables de dichos departamentos • Registrar la información mas relevante y obtener el soporte requerido (bitacoras por ejemplo) • Registrar pendientes	• Visitas de revision y verificación efectuadas • Documentación de los datos relevantes relacionados con debilidades o falta de control y seguridad • Registro de causas de visitas canceladas • Fechas de visitas pendientes aprobadas por los usuarios y personal de informatica responsables de los lugares por visitar

(Continua)

Cuadro 5.1. Etapa de Desarrollo

TAREA	ACTIVIDADES PRINCIPALES	PRODUCTOS TERMINADOS
Elaborar informe preliminar	• Analizar la información documentada que se origino de las entrevistas, visitas y aplicación de cuestionarios • Elaborar observaciones y conclusiones de cada uno de los componentes y áreas auditadas • Llenar la hoja de resumen de observaciones y recomendaciones de la auditoría en informática	• Hojas de resumen de observaciones y recomendaciones de la auditoría • Observaciones, conclusiones y recomendaciones por: - Componente - Área
Revisión del informe preliminar	• Verificar cada una de las observaciones y recomendaciones por componente y área • Registrar sugerencias para el mejor planteamiento de observaciones y recomendaciones • Asegurarse de tener por escrito todo el soporte requerido para hacer valida cada una de las observaciones (copias de reportes bitácoras, documentos fuente, minutas, memorandos, etc.) • Concertar citas con el responsable de informática y de los usuarios para dar un avance del proyecto y sus principales conclusiones y recomendaciones	• Observaciones conclusiones y recomendaciones verificadas y depuradas • Reunión informal de notificación de avance del proyecto con el responsable de informática y el responsable de los usuarios. • Compromiso de terminación de pendientes por medio de entrevistas, visitas o aplicación de cuestionarios
Clasificación y documentación del informe preliminar	• Registrar de manera formal cada observación, conclusión y recomendación sugerida, revisada y aprobada • Clasificar la información por componente y área auditada	• Observaciones, conclusiones y recomendaciones clasificadas y documentadas por: - Componente - Área
Finalizar tareas o productos pendientes	• Verificar lista de entrevistas, visitas y cuestionarios pendientes • Finalizar cada pendiente • Analizar la información emanada de cada entrevista, visita y cuestionario terminados • Elaborar observaciones y recomendaciones correspondientes • Actualizar, documentar y clasificar el informe de la auditoría en informática	• Entrevistas, visitas y cuestionarios terminados • Observaciones y recomendaciones clasificadas y documentadas en el informe de auditoría en informática por: - Componente - Área

Elaborar el informe final de la auditoría en informática	• Elaborar un informe orientado a la alta dirección
	• Redactar un informe detallado para el responsable de informática y los usuarios clave
	• Verificar que el informe contenga al menos:
	  ◦ antecedentes,
	  ◦ observaciones,
	  ◦ conclusiones,
	  ◦ recomendaciones,
	  ◦ responsables y tiempos por área auditada
		• Informe para la alta dirección
		• Informe detallado para:
		- Responsable de informática y usuarios clave

(Continúa)

Cuadro 5.1. Etapa de Desarrollo

TAREA	ACTIVIDADES PRINCIPALES	PRODUCTOS TERMINADOS
Presentacion a la alta direccion e involucrados clave	• Verificar que los informes sean claros, completos y congruentes entre si • Comprobar que se tenga el soporte de lo mencionado en los informes • Formalizar fecha de la presentacion de informes • Presentar los informes de la alta dirección • Elaborar una minuta	• Informes verificados • Informes finales • Informes presentados a la alta dirección e involucrados clave del proyecto (responsable de informática y responsable de los usuarios) • Minuta de la reunion
Aprobacion del proyecto y compromiso ejecutivo	• Obtener la aprobacion formal (documento) de la terminacion del proyecto de la auditoria en informatica • Obtener el compromiso formal (documento) de la alta direccion para la implantacion de los cursos de acción recomendados por la auditoria en informatica en los dos informes • Delegar en informática y las areas usuarias la implantación de las acciones recomendadas	• Aprobacion formal de la alta direccion de la terminacion del proyecto de la auditoria en informatica • Compromiso ejecutivo para brindar el apoyo requerido en la etapa de implantacion de todas las recomendaciones contempladas en los informes • Compromiso del responsable de informatica y de las areas usuarias para ejecutar la etapa de implantación

5.2. PROGRAMAS DE TRABAJO DE AUDITORÍA EN INFORMÁTICA

En esta sección presentamos los programas de trabajo que servirán de guía al auditor en informática para realizar su trabajo. Estos programas de trabajo están diseñados para la revisión de las siguientes áreas:

- Administración de informática
- Dirección y niveles ejecutivos
- Usuarios de informática
- Control interno
- Ciclo de desarrollo e implantación de sistemas de información
- Sistemas de información
- Mantenimiento
- Redes locales
- Telecomunicaciones
- Hardware
- Software
- Seguridad
- Planeación de informática
- Investigación tecnológica

Cabe señalar que estas áreas no son las únicas que se pueden revisar, sino que son una propuesta y pueden variar de acuerdo al criterio del auditor o a las necesidades de la empresa.

La presentación de los programas de trabajo la realizamos a manera de cuadros (5.2 al 5.14) para facilitar su entendimiento y utilización.

En dichos cuadros incluimos un apartado de identificación que contiene al auditor que desarrolló el programa de trabajo, quien lo supervisó y la empresa donde se aplicó; un título para identificar cada programa de trabajo de acuerdo al área de revisión; un objetivo general por cada área de revisión; objetivos particulares por área de revisión y los cuestionarios necesarios para su cumplimiento; apartados para comentarios, cédulas de referencia e involucrados.

Los cuestionarios incluidos en los programas de trabajo pueden variar de acuerdo al criterio del auditor o a las necesidades de la empresa.

Cuadro 5.2. Programa de trabajo del área de Administración de Informática

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

ADMINISTRACIÓN DE INFORMÁTICA

OBJETIVO: Conocer y verificar el nivel de administración de los recursos informáticos de la organización, a través de la revisión de la misión, funciones, organización, servicios y parámetros de medición del área.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Verificar que exista un uso eficiente de los recursos de informática (personal, tiempo, tecnología y dinero) 2 Asegurar que la función de informática cubra los mayores riesgos y exposiciones existentes en el medio informático 3 Asegurar que los recursos de informática (hardware, software, telecomunicaciones, servicios, personal, etc.) estén orientados hacia los objetivos y estrategias del negocio 4 Confirmar que exista • Elaboración y formalización de los planes de informática • Organización y control formal sobre los recursos de informática • Dirección, coordinación y control de los proyectos de informática 5 Comprobar la existencia de servicios de informática documentados y difundidos en el negocio	Misión y funciones de la informática 1 ¿Existe un documento formal que describa claramente los siguientes aspectos? • Misión de la informática en el negocio • Estructura organizacional de la función • Funciones y actividades por cada puesto existente en el organigrama • Funciones y actividades por cada puesto existente en el organigrama • Políticas y procedimientos de informática • Otros 1.1 Si no hay tal documento, ¿Cuál ha sido la causa o motivo para no hacerlo formalmente (en documento)? 2 En caso de que exista dicho registro, ¿fue comentado con las áreas internas de informática, áreas usuarias y la alta dirección? 3 Si es así, ¿Qué procedimiento se utilizó? • Juntas • Vía memorandos, circulares, etcétera • Publicado en una reunión informal • Inducción al momento de que el personal de informática ingresa al negocio • Otros			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
6 Asegurar que existen parámetros de medición para el desempeño de cada una de las funciones de informática 7 Verificar que se lleve a cabo de manera formal la evaluación del desempeño 8 Asegurar la existencia de un comité de informática, alta dirección y usuarios clave 9 Confirmar la presencia de un apoyo formal a informática de parte de la alta dirección 10 Asegurar que informática elabore, formalice difunda y aplique las políticas y procedimientos relativos a informática de manera permanente 11 Verificar que existan metodologías, técnicas y herramientas para cada función 12 Comprobar que haya un proceso formal de capacitación y actualización del personal 13 Detectar el grado de confianza, satisfacción y respaldo que brinda al negocio la función de informática 14 Confirmar que los planes y políticas de informática sean difundidos y conocidos por la alta dirección	4 ¿Fue aprobado por la alta dirección? 5 ¿Está consciente el personal de informática de la importancia de orientar los esfuerzos al cumplimiento formal y oportuno de la misión, objetivos, estrategias, políticas y procedimientos de la función de informática 6 ¿Se encuentran bien establecidas y entendidas las funciones de informática en la organización? 6.1 ¿Cuáles son desde un punto de vista objetivo y práctico? 6.2 ¿Las funciones ejecutadas en la actualidad son las requeridas por el negocio? 6.3 En caso de que se deban actualizar o complementar, ¿Cómo las desarrollaría para un apoyo más significativo al negocio? 7 ¿Existe un comité de informática? 7.1 ¿Quiénes lo integran? 7.2 ¿Cuáles son los objetivos y funciones principales del comité? Organización 1 ¿Hay una estructura formal de informática (manual, documento, etc.) que contemple al menos lo siguiente? • Organigrama • Descripción de objetivos, funciones, responsabilidades, y métodos de trabajo por cada puesto existente en el organigrama • Flujos de información entre los diferentes niveles y áreas de informática • Otros aspectos organizacionales 1.1 Si existe dicho manual o documento, indique cuáles fueron los criterios o procedimientos utilizados para su • Definición y elaboración			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
15 Evaluar el grado de compromiso de la alta dirección con informática para establecer si el apoyo que le brinda es el adecuado	• Difusión y asimilación por el personal de informática • Autorización por parte del responsable de informática 1.2 ¿Que procedimiento utiliza para asegurarse de que todos los elementos señalados en dicho documento sean actualizados y autorizados formal y oportunamente de acuerdo con las necesidades del negocio? 2 ¿En el último año se han presentado cambios a nivel organizacional que afecten de manera significativa el desarrollo eficiente de las actividades de la función de informática? 2.1. Si es así ¿Qué aspectos de la función han sufrido el impacto de dichos cambios? 3 ¿El responsable de informática o la alta dirección tienen planeado algún cambio significativo en la estructura de informática para los próximos doce meses? 3.1 Si es así ¿Qué elementos de la organización de informática se verán afectados? 4 ¿Qué procedimientos se llevan a cabo para minimizar el riesgo de generar hechos negativos de la función de informática derivados de cambios organizacionales o fusiones con otras empresas? 4.1. ¿Cuáles de los siguientes factores negativos se presentan en la función de informática? • Improductividad • Falta de motivación • Áreas de informática desintegradas • Individuos reactivos y no proactivos • Falta de planeación estratégica en informática • Bajos sueldos • Imagen negativa en el negocio • Otros 4.2 ¿Cuáles considera que sean las causas de cada uno y cómo piensa solucionarlos? 5 ¿Existe un proceso formal de comunicación interna entre el personal de informática? 5.1 ¿Cuál es el sistema? 5.2 ¿Cuáles son las barreras obstáculos principales de comunicación entre los diferentes niveles y funciones de la función de informática y cómo piensa solucionarlos? 6 ¿Qué tipo de estructura existe jerárquica, lineal o de red? 6.1 ¿Por qué se decidió que era la más adecuada? 6.2 ¿No se crean cuellos de botella para la toma de decisiones debido a la estructura actual?			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	6.3 ¿Considera que la estructura actual limita la iniciativa, creatividad y superación profesional de cada uno de los integrantes de su función? ¿Porqué? 6.4 ¿Existen algunas comparaciones con estructuras de empresas similares a nivel local, nacional o internacional para la definición y actualización de organización? ¿Por que? 7 ¿En la organización hay áreas usuarias que desempeñen funciones correspondientes a la función de informática? 7.1 Si es así, ¿Cuáles son y que acciones se toman al respecto? 8 Anote los factores básicos para el logro de una administración eficiente de la función de informática 8.1 ¿Qué acciones ejecuta para llevar a buen término cada uno de esos factores? 9 ¿Que actividades realiza para asegurar cada uno de los siguientes aspectos administrativos? • Organización • Planeación • Dirección • Control 9.1 ¿Cuáles son ejecutadas de manera informal? ¿Porqué? ¿Cómo piensa eliminar esa deficiencia y en cuánto tiempo? Servicios 1 ¿Existe un catalogo de servicios de informática? 1.1 ¿Es congruente con las áreas de la función de informática? 1.2 Si no existe, ¿Cómo se enteran los usuarios y la alta dirección de los servicios disponibles? 2 ¿Que procedimiento se llevó a cabo para elaborarlo? 2.1 ¿Quiénes fueron los responsables? 2.1 ¿Esta documentado? 2.3 ¿Se describen los objetivos, alcances, productos terminados, responsables y beneficios de cada uno de los servicios que proporciona informática? 3 ¿Se presentó a la alta dirección para su aprobación? 3.1 ¿Fue aprobado formalmente? 3.2 ¿Cómo se difunden los servicios o funciones de informática través de la organización?			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4 ¿Cuál es el procedimiento para la solicitud de servicios de informática? 4.1 ¿Cómo se asegura el cumplimiento oportuno de los servicios solicitados? 5 ¿Cuál es el procedimiento para la recuperación de costos emanados de cada servicio? 5.1 Cuando los servicios son ejecutados por terceros (asesores). ¿Es el mismo procedimiento? 5.2 Si no es así, ¿Cómo se lleva a cabo la recuperación de costos? 5.3 ¿La función de informática es vista en la organización como un área que debe producir ganancias o es sólo una prestadora de servicios que recupera costos originados por cada servicio? 5.4 Cuando los gastos son originados por actividades internas (capacitación, equipos de cómputo, adquisición de metodologías, etc.) ¿Cómo se recuperan los mismos? 6 ¿Existe un procedimiento definido formalmente para los puntos siguientes? • Actualización del catálogo • Eliminación de algún servicio • Agregar un nuevo servicio • Modificar objetivos, alcances, productos terminados, costos, etcétera • Documentación de los cambios al catálogo • Revisión de los cambios • Autorización de los cambios • Difusión del catálogo de servicios de informática en el negocio. 7 Cuando existen servicios de informática proporcionados por terceros con un alcance periódico y estratégico en el negocio (planeación de informática, desarrollo de sistemas, asesoría al personal usuario, alta dirección o informática, etc.). ¿Se integran al catálogo de servicios? 7.1 Si es así, ¿Se reflejan los datos que contienen los otros servicios del catálogo proporcionados por el personal de informática del negocio?			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Parámetros de medición 1 ¿ Se tiene un procedimiento formal de seguimiento al desempeño y rendimiento del personal de informática? 1.1 Indique si dicho procedimiento al menos contempla los siguientes puntos • Parámetros de medición por puesto • Parámetros de medición para cada una de las funciones o actividades primordiales de cada puesto • Objetivos y alcances de cada puesto • Resultados esperados por cada puesto • Tiempos esperados para la ejecución formal de cada función o actividad fundamental • Actividades de control y seguimiento requeridas para cada función (revisiones formales e informales, verificación del cumplimiento de estándares, aseguramiento de calidad, etcétera) • Responsables de dar seguimiento de cada puesto • Encuestas a usuarios al final de cada proyecto 1.2 ¿Se documenta formalmente dicho procedimiento? 1.3 ¿Quiénes son los responsables de elaborar, autorizar difundir y actualizar dicho documento? 1.4 ¿El procedimiento actual fue aprobado por el responsable de la función de informática? 1.5 Si no es así ¿Como se asegura su entendimiento, cumplimiento y actualización conforme necesidades específicas del negocio y del medio informático? 2 ¿Existen fechas predefinidas para la aplicación de los parámetros de medición o éstos se aplican durante el desarrollo de cada proyecto? 2.1 ¿Se apoyan en asesores externos para la elaboración y aplicación de los parámetros de medición del desempeño de la función de informática?. 2.2 ¿Se dan a conocer al personal de informática los resultados de las evaluaciones de desempeño, así como los parámetros con que se mide su función? ¿Por qué? 3 ¿Las funciones de controlar y ejecutar están divididas? 4 Cuando los servicios de informática son ejecutados por personal externo, ¿Se someten a los parámetros de medición definidos en la primera pregunta? 4.1 De no ser así, ¿Por qué no se mide su desempeño y calidad de trabajo?			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CEDULA DE REF.	INVOLUCRADOS
	5 ¿Existe privacidad en los resultados obtenidos de cada evaluación de desempeño? 6 ¿El personal de informática participa directamente en el proceso de evaluación de su desempeño o sólo se le notifican los resultados de dicha evaluación? 6.1 Cuando no existe un proceso formal de evaluación de desempeño, ¿Cómo se justifica a los empleados el aumento de sueldos, ascensos, o en su caso contrario, su despido de la empresa o la falta de incremento salarial por periodos largos? 7 ¿El procedimiento actual de evaluación y seguimiento que se da al desempeño de las funciones es apropiado? 7.1 Si no lo es, ¿Dónde radican las principales debilidades? • En los parámetros de medición • En el cumplimiento de los objetivos, alcances, estándares, etc., de cada puesto • En la supervisión y seguimiento de cada puesto en el transcurso de los proyectos o ejecución de los servicios de informática • En la evaluación final específica para cada función. • Otros 7.2 ¿Qué acciones piensa poner en práctica para eliminar las debilidades encontradas? 8 ¿Existe un análisis costo/beneficio (anual) de la función de informática? 8.1 Si lo hay, ¿Quién lo elabora y quién lo revisa? 8.2 ¿Cómo se han comportado las estimaciones de inversión y gastos en los últimos años? 9 ¿La dirección considera que el apoyo de informática es pobre ¿Por qué? 10 ¿Existen políticas formales en la alta dirección relativas a la administración y organización de la función de informática? 10.1 Si es así, ¿Quién las formuló? 10.2 ¿Quién las aprobó? 10.2 ¿Quién las aplicó? 10.3 ¿Quien las conoce en la organización? 10.4 ¿Cómo se dieron a conocer? 10.5 ¿Las conoce el encargado de informática? 10.6 ¿Las acepta todo el personal de informática? 10.7 ¿Se actualizan formalmente cuando es necesario? 10.8 ¿Se emplantan con éxito?			

(Continúa)

Cuadro 5.2. Programa de trabajo del área de Administración en Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	11 ¿Las políticas están definidas para cada área o función de informática? 12 ¿Definen la pauta en el manejo de proyectos? • Evaluación y adquisición de hardware y software • Renta de equipo • Telecomunicaciones • Reclutamiento y Capacitación • Desarrollo de sistemas • Otros 13 ¿Existen reportes de desempeño que apoyen la medición de las funciones? 13.1 ¿Están orientados a obtener los siguientes parámetros de medición? • Productividad y calidad de los proyectos • Resultados • Avances de los proyectos • Áreas susceptibles de control y seguimiento • Seguimiento individual y de grupo 14 Elaborar cédula de observaciones con las siguientes columnas: • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda.

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

DIRECCIÓN Y NIVELES EJECUTIVOS

OBJETIVO: Conocer y verificar el grado de comunicación y apoyo que tiene la alta dirección hacia el área de informática y el apoyo que brinda ésta al negocio y a la toma de decisiones.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1. Detectar el grado de confianza, satisfacción y respaldo que brinda la función de informática al negocio 2. Verificar que las bondades y limitaciones de cada uno de los sistemas de información sean percibidos conceptualmente por la alta dirección y que este entendimiento sea congruente con la realidad 3. Confirmar que exista una clasificación y entendimiento de los servicios de informática para la alta dirección 4. Comprobar que la tecnología de informática (hardware, software, comunicaciones, etc.) se encuentre al alcance de los niveles directivos de una manera amigable y productiva 5. Asegurar que la alta dirección tenga los sistemas de información, los servicios y la tecnología de informática que requiere para la toma de decisiones, el mejoramiento de las actividades de sus funciones, la obtención de un valor agregado por el uso de informática, etcétera	Seguimiento a la función de informática 1. ¿De qué dirección o gerencia depende la función de informática? 2. ¿Existen parámetros de medición de la función de informática (costos de informática vs. Ventas, beneficios reales contra esperados, etc.)? 2.1 ¿De qué manera utiliza la dirección esos parámetros de medición? 2.2 ¿La frecuencia de aplicación de esos parámetros es por proyecto terminado o por periodos? 2.3 ¿Se apoyan en asesores externos para la elaboración y aplicación de los parámetros de medición del desempeño de la función de informática? 2.4 ¿Se dan a conocer al responsable de informática los resultados de las evaluaciones de desempeño, así como los parámetros con que se mide su función? ¿Por qué? 3. ¿La estructura organizacional contempla de manera formal la posición de informática dentro de la empresa, negocio u organización? 4. ¿Con base en qué criterios se ubicó a informática en esa posición? 5. ¿Son suficientes o necesarias para la dirección las funciones existentes? 6. ¿Las funciones de control y ejecución están divididas? 7. ¿Existe una descripción de puestos? 8. ¿Las funciones son congruentes con la estructura organizacional?			

(Continúa)

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
6 Verificar que exista un análisis costo/beneficio de la función de informática dentro del negocio 7 Comprobar que los planes y políticas de informática sean difundidas y conocidas por la alta dirección 8 Evaluar el grado de compromiso de la alta dirección con informática para establecer si el apoyo que le brinda es el adecuado o es limitado	9 ¿Cómo se evalúa el desempeño de esas funciones? 9.1 ¿Los objetivos, funciones y actividades de la función de informática son realistas y congruentes con las necesidades de la organización? 9.2 ¿Los salarios corresponden a las funciones del personal de informática (tomando como referencia la responsabilidad y alcance del puesto, sueldos de los niveles similares en la organización, sueldos promedio del mercado en funciones y alcances similares)? 10 ¿La dirección aprueba los planes y avances de los proyectos de informática? 11 Mencione si el personal de informática participa en todos los proyectos relacionados con • Evaluación y adquisición de hardware, software y aplicaciones • Definición de estrategias tecnológicas • Contratación de asesores externos 12 ¿Existe privacidad en los acuerdos de la alta dirección e informática? 12.1 ¿La comunicación entre ellos es formal (juntas, memorandos, etc.)? 12.2 ¿La alta dirección considera al encargado de informática en la toma de decisiones? 13 ¿Es complicado administrar y supervisar la función de informática? 14 ¿Existe un análisis costo/ beneficio (anual) de la función de informática? 15 ¿Quién lo elabora y quién lo revisa? 16 ¿Cómo se han comportado las estimaciones de inversión y gastos en los últimos años? 17. ¿La dirección considera que el apoyo de informática es pobre? 18 ¿Existen políticas formales en la alta dirección relativas a la administración y organización de la función de informática? 18.1 Si es así, ¿quién la formuló? 18.2 ¿Quién las aprobó? 18.3 ¿Quién las conoce en la organización? 18.4 ¿Cómo se dieron a conocer? 18.5 ¿Las conoce el encargado de informática? 18.6 ¿Las acepta todo el personal de informática? 18.7 ¿Se actualizan formalmente cuando es necesario? 18.8 ¿Se llevan a la práctica con éxito? 19 ¿Las políticas se definen para cada área o función de informática?			

(Continúa)

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	20 ¿Establecen la pauta en el manejo de proyectos los siguientes puntos? • Evaluación y adquisición de hardware • Renta de equipo • Telecomunicaciones • Reclutamiento y capacitación • Desarrollo de sistemas • Otros Comunicación e Integración 1 ¿La alta dirección y los niveles ejecutivos conocen la misión de informática en la empresa? 2 ¿Están al tanto de las funciones de informática en la empresa? 3 ¿El área de informática notificó formalmente los conceptos anteriores a la alta dirección? 3.1 ¿Están por escrito? 3.2 ¿Cómo los han difundido (reuniones entre la alta dirección e informática, entre otros)? 3.3 ¿Fueron aprobados formalmente? 4 ¿Existe un compromiso formal por parte de la alta dirección para brindar el apoyo necesario a la función de informática en el cumplimiento oportuno y satisfactorio de sus responsabilidades? 4.1 Si es así, ¿En que forma se da este compromiso? 4.2 ¿Existe un comité integrado por la dirección e informática? 4.3 ¿Se reúnen periódica y formalmente? 4.4 ¿Cuáles son las funciones de dicho comité? 5 Si no hay comité, ¿quien se responsabiliza de la función de informática por parte de la alta dirección? 6 ¿El nivel del encargado de la función de informática le proporciona suficiente autoridad y proyección en la organización? ¿Lo reconocen los usuarios? 7 ¿Están formalizados estos aspectos? 8 ¿La alta dirección conoce las funciones y responsabilidades de los puestos clave (gerencias, jefaturas) del personal de informática? 9 ¿Cómo difunde la alta dirección la funciones y responsabilidades de informática a través de la organización? 10 ¿Existen sugerencias que considere la alta dirección que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la función de informática?			

(Continúa)

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	11 ¿Existen sugerencias para la alta dirección que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la organización por medio de los servicios de informática? 12 ¿Cómo considera el nivel de comunicación entre dirección e informática actualmente? ¿Por qué? 13 ¿De qué manera se asegura que los compromisos, planes, aprobaciones o cancelaciones de proyectos requieren el visto bueno de la alta dirección? 14 ¿Cómo se aseguran de que tanto apoyo y seguimiento como aprobación de la alta dirección a los proyectos de informática sean oportunos y formales? 15 ¿Se cuenta con la planeación estratégica de informática? 15 1 Si es así • ¿Quién la elaboró (participó el usuario)? • ¿Quién la evaluó y aprobó? • ¿Es a dos, tres, cuatro o cinco años? 16 ¿El plan estratégico se difundió a todos los niveles ejecutivos de la organización? 17 ¿La alta dirección toma en cuenta la planeación? 18 ¿Se entienden los objetivos y alcances del plan? 19 ¿La alta dirección sabe en qué etapa de avance se encuentra esta planeación? Apoyo a la toma de decisiones 1 ¿Se tiene conciencia en toda la organización de que la función de informática es primordialmente proporcionar un servicio estratégico a las áreas de la empresa? 2 ¿Se definieron los productos y servicios con base en las prioridades de la empresa o en las prioridades de una de las áreas de la empresa? 3 ¿Quiénes participaron en la definición, formalización, aprobación y distribución de los productos y servicios de la función de informática dentro de la empresa? 4 ¿La alta dirección considera que los productos y servicios de informática son estratégicos? 4 1 ¿Informática ha brindado beneficios palpables a la empresa (en ventas, producción, administración etc.)?			

(Continúa)

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CEDULA DE REF.	INVOLUCRADOS

	4.2 ¿Se pueden cuantificar los costos/ beneficios de informática (por ejemplo de los últimos tres años)?
	• Costos en
	  • Tecnología (hardware, comunicaciones, EDI, entre otros)
	  • Software (como paqueles administrativos, sistemas operativos)
	  • Sistemas de información
	  • Personal
	  • Asesoría externa
	  • Otros
	• Beneficios en
	  • Sistemas de nivel ejecutivo
	  • Sistemas integrales
	  • Aumento en ventas (sistema comercial)
	  • Automatización de procesos
	  • Administración de personal(nómina y sistemas organizacionales)
	  • Productividad y calidad
	  • Disminución de costos
	  • Otros
	5 ¿La alta dirección considera que informática sólo apoya las funciones operativas?
	5.1 ¿Es una función que trabaja para las jefaturas?
	5.2 ¿Brinda apoyo a la toma de decisiones?
	6 ¿Justifica el costo (solicitar análisis costo/beneficio)?
	7 ¿A qué plazos se proyectaron los productos y servicios de informática (corto, mediano y largo plazo)?
	8 ¿Utilizan productos o servicios de asesores externos?
	9 ¿Apoyan éstos las estrategias de la empresa?
	10 ¿Los aprobó la alta dirección?
	11 ¿Justifican el costo (solicitar análisis costo/beneficio)?
	12 ¿La función de informática de la organización no puede proporcionar éstos productos y servicios?
	13 ¿Quién monitorea los servicios externos de sistemas?
	14 ¿Los sistemas de información son los apropiados para la empresa?
	14.1 ¿Son oportunos?
	14.2 Tienen los controles adecuados en cuanto
	  • Privacidad, actualización, autorización, totalidad y mantenimiento			

(Continúa)

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	14 3 ¿Existe un grado aceptable de automatización en los procesos de la organización? 14 4 ¿Qué tipo de proceso (manual o automatizado) maneja mayores volúmenes? 14 5 ¿Cuál es la causa principal de que los procesos manuales no se hayan automatizado? 14 6 ¿Se han pensado automatizar los procesos manuales en un futuro próximo? • Si no es así, ¿por qué? 14 7 ¿Se ha solicitado la automatización formalmente? 15 ¿Se tienen problemas económicos, organizacionales y de otro tipo por el uso actual de informática? 16 ¿Se ha pensado prescindir de este servicio en menor medida y utilizar más los servicios externos? 17 Si el servicio es bueno, ¿se ha pensado en extender o ampliar los servicios en toda la organización? 18 Desde su punto de vista, ¿hay descontento en la empresa por los servicios que brinda informática? 19 ¿Cuál ha sido el apoyo o soporte que brinda la alta dirección a informática? 20 ¿Se involucra la alta dirección en soluciones que requiere implantar informática? 21 ¿La empresa ha brindado las facilidades económicas y tecnológicas que requiere informática? 22 Entre las estrategias de la empresa ¿está incluido el soporte a la función de informática? 23 ¿Cómo se evalúan los productos y servicios de la función informática? ¿Cómo se van a evaluar en el futuro? 24 ¿Tienen una propuesta formal de productos y servicios para los próximos años por parte de informática? 25 ¿Los sistemas de información apoyan estratégicamente los principales procesos de la empresa (producción, ventas, administración, otros)? 26 Desde su punto de vista, ¿los sistemas son flexibles y se adaptan a los cambios que requiere la empresa? ¿Su tiempo de adaptación es lento? 27 ¿Qué niveles de análisis utilizan para identificar los procesos y flujos de información relevantes de la organización? 28 ¿Se hizo un análisis costo/beneficio del plan?			

(Continúa)

Cuadro 5.3. Programa de trabajo del área de Dirección y Niveles Ejecutivos

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	29 ¿Está satisfecha la dirección con los resultados de la ejecución del plan? 30 ¿Hay requerimientos o prioridades definidos en el plan como urgentes que no haya satisfecho la función de informática? 31 Si es así, ¿esto ha afectado las estrategias de la organización? 32 ¿Quien definió las prioridades y requerimientos de los usuarios? 33 ¿Quien estableció las prioridades para la secuencia de los proyectos dentro del plan? 34 ¿El proceso de planeación fue un proceso dinámico y benéfico desde su punto de vista? ¿Por qué? • ¿Qué sugerencias tiene al respecto? 35 Elaborar cédula de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

USUARIOS DE INFORMÁTICA

OBJETIVO: Conocer y verificar el grado de satisfacción que tienen los usuarios ante los servicios de informática en la organización

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Detectar el grado de confianza, satisfacción y respaldo que perciben los usuarios de parte de la función de informática 2 Detectar el soporte real que brinda la función de informática a los diferentes departamentos usuarios del negocio 3 Verificar que las bondades y limitaciones de cada uno de los sistemas de información sean percibidas claramente por los usuarios y que este entendimiento sea congruente con la realidad 4 El auditor ha de definir la calidad oportunidad y confiabilidad real de cada sistema de información, mismas que validarán los responsables de informática y los usuarios 5 Estudiar el grado de involucramiento de los usuarios en proyectos específicos como desarrollo de sistemas, evaluación y adquisición de paquetes que serán utilizados por los mismos usuarios, etcétera 6 Asegurar que existen parámetros de medición para el desempeño de cada una de las funciones de informática	Comunicación e integración 1 ¿Las áreas usuarias conocen la misión de informática en la empresa? 2 ¿Saben cuáles son las funciones de informática en la empresa? 2.1 ¿Los usuarios están al tanto de los servicios y productos que proporciona informática? 3 ¿El área de informática ha difundido los conceptos anteriores de manera formal entre las áreas usuarias? 3.1 ¿Están por escrito? 3.2 ¿Cómo lo ha difundido, por ejemplo, reuniones con las áreas usuarias? 3.3 ¿Fueron aprobados formalmente? 4 ¿Hay un compromiso formal por parte de las áreas usuarias para cooperar en lo necesario con la función de informática en el cumplimiento oportuno y satisfactorio de las responsabilidades de esta última? 4.1 Si es así, ¿en qué forma se da este compromiso? 4.2 ¿Existe un comité integrado por los usuarios e informática? 4.3 ¿Se reúne periódica y formalmente? 4.4 ¿Cuáles son las funciones de dicho comité? 5 Si no hay comité, ¿Quién se responsabiliza de la función de informática por parte de las áreas usuarias? 6 ¿El nivel del encargado de la función de informática le proporciona suficiente autoridad y proyección en la organización? ¿Lo reconocen los usuarios?			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
7. Confirmar si existen procedimientos formales para el seguimiento de la comunicación entre los usuarios e informática 8. Comprobar si se cuenta con un comité formal integrado por representantes de informática y de los departamentos usuarios 9. Detectar áreas de oportunidad donde el usuario requiera el apoyo de la función de informática 10. Confirmar la presencia de un análisis costo/beneficio de los diferentes productos y servicios que brinda informática a los usuarios 11. Constatar que los planes y políticas de informática sean difundidos y conocidos por las áreas usuarias 12. Evaluar el grado de compromiso de las áreas usuarias hacia el comité de usuarios e informática (si existe)	7 ¿Están formalizados estos aspectos? 8 ¿Las áreas usuarias conocen las funciones y responsabilidades de los puestos clave (gerencias, jefaturas) del personal de informática? 9 ¿Cómo se informa a las áreas usuarias acerca de las funciones y responsabilidades de informática en la organización? 10 ¿Las áreas usuarias emiten sugerencias que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la función de informática? 10.1 Indique cómo se han expuesto hasta ahora las sugerencias para el mejoramiento de la comunicación e integración con la función de informática? • Por teléfono • En reuniones formales • Otros (especifique) 11 ¿Los usuarios han hecho sugerencias que puedan apoyar los objetivos estrategias, funciones y responsabilidades de la organización por medio de los servicios de la informática? 11.1 Mencione cómo se han expuesto hasta ahora las sugerencias para el mejoramiento de la comunicación e integración con la función de informática? • Por teléfono • En reuniones formales • Otros (especifique) 12 ¿Cómo considera el nivel de comunicación que existe entre ustedes e informática actualmente? 13 ¿De qué manera se aseguran de que los compromisos, planes, aprobaciones o cancelaciones de proyectos requieran el visto bueno de las áreas usuarias? 14 ¿Cómo se aseguran de que los compromisos de apoyo, seguimiento y aprobación a proyectos de informática para las áreas usuarias se lleven a cabo oportuna y formalmente? 15 ¿Se cuenta con la planeación estratégica de informática? 16 ¿Se difundió el plan estratégico entre todas las áreas usuarias de la organización? 17 ¿Las áreas usuarias cuentan con la documentación de la planeación? 18 ¿Se entienden los objetivos y alcances del plan?			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	19 ¿Las áreas usuarias cuentan con la documentación de la planeación (al menos de los proyectos en que se involucra como usuario)? 19.1 ¿Conoce cuáles son los proyectos a corto, mediano y largo plazo donde el usuario debía involucrarse? 19.2 ¿Informática ha explicado los conceptos anteriores a los usuarios? 19.4 ¿Cómo lo ha hecho? 19.5 ¿Fueron apoyados en términos formales? Proyectos conjuntos 1 ¿Existen proyectos en su área relacionados directa o indirectamente con la función de informática? 1.1 Si es así, mencione que tipo de proyectos serán o están siendo desarrollados en conjunto con informática • Captación (equipos de cómputo, software, aplicaciones, entre otros) • Implantación de sistemas de información • Desarrollo a la medida (customized). • Compra de un sistema desarrollado por externo • Legislación del software • Estandarización de tecnología • Elaboración de políticas y procedimientos. • Otros (especifique) 2 ¿Los usuarios y el personal de informática responsable de las tareas de dichos proyectos los planearon a nivel formal? 3 ¿Los proyectos mencionados en la pregunta 1.1 concuerdan con la planeación de informática y los planes de trabajo de las áreas usuarias? 4 Mencione si existe una función responsable de los planes conjuntos de usuarios e informática para las siguientes tareas • Elaboración, difusión, actualización, documentación y seguimiento de proyectos conjuntos 4.1 Si es así ¿Qué actividades básicas realiza para cada una de las tarea señaladas? 4.2 ¿Quién y de qué forma da seguimiento al cumplimiento oportuno y formal de tales tareas y actividades? 4.3 ¿Se registran las anomalías detectadas en dicho seguimiento?			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	5 ¿El proceso de planeación de proyectos conjuntos se efectuó por medio de los compromisos emanados del comité de informática? 5.1 Si no hay un comité de usuarios e informática, indique cómo se integró a los equipos de trabajo para • Definición de requerimientos • Detección de áreas de oportunidad • Definición de objetivos y alcances de proyectos conjuntos • Estimación de tareas, responsables y tiempo de cada proyecto • Análisis costo/beneficio • Otros aspectos relacionados con el proceso de planeación 6 En caso de que no existan planes formales para los proyectos conjuntos de usuarios e informática, indique cuáles son los medios utilizados para • Comunicación de requerimientos de las áreas usuarias • Proyectos propuestos para el incremento de la productividad en las áreas usuarias por parte de la función de informática • Acciones específicas de apoyo a las diferentes funciones y niveles de las áreas usuarias del negocio • Otros aspectos de integración de proyectos de los usuarios e informática 7 ¿En los últimos tres años ha participado formalmente en algunos de los proyectos de informática mencionados a continuación? • Desarrollo de la planeación de informática • Definición de objetivos requerimientos y estrategias del negocio • Definición de la situación tecnológica actual • Definición de la tecnología propuesta • Definición de la planeación final de informática • Desarrollo, compra o adecuación de algún sistema de información • Definición del alcance del proyecto • Análisis y especificación de requerimientos • Diseño • Generación de códigos y pruebas modulares del sistema • Pruebas de aceptación del sistema • Liberación del sistema • Revisión de posimplantación • Proyectos de capacitación en el uso y aprovechamiento de los recursos de informática			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS

	• Proyectos de investigación
	• Evaluación y adquisición de hardware y software
	  • Definición de requerimientos
	  • Evaluación de las propuestas de los proveedores
	  • Selección y aprobación de la propuesta apropiada
	  • Pruebas
	  • Aprobación de la implantación
	• Desarrollo de planes de contingencia y recuperación
	  • Definición
	  • Aprobación
	  • Difusión
	  • Simulacros para probarlos
	  • Actualización
	• Auditorías en informática
	• Otros proyectos (especifique)
	7.1 Mencione qué aspectos relevantes emanaron de esos proyectos en lo relativo a
	  • Calidad esperada
	  • Productividad esperada
	  • Costos esperados
	  • Beneficios esperados
	  • Otros
	7.2 Si participan en alguno de los proyectos anteriores, señale que opina de lo siguiente
	  • Su participación ¿Fue oportuna y suficiente?
	  • Indique si se especificaron claramente los siguientes puntos:
	  • Objetivos y alcance del proyectos
	  • Objetivos y alcance de su participación durante el proyecto
	  • Etapas del mismo
	  • Sus funciones y responsabilidades en cada etapa
	  • Los productos terminados de cada proyecto
	  • Especificaciones para la revisión y aprobación de cada proyecto
	  • ¿Qué beneficios obtuvo su área al término de los proyectos?
	  • Si no participó formalmente en estos proyectos, ¿A que cree que se debió?
	7.3 ¿Qué podría comentar para el mejoramiento del desarrollo de dichos proyectos desde su inicio hasta la terminación?			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS

	Administración de los recursos de informática
	
	1 ¿Hay procedimientos relativos a la administración de los recursos de informática que se encuentran en las áreas usuarias?
	2 Indique cuál de los siguientes recurso de informática tienen en su departamento área u oficina
	• Microcomputadoras
	• Servidores para redes locales
	• Impresoras
	  • Láser
	  • De otro tipo
	• Equipos para telecomunicaciones (módems, controladores, etc.)
	• Manuales de sistemas de información, de paquetes de software.
	• Disquetes de
	  • Procesamiento de palabras
	  • Hojas electrónicas
	  • Graficadores
	  • Presentadores
	  • Diagramadores
	  • Otros de uso específico
	• Dispositivos de almacenamiento
	  • Discos
	  • Cintas
	  • Otros
	• Papelería
	• Otros
	3 Indique si hay una responsabilidad directa de parte de cada uno de los usuarios en lo que se refiere a
	• Justificación de la tecnología de informática que requiera (equipo, software, etc.)
	• Verificación de que el software instalado en su equipo sea legal.
	• Aprobación del hardware o software que se instale en su departamento, área u oficina
	• Actualización de los paquetes de software que maneja
	• Actualización tecnológica del hardware
	• Depuración de los discos duros o espacio en un disco
	• Respaldo de información
	• Otros (especifique cuáles y cómo ejecuta dicha responsabilidad)			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	5 ¿Tiene algunos comentarios o sugerencias respecto a la administración de los recursos de informática localizados en su departamento, área u oficina? Grado de satisfacción 1 ¿La función de informática ha difundido los productos y servicios que ofrece a los usuarios? 2 Si es así, ¿Como los difundieron en su área? 3 ¿Utiliza actualmente alguno de esos productos o servicios? 4 ¿Que opina de los productos o servicios que usa? 5 ¿Algun requerimiento de su departamento no es apoyado por los productos y servicios de la función de informática? 6 Si es así, ¿Se ha solicitado a informática que satisfaga estas necesidades? 6.1 ¿Ha sido formal esta petición (memorando, solicitud de servicio, etc.) 6.2 Según su opinión ¿Se da atención oportuna y formal a las solicitudes de servicios que emite? 6.3 ¿Cuáles motivos aduce el encargado de informática cuando el servicio no es oportuno? 6.4 ¿Existe una disponibilidad aceptable por parte de informática para la implantación de soluciones requeridas y justificadas por el usuario? 6.5 ¿Cuál es la principal problemática de la función de informática en cuanto • El procedimiento existente para la recepción de solicitudes • Tiempos de respuesta en la planeación, implantación y desarrollo de soluciones • Capacidad profesional por parte del personal de informática • Otros 7 Responda a la siguiente tabla con base en el servicio y facilidades que se han brindado a su departamento en los últimos tres años 8 ¿Informática le brinda cursos de capacitación? 8.1 ¿Son formales, es decir, cuentan con calendario y material de curso, equipos de cómputo, talleres? 8.2 ¿Se efectúa a solicitud expresa del usuario, como una propuesta de informática o ambos? 8.3 ¿Son congruentes con los recursos y necesidades de su departamento?			

(Continúa)

Cuadro 5.4. Programa de trabajo del área de Usuarios de Informática

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	8.4 ¿Se programan y notifican a usted con anterioridad? 8.5 ¿Tiene alguna sugerencia a este respecto? 9. Elaborar cédula de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda.

Cuadro 5.5. Programa de trabajo del área de Control Interno

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

CONTROL INTERNO

OBJETIVO: Conocer y verificar el nivel de control interno que se tiene en informática, a través de la revisión de la políticas y estándares que se aplican en la misma.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CEDULA DE REF.	INVOLUCRADOS
1 Detectar el grado de estandarización y seguimiento formal que existe en el medio informático 2 Evaluar la existencia de políticas y procedimientos requeridos para el desempeño eficiente de cada una de las funciones de informática • Administración de la función de informática • Telecomunicaciones • Planeación de informática • Soporte a usuarios (capacitación, asesoría en hardware, software, aplicaciones, etcétera) • Desarrollo e implantación de sistemas de información • Mantenimiento de sistemas de información • Operación de sistemas de información • Investigación de tecnología relacionada con informática • Automatización de oficinas • Seguridad • Auditoría en informática • Aseguramiento de calidad • Otras especificaciones del negocio	Políticas y procedimientos 1 ¿Existen políticas y procedimientos formales (aprobados por el responsable de informática, la alta dirección o de la auditoría en informática relativos a la administración de cada una de las funciones de informática)? 1.1 Si es así, mencionelas explicando brevemente en qué consiste cada una y las acciones que ejecuta para asegurar que se difundan, se entiendan, se cumplan y se les dé seguimiento formal y oportunamente. 1.2 ¿Qué acciones o actividades se llevaron a cabo para asegurar que tanto políticas como procedimientos cumplan los propósitos específicos del negocio, así como los estándares, políticas y procedimientos sugeridos por las asociaciones e institutos profesionales para cada una de las áreas de informática? 2 ¿Existe una función dentro de la organización o alguna función externa encargada de evaluar el grado de cumplimiento de las políticas y procedimientos establecidos por el control interno (o funciones similares)? 2.1 Si es así, ¿cuáles son las tareas y actividades que lleva a cabo? ¿En qué periodos efectúa dicha evaluación? ¿Que tipo de informes presenta y a quienes los entrega? ¿Como se da seguimiento a sus recomendaciones?			

(Continúa)

Cuadro 5.5. Programa de trabajo del área de Control Interno

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	ENCARGADO	INVOLUCRADOS
3 Verificar y asegurar el cumplimiento oportuno y formal de las políticas y procedimientos relacionados con la función de informática 4 Confirmar la existencia de controles y procedimientos formales para el uso adecuado de los datos y recursos tecnológicos de informática 5 Comprobar y asegurar el cumplimiento oportuno y formal de las políticas y procedimientos relacionados con el manejo de los datos del negocio a través de sistemas de información y de recursos de la función de informática como equipos de cómputo y telecomunicaciones 6 Implantar y dar las recomendaciones necesarias para que se eliminen las debilidades y falta de controles detectados durante esta revisión 7 Asegurar que dichos controles y procedimientos cumplan con los objetivos, propósitos y sugerencias conocidos generalmente a través de institutos y asociaciones profesionales a nivel nacional e internacional	2 2 ¿Dicha función comprueba el grado de actualización que requieren esas políticas y procedimientos para satisfacer los objetivos de control requeridos por el negocio? 3 ¿Qué acciones de control se realizan cuando algunas de las siguientes funciones no cuentan con políticas y procedimientos que aseguren al negocio que la implantación, operación de tales servicios y productos no alteren la integridad, veracidad ni confidencialidad requerida en el manejo de la información del negocio? 4 ¿Existe una adecuada segregación de funciones para el desarrollo de cada uno de los conceptos mencionados? 5 Elaborar cédula de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con				

NOTA: Todas las cédulas deberán contener encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.8. Programa de trabajo del área de Ciclo de Desarrollo e Implantación de Sistemas de Información (Soluciones de Negocio)

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

CICLO DE DESARROLLO E IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN

OBJETIVO: Verificar que el desarrollo de sistemas de información se lleve a cabo con una metodología adecuada y estandarizada.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1. Asegurar que exista un proceso metodológico para ejecutar el ciclo de vida de desarrollo e implantación de sistemas de información formal y estandarizado en la organización 7. Verificar y asegurar que se utilice la metodología del ciclo de vida en cada proyecto de implantación de sistemas de información 3. Confirmar que el personal de desarrollo de sistemas de información conozca dicha metodología con el fin de que se asegure calidad y productividad durante el desarrollo de estos 4. Evaluar el nivel de estandarización que contiene dicha metodología con respecto a las comúnmente aceptadas en el mercado para el desarrollo de sistemas 5. Exponer las recomendaciones pertinentes para que dicha metodología satisfaga las necesidades de desarrollo e implantación de sistemas de información	Metodología 1. ¿Existe en su área una metodología formal de desarrollo de sistemas? 1.1. ¿Dicha metodología contempla qué hacer, quién debe hacerlo y cuándo se debe hacer durante los proyectos de desarrollo e implantación de sistemas? 2. Si es así ¿Cuáles los pasos y lineamientos requeridos para la siguiente clasificación de proyectos? a) Planeación de sistemas de información a desarrollar e implantar b) Desarrollo de sistemas c) Compra de aplicaciones de mercado d) Adaptación de aplicaciones adquiridas a externos e) Rediseño de sistemas existentes g) Aseguramiento de calidad 3. ¿Está documentada formalmente dicha metodología 3.1. Si es así ¿La documentación contempla al menos cada uno de los siguientes puntos ? • Un panorama general de la metodología • Equipos de trabajo sugeridos de acuerdo con el tipo de proyecto • Etapas de la metodología			

(Continúa)

Cuadro 5.6. Programa de trabajo del área de Ciclo de Desarrollo e Implantación de Sistemas de Información (Soluciones de Negocio)

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
6 Comprobar que exista un proceso formal de capacitación para el entendimiento y manejo satisfactorio de la metodología por todo el personal responsable de los proyectos de desarrollo e implantación de sistemas de información 7 Verificar que exista un curso de orientación básica enfocado al personal involucrado en los proyectos que no pertenecen al área de desarrollo y que, sin embargo, desempeñan una función importante en este tipo de proyectos	• Tareas de cada etapa • Secuencia de las etapas y tareas • Responsables e involucrados en cada etapa y tarea • Productos terminados por cada etapa o tarea • Requerimientos técnicos y administrativos para el cumplimiento de cada tarea • Revisiones formales e informales de cada etapa • Duración estimada de cada etapa • Consideraciones para proyectos especiales • Otros que el auditor considere 3.2 ¿Cómo asegura un compromiso formal, un desarrollo y seguimiento eficiente, así como la aprobación final de los proyectos si no se cuenta con una metodología formal que contenga la mencionado en las preguntas 2.3, y 3.1.? 4 En caso de contar con una metodología de desarrollo e implantación de sistemas, ¿La misma fue desarrollada por el personal de informática de la empresa, fue comprada o la rentan cuando se requiere? 5 ¿Se capacitó al personal de desarrollo en el manejo y uso práctico de la misma? 5.1 ¿La capacitación fue impartida de manera formal? • Por grupos de trabajo • Individual • Con casos prácticos • Otros aspectos 5.2 Si no se capacitó al personal en el uso de la metodología ¿Cómo se asegura su entendimiento y uso eficiente durante los proyectos? 6 ¿Desde cuándo la están usando? 7 ¿Se capacita al personal de desarrollo de recién ingreso en el entendimiento y uso de la metodología? 8 ¿Se actualiza la metodología cuando es necesario? 8.1 ¿Qué actividades de investigación o consulta se realizan para formular cambios o adaptaciones en la metodología? 9 ¿Se documentan formalmente estos cambios? 10 ¿Quién los aprueba? 11 ¿Capacitan formalmente al personal requerido en la actualización de la metodología? 12 ¿Existe una congruencia de la metodología de desarrollo con las metodologías recomendadas como estándar en el mercado?			

(Continúa)

Cuadro 6.6. Programa de trabajo del área de Ciclo de Desarrollo e Implantación de Sistemas de Información (Soluciones de Negocio)

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	13. ¿Como se asegura que las metodologías de desarrollo e implantación compradas o rentadas o externos satisfagan los requerimientos del negocio? 14. Comprobar, que las etapas tareas, productos terminados y responsables de la metodología de desarrollo de sistemas se encuentren descritos para todo tipo de proyectos relativos al desarrollo e implantación de sistemas de información. Técnicas 1. ¿El personal de informática conoce cuáles son las técnicas requeridas para el desarrollo, seguimiento y documentación formal de las etapas del desarrollo antes mencionadas? 2. ¿Existen dichas técnicas para el desarrollo de sistemas formal en la empresa? 3. ¿Se capacita al personal de desarrollo de sistemas recién contratado en el manejo de estas técnicas? 4. ¿Qué procedimiento se utiliza para la capacitación del personal de desarrollo en el uso de metodologías y técnicas? 5. ¿Quiénes y cómo determinaron cuáles eran las técnicas requeridas para el desarrollo e implantación de sistemas de información en el negocio? 5.1. ¿Su uso es general en la empresa? ¿Como aseguran de que se aplique? Herramientas. 1. ¿Existe una clasificación de las herramientas de productividad utilizadas en el desarrollo e implantación de sistemas de información de la empresa?			

(Continúa)

Cuadro 5.6. Programa de trabajo del área de Ciclo de Desarrollo e Implantación de Sistemas de Información (Soluciones de Negocio)

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2 Si es así, ¿Podría indicar cuáles de los siguientes se utilizan en la empresa? • Procesadores de palabras • Hojas Electrónicas • Graficadores • Diagramadores • Presentadores • Generadores de aplicaciones • Generadores de bases de datos • Ingeniería de software • Índices de referencia (benchmarks) • Otros (especifique) 3 ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique? **Capacitación y actualización.** 1. Investigue si existen procedimientos formales para capacitar al personal de desarrollo de sistemas de información (o puestos equivalentes) en • Entendimiento y aplicación de • Metodología de desarrollo de sistemas • Técnicas para efectuar las etapas del ciclo de vida de sistemas. • Herramientas de productividad requeridas en el desarrollo 2 ¿Existe una documentación formal de dichos procedimientos? 3 ¿Se cuenta con un responsable directo de elaborar, actualizar, documentar y definir dichos procedimientos de capacitación? 4 ¿Cómo se asegura el cumplimiento oportuno de los procedimientos? 5 Si existen los procedimientos, ¿Al menos contemplan lo siguiente? • Calendarios de los cursos • Responsables de impartir los cursos (personal externo o interno) • Puestos o funciones que requieren dichos cursos • Costos estimados de los cursos • Beneficios esperados de cada curso • Parámetros de medición para asistentes y expositores • Material requerido para cada curso • Responsables de la organización de los cursos			

(Continúa)

Cuadro 5.6. Programa de trabajo del área de Ciclo de Desarrollo e Implantación de Sistemas de Información (Soluciones de Negocio)

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	6 Si no existe un proceso formal de capacitación, ¿Cómo se da seguimiento al entendimiento, uso y actualización oportunos de la metodología, técnicas y herramientas de productividad requeridas por parte del personal durante el desarrollo de sistemas? 7 ¿El responsable de informática está consciente de la importancia que tienen la actualización y mejoramiento continuos del personal de desarrollo de sistemas de información para la implantación de soluciones en el negocio? 8 Cuando se involucran terceros (personal externo) en proyectos de desarrollo e implantación de sistemas de información, ¿Cómo se aseguran de que su metodología, técnicas y herramientas de productividad correspondan por lo menos con el estándar o norma de la empresa? ¿Qué se hace si la empresa no tiene definidos dichos estándares? 9 Elaborar cédula de observaciones con las siguientes columnas: • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda.

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

SISTEMAS DE INFORMACIÓN

OBJETIVO: Verificar el uso de una metodología de desarrollo de los sistemas, las políticas, controles y procedimientos para usarlos y, en su caso, el procedimiento de adquisición de los mismos.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Verificar que los sistemas de información desarrollados e implantados se deriven del proceso formal de planeación de sistemas	Planeación y desarrollo 1 ¿Se cuenta con un plan de proyectos de desarrollo de sistemas a mediano o corto plazo?			
2. Asegurar que los sistemas de información por desarrollar cuenten con el involucramiento y aprobación de la alta dirección y las áreas usuarias correspondientes	2 Si es así, ¿Se ha contemplado la posibilidad de integrar a los equipos de proyectos funciones que aseguren la aplicación formal de los estándares y procedimientos contemplados en la metodología de desarrollo de sistemas? a) Auditor en informática b) Consultor externo c) Otro (especifique)			
3 Comprobar que existan y se lleven a cabo las funciones estándares y procedimientos requeridos durante el desarrollo de un sistema de información	2.1 Si no se involucran funciones de aseguramiento de calidad, ¿Qué procedimientos y qué personal de informática garantiza el cumplimiento de los proyectos y compromisos hechos en la etapa de planeación de sistemas de información por desarrollar?			
4 Verificar y asegurar que se utilice la metodología del CDISI en cada proyecto de implantación de sistemas de información	3 ¿Qué sistemas se encuentran en desarrollo? 3.1 ¿Tales sistemas surgen de la planeación de sistemas?			
5 Confirmar que el personal de desarrollo de sistemas de información ejecute de manera total la metodología de CDISI, con el fin de que se asegure calidad y productividad durante el desarrollo de estos	3.2 Si no es así, ¿Qué criterios y argumentos justificaron su desarrollo? 3.3 ¿Los sistemas que empiezan a desarrollar se integran a la documentación de la planeación de sistemas de información en caso de que no se hayan registrado en esa etapa? 3.4 ¿Quién autoriza el desarrollo de sistemas de información cuando éstos no fueron planeados formalmente?			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CEDULA DE REF.	INVOLUCRADOS
6 Evaluar el nivel de estandarización que se utiliza en el desarrollo de sistemas con respecto a la metodología de desarrollo de sistemas; si no se cuenta con ella, comprobar el apego a los estándares aceptados en el CDISI	3.5 ¿Es una autorización formal? ¿Existen registros de todas estas autorizaciones? 3.6 ¿Qué actividades se llevan a cabo cuando se cancelan proyectos de desarrollo de sistemas de información planeados formalmente? 3.7 ¿Quién autoriza la cancelación de estos proyectos? ¿Qué sucede con estos proyectos? 3.8 ¿Qué actividades se realizan cuando no se cumplen las fechas de proyectos de desarrollo de sistemas de información planeados formalmente?			
7 Hacer las recomendaciones pertinentes para que dicho desarrollo satisfaga las necesidades de los requerimientos planteados en la planeación inicial del proyecto	4 ¿Qué proyectos de desarrollo de sistemas de información hay actualmente?			
8 Verificar que el desarrollo de sistemas de información se efectúe en condiciones de alta calidad y productividad	5 ¿Existen algunas dificultades o contratiempos que afecten de manera significativa algunos proyectos de desarrollo? Si es así, ¿Cuáles son los sistemas de desarrollo afectados? 5.2 Mencione las causas principales de dicha problemática 5.2 ¿Tienen algunas sugerencias que convertan esa problemática en un conjunto de áreas de oportunidad? Si es así ¿Puede Enunciarlas?			
9 Verificar la existencia de políticas y procedimientos formales relativos a la operación de los sistemas de información	6 ¿Durante el desarrollo de sistemas se tiene alguna función que verifique y lleve a cabo el control en los puntos siguientes? • El uso formal, adecuado y oportuno de la metodología de CDISI ¿Cómo? • El desempeño eficiente de los involucrados en el desarrollo de los sistemas ¿Cómo? • Coordinación entre usuarios e informática ¿Cómo? • Coordinación entre informática y los asesores externos durante el proyecto ¿Como? • Programación de revisiones para asegurar la calidad en los productos terminados que se obtienen a lo largo del CDISI ¿Cómo? • Otros que orienten a desarrollo de sistemas de información eficientes y oportunos ¿Cómo?			
10 Comprobar que la liberación de los sistemas en operación haya sido aprobada por los usuarios de manera formal				
11. Obtener el siguiente conocimiento de los sistemas de información en operación • Procedimientos y controles relativos a la operación • Datos y procesos (manuales y computacionales) • Interfases • Tecnología de soporte • Seguridad				

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
12. Asegurar que existan los controles y procedimientos requeridos para • Entendimiento y uso eficiente de los sistemas de información en operación • Documentación • Capacitación previa a la operación inicial y capacitación a personal de nuevo ingreso que estará involucrado en la operación de los sistemas • Satisfacción de los requerimientos de usuarios • Procedimientos que aseguren la continuidad de la operación • Seguridad en la operación de los sistemas • Totalidad, mantenimiento, actualización, autorización, exactitud y registro de datos 13. Asegurar que los sistemas de información que se adquieran de terceros contemplen el proceso metodológico CDISI en la medida que lo requiera el proyecto 14. Estudiar si en este tipo de proyectos se han evaluado diferentes productos y proveedores para asegurar la adquisición de soluciones de vanguardia que se orienten al cumplimiento de los objetivos del negocio y aporten como valor agregado una ventaja competitiva	7. ¿Se tienen procedimientos formales para garantizar que los acuerdos o compromisos que se originen en las reuniones o juntas durante las fases de desarrollo sean efectuados oportunamente? 7.1 Si es así especifique cuáles son esos procedimientos (pasos, responsables del seguimiento de los acuerdos, etcétera) 8. Cuando hay problemas retrasos u otros hechos que obstaculicen el desempeños del desarrollo de sistemas, ¿Se analizan los siguientes aspectos para determinar la solución de dichas limitantes? • Seguimiento de planes y estándares • Supervisión del proyecto • Experiencia y conocimiento técnico de los involucrados en el proyecto • Comunicación entre los integrantes del mismo • Involucramiento y comunicación con los departamentos usuarios • Cargas de trabajo • Entendimiento real de la metodología, técnicas y herramientas • Conocimiento y entendimiento real de los requerimientos del usuario • Asignación de responsabilidades • Administración del proyecto • Otros 9. ¿Con qué periodicidad se revisan los resultados del proyecto, quiénes lo realizan y cómo documentan los resultados? 10. ¿Existe una bitácora que muestre los cambios a los planes, con respecto a lo planeado originalmente? 11. ¿Hay documentación que muestre dichos cambios, motivos o causas de los mismos y sus respectivas autorizaciones (verificar si es la misma bitácora)? 12. ¿Quiénes autorizan dichos cambios? 13. ¿En las especificaciones del sistema propuesto qué procesos son básicos y confidenciales para los usuarios y el negocio en particular? 14. ¿Cómo se asegura que permanezca dicha confidencialidad a lo largo del proyecto de desarrollo y después se implante dicho sistema? 15. ¿La función de aseguramiento de calidad (o función similar) en el desarrollo del sistema contempla los siguientes aspectos de la etapa del análisis? • Puntos de revisión del análisis • Alcance conformado del proyecto			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Perfil y responsabilidades del equipo del proyecto de acuerdo con sus funciones y tareas • Diagramas de procesos (manuales y automatizados) • Modelos de datos • Requerimientos – Seguridad – Procedimientos – Tecnológicos – Otros. • Evaluación del sistema actual • Alternativas (tecnológicas, de procesos, de datos, de organización, económicas, etcétera) • Sistema sugerido de información (solución propuesta) – Diagramas de procesos – Modelos de datos – Interfaces (manuales y automatizadas, internas y con otros sistemas) – Estructuras de datos – Volúmenes de información – Seguridad – Procedimientos – Tecnológicos – Conversión – Evaluación costo/beneficio del sistema propuesto – Otros. • Aprobación de la solución del líder del proyecto por parte de las siguientes áreas del negocio: – Alta dirección (indispensable) – Usuarios responsables del sistema de información (indispensable) – Auditoría (recomendable) – Auditoría en informática (recomendable)			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Puntos de revisión en la construcción o programación del sistema • Compatibilidad y congruencia con el diseño • Elaboración, verificación y documentación de – Diseño de base de datos – Diseño de reportes – Diseño de programas – Diseño de procedimientos y controles – Diseño de interfases (gráficas, narrativas, etc.) – Otros aspectos • Aprobación del diseño • Puntos de revisión en la construcción o programación del sistema • Compatibilidad y congruencia con el diseño • Elaboración, verificación y documentación de – Construcción o programación de base de datos – Construcción o programación de reportes – Construcción o programación de programas – Construcción o programación de procedimientos y controles – Construcción o programación de interfases (gráficas, narrativas, etc.) – Otros aspectos • Aprobación del diseño • Puntos de revisión en las pruebas del sistema (incluye pruebas en el ambiente real) • Planes de pruebas y capacitación • Programas y procedimientos (unitarios) • Subsistemas • Del sistema • Documentación (manual técnico, usuario y de operación del sistema) • Aceptación formal del usuario y del líder del proyecto • Puntos de revisión en la producción o liberación del sistema • Conversión de datos y liberación del sistema • Arranque y formalización del uso inicial del sistema de información • Mejoras o adaptaciones posteriores al sistema de información (justificadas)			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	16 Si el personal de desarrollo de recién ingreso participa en el desarrollo de algún sistema, ¿Se le capacita en el uso de metodología, técnicas y herramientas? 17 ¿Existe un procedimiento formal que asegure el cumplimiento satisfactorio de los estándares, técnicas y herramientas de productividad de dicho personal? 18 Explique cuáles técnicas y herramientas de productividad se emplean en cada etapa del desarrollo de sistemas Operación 1 ¿Cuáles sistemas de información requiere para el soporte de las funciones y actividades de su gerencia, área o departamento? 2 ¿Cuáles están en operación o producción formal? 3 ¿El personal de su área se involucró de m manera activa y permanente cuando se desarrollaron estos sistemas? 4 ¿Los usuarios están debidamente capacitados en el uso de los sistemas que operan en la actualidad? 5 ¿Manejan de manera formal y satisfactoria? • Llenado de documentos . • Captura de transacciones • Proceso de transacciones • Uso y distribución de reportes • Manejo de los manuales de usuario • Procedimientos y controles del sistema 6 Califique en un nivel de 1 a 10 los siguientes puntos Oportunidad ( ) Calidad ( ) Contenido ( ) Veracidad ( ) Confiabilidad ( ) Adecuaciones o nuevos requerimientos ( ) Otros (especifique) ( ) 7 ¿Qué procedimientos se siguen en la atención y solución de los nuevos requerimientos de su área? 8 ¿Cómo se definieron, autorizaron y difundieron estos procedimientos? 9 ¿Existe una función encargada de dar seguimiento oportuno a dichos procedimientos, ya sea de su área o de informática?			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	10 ¿Todos los usuarios que operan los sistemas conocen dichos procedimientos? ¿Por qué? 10.1 ¿Considera que los procedimientos mencionados son suficientes? 11 ¿Existen procedimientos para el manejo de errores o cambios en los sistemas actuales? 11.1 ¿Los cambios y adiciones a los nuevos sistemas son aprobados formalmente por los usuarios? 12 ¿Se tiene una documentación formal de los sistemas en operación? 12.1 Si la respuesta es afirmativa verifique si existe al menos la siguiente documentación • Manuales de usuarios • Manuales de operación • Manuales técnicos • Procedimientos de contingencia y recuperación • Datos de referencia del personal de informática responsable de los sistemas de su área • Fechas en que los sistemas fueron formalmente liberados • Responsables del área usuaria y del área de informática que autorizaron dicha liberación • Procedimientos para el manejo del equipo en el sitio donde operan los sistemas • Procedimientos de seguridad que garanticen la continuidad de la operación de los sistemas • Lista de usuarios responsables de cada sistema y sus principales funciones • Personal de informática responsable de cada sistema • Otros 13 ¿Existe un conocimiento real, por parte de los usuarios, de los alcances y limitaciones de cada sistema en operación? ¿Por qué? 14 ¿Se conocen de manera satisfactoria los siguientes puntos? a) El procedimiento de llenado y captura de documentos fuente para alimentar datos a los sistemas ¿Por qué? b) El manejo de errores y realimentación de datos para asegurar que sean válidos y correctos ¿Porque? c) El uso de los reportes que generan los sistemas ¿Por qué? d) La distribución y periodos de dichos reportes ¿Por qué? e) Procedimientos para el manejo de papelería, reportes rechazados, documentos fuente alimentados, etc ¿Por qué?			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	f) El almacenamiento y destrucción de papelería no útil al negocio ¿Por qué? h) Otros 11) Indique si en la operación de los sistemas de información existen controles para • Verificar totales • Documentos vs. reportes • Cifras de control de computadora vs. totales alimentados • Otros (especifique) • Comprobar que no se omitan movimientos • Confirmar que las correcciones sean autorizadas, correctas y registradas en los archivos correspondientes oportunamente • Verificar que la información confidencial no sea conocida por personal no autorizado • Los procedimientos de verificación dentro de los sistemas en operación que eliminen • Posibilidades de error en el manejo de la información • Tiempos de revisión y captura • Acceso a información confidencial • Información duplicada • Otros • Registros de • Usuarios que operaron los sistemas • Tiempo de operación • Accesos rechazados a módulos del sistema • Datos alimentados a los sistemas • Datos aceptados como válidos • Datos rechazados • Datos corregidos y realimentados • Otros • Para asignación, borrado y cambio oportuno y formal de contraseñas o claves de acceso a los usuarios • Capacitación formal y oportuna de la operación de los sistemas. • Uso adecuado de utilerías de los sistemas • Acceso a la documentación de los sistemas por personal autorizado • Evitar accesos no autorizados a los archivos de datos de los sistemas			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CEDULA DE REF.	INVOLUCRADOS
	• Comprobación de la congruencia de la documentación de los sistemas con lo que existe en los sistemas de operación • Otros 15 ¿Existe documentación de los sistemas en producción? Si es así verifique que exista al menos • Manual de usuario • Manual computacional o técnico del sistema • Manual de operación 16.1 ¿Estos manuales están donde les corresponde? 16.2 ¿Se capacitó al personal en el uso de estos manuales? 16.3 ¿Se actualiza la documentación cuando hay cambios? 16.4 ¿Existe algún sistema a punto de liberarse? 17 ¿Alguna sugerencia para mejorar los sistemas en operación? Soluciones de mercado 1 ¿Existen proyectos relativos a la evaluación, compra e instalación de soluciones de mercado (sistemas de información hechos fuera de la empresa) para el negocio? 1.1 ¿Son proyectos emanados de la planeación de sistemas? 1.2 Si no es así ¿Cómo se justifican? 2 ¿La ejecución y administración de este tipo de proyectos se basan en la metodología del CDISI? 2.1 Si no es así, ¿Cómo se definen, planean, evalúan, seleccionan, aprueban y compran las soluciones de mercado antes de instalarlas en el negocio? 2.2 ¿Con que procedimientos y controles de aseguramiento de calidad se cuenta para las actividades mencionadas en la pregunta 2.1? 3 Mencione los productos terminados, tareas y responsables de las etapas de este tipo de proyectos ejecutados en la empresa 3.1 Mencione las técnicas y herramientas de productividad que utiliza por cada etapa			

(Continúa)

Cuadro 5.7. Programa de trabajo del área de Sistemas de Información

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4 ¿Qué etapas y tareas adicionales realiza cuando compra una solución de mercado y tiene que agregarle o modificarle ciertos módulos o subsistemas para que el sistema de información satisfaga los requerimientos específicos de los usuarios? 5 ¿Qué actividades se efectúan para evaluar las diferentes alternativas que se ofrecen en el mercado en relación con aplicaciones o sistemas de información mientras no existen en el negocio proyectos de este tipo? ¿Quién las lleva a cabo? 6 Elaborar cédula de observaciones con las siguientes columnas: • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones; objetivo, conclusión y observación en caso que proceda.

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

MANTENIMIENTO

OBJETIVO: Conocer y verificar el plan de mantenimiento de la empresa, las políticas y procedimientos para su ejecución y la difusión que existe del mismo

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Comprobar la existencia de políticas y procedimientos formales relativos al mantenimiento preventivo y correctivo del hardware, software sistemas de información y red de telecomunicaciones dentro de la organización 2 Ver que el mantenimiento efectuado a los elementos mencionados garantice la continuidad de las operaciones principales del negocio 3 Verificar que exista un proceso de planeación formal del mantenimiento para los diferentes elementos señalados 4 Asegurar que el mantenimiento sea preventivo, más que correctivo 5 Confirmar que las áreas de informática y usuarias sean informadas con oportunidad de los calendarios de mantenimiento 6. Si se trata de mantenimiento correctivo, proveer a las áreas afectadas de los elementos necesarios que les garantice la continuidad en el manejo de equipo, sistemas y software	Hardware 1 ¿Existe una lista de hardware existente en el negocio (departamento de informática y áreas usuarias)? 1.1 ¿Cómo se levantó el inventario del hardware (inventarios físicos, por software, con base en compras, etc.)? (El auditor en informática debe validar esta información.) 2 ¿Está identificado el lugar físico del hardware y los responsables de su uso y custodia? 3 ¿Se cuenta con manuales o procedimientos para el manejo del equipo? 4 ¿Dichos manuales o procedimientos están actualizados? 5 ¿Existe un procedimiento formal para dar mantenimiento al hardware? 5.1 ¿Dicho procedimiento contempla lo siguiente? • Formulación y difusión del plan de mantenimiento preventivo/correctivo • Difusión del plan de mantenimiento preventivo/correctivo • Medidas que garanticen la continuidad de las operaciones durante este proceso • Desarrollo de las actividades de mantenimiento preventivo/correctivo • Identificación del tipo de mantenimiento (preventivo o correctivo) y las causas o razones de su realización • Identificación de los recursos de hardware que recibirán mantenimiento			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
7. Verificar que existan funciones asignadas de manera formal para las tareas de • Formulación y difusión del plan de mantenimiento preventivo • Difusión del plan de mantenimiento preventivo • Medidas que garanticen la continuidad de las operaciones durante este proceso • Desarrollo de las actividades de mantenimiento preventivo • Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo • Otros 8. Asegurar que se tengan funciones asignadas formalmente para las tareas de • Formulación y documentación de acciones de mantenimiento correctivo • Difusión de las acciones correctivas a las áreas afectadas por este proceso • Medidas que garanticen la continuidad de las operaciones durante este proceso • Desarrollo de las actividades de mantenimiento correctivo • Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo • Otros	• Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo/correctivo • Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática del negocio, usuarios, entre otros) • Elaboración y análisis de estadísticas para fortalecer el mantenimiento preventivo 5.2 ¿señale si este procedimiento es válido para • Microcomputadoras • Minicomputadoras • Mainframes • Equipo periférico • Otro equipo 6. ¿Existen acciones complementarias que apoyen el mantenimiento y que registren algunos datos relacionados con el mismo? 6.1 Indique si entre dichas acciones se cuentan las siguientes • Registro del hardware que reemplazará al equipo que recibirá mantenimiento • Registro del costo originado por el mantenimiento preventivo y el causado por el mantenimiento correctivo para los siguientes elementos 1. Microcomputadoras 2. Minicomputadoras 3. Mainframes 4. Equipo periférico 5. Otro equipo • Todo mantenimiento deberá ser autorizado por el responsable del equipo • Procedimientos de seguridad (egreso e ingreso del equipo) • Elaborar estadísticas que ayuden a identificar las áreas del negocio y los componentes del equipo que "viven en mantenimiento correctivo" • Otros 7. ¿Se actualiza la información de los manuales de alguno de los elementos del hardware cuando se libera una nueva versión? 7.1 ¿Se capacita a los usuarios cuando esto sucede? 8. ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los equipos de cómputo y periféricos? 8.1 Si es así, ¿cuáles son esos controles?			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	9 ¿Se implantan controles y procedimientos a los equipos y periféricos que reciben mantenimiento con objeto de garantizar que la integridad de la información que guardan sea íntegra y correcta antes, durante y después de dicho proceso? 9.1 Si es así, ¿qué controles y procedimientos se tienen contemplados? 9.2 ¿Quién es el responsable de dar seguimiento a dichos controles? 10 ¿Está consciente el personal de informática de que un buen equipo y los procedimientos de uso y cuidado del mismo deben evitar en gran medida los problemas típicos del mantenimiento tradicional? • Altos costos • Cargas de trabajo • Caídas de los equipos • Dificultad en el manejo del equipo • Medidas de seguridad incompletas • Insatisfacción del usuario • Otros 10.1 ¿Está consciente el usuario de la importancia de seguir de manera formal y oportuna los procedimientos de uso y buen cuidado del equipo para evitar en gran medida los problemas mencionados en la pregunta 10? ¿Por qué? 11. ¿La actualización oportuna del hardware es originada por sugerencias del proveedor o usted la solicita? 11.1 ¿Cuáles de las siguientes son las principales razones de la actualización del hardware? • El equipo tiene mal desempeño (velocidad de procesamiento, E/S, otros) • Capacidades de memoria y almacenamiento insatisfactorias • Leyó en el periódico las bondades y facilidades del nuevo modelo • Algún conocido le recomienda adquirir la nueva versión • El gerente o director de informática ha utilizado en las empresas donde ha trabajado y le ha funcionado de "maravilla" • La presión de los usuarios para instalar equipos modernos • Obedece a las nuevas estrategias de la empresa • Se lo prestó un proveedor y prefirió comprarla que volver a usar el equipo viejo • Otros de carácter técnico, estratégico o sentimentales			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	12 Señale si existe algún sistema computarizado que apoye la administración del mantenimiento en aspectos como • Calendarización del mantenimiento (correctivo y preventivo) • Niveles de servicio • Costos del mantenimiento • Causas y soluciones del mantenimiento • Tareas, fechas y responsables del mantenimiento • Otros Software 1 ¿Hay una lista del software existente en la organización (departamento de informática y áreas usuarias)? 1 1 ¿Como se hizo el inventario del software (inventarios a los diferentes equipos por medio de algún software, con base en compras, etc.)? (El auditor en informática debe validar esta información.) 2 ¿Está identificado el equipo donde se encuentra el software y los responsables de su uso y custodia? 3 ¿Se cuenta con manuales o procedimientos para el manejo del software? 4 ¿Están actualizados? 5 ¿Existe un procedimiento formal para dar mantenimiento (actualización) al software? 5 1 Indique si dicho procedimiento contempla lo siguiente • Formulación y difusión del plan de mantenimiento (actualización) preventivo/correctivo • Medidas que garanticen la continuidad de las operaciones durante este proceso • Desarrollo de las actividades de mantenimiento (actualización) preventivo o correctivo • Identificación del tipo de mantenimiento o actualización (preventivo o correctivo) y las causas o razones de su realización • Identificación del software que recibirá mantenimiento o requiere actualización • Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento (actualización) preventivo o correctivo			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática, usuarios, otros) • Elaboración y análisis de estadísticas para fortalecer el mantenimiento (actualización) preventivo 5.2 ¿Este procedimiento es válido para? • Paquetes de software (procesadores de palabras, hojas electrónicas, etc.) • Lenguajes de programación (tercera, cuarta generación, CASE, etc.) • Bases de datos • Sistemas operativos, utilerías, software de comunicaciones • Otro software 6. ¿Está identificado el software original y las copias? 7. ¿Existe un mismo procedimiento para dar mantenimiento (actualización) al software instalado en micros, minis y mainframes? 7.1 Si no es así, ¿existe el siguiente procedimiento? a) Definición de los responsables de dar mantenimiento o actualización del software b) Razones o causas que justifiquen el proceso de mantenimiento o actualización c) Identificación del tipo de mantenimiento o actualización (preventivo o correctivo) d) Calendario de programación (fechas, usuarios afectados, etc.) e) Identificar las partes del software que serán afectadas por dicho mantenimiento o actualización f) Registro del software que recibirá mantenimiento o será actualizado g) El software afectado por el mantenimiento debe ser alojado en el siguiente orden: • Área de prueba • Área de instalación del producto h) Todo cambio ha de ser probado y autorizado por un responsable definido con anterioridad y) Seguridad (acceso para cambios y adaptaciones) j) Identificar productos del software que "viven en mantenimiento correctivo" k) Otros 8. ¿La información de los manuales del producto se actualiza cuando se coloca una nueva versión?			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	9. ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los productos del software que se está operando? 9.1 Si es así, ¿cuáles son esos controles? 10. ¿Se implantan controles y procedimientos inherentes a los productos de software que reciben mantenimiento con objeto de garantizar la integridad de la información que se relaciona con estos productos? 10.1 Si es así, ¿cuáles son esos controles y procedimientos? 11. ¿Está consciente el personal de informática de que un buen producto evita en gran medida los problemas típicos del mantenimiento tradicional? • Cargas de trabajo • Eliminar módulos que no cumplen la totalidad de los requerimientos de informática • Dificultad en el manejo del software • Medidas de seguridad incompletas • Otros 12. ¿La actualización constante del software es originada por sugerencias del proveedor o usted la solicita porque? • No cumple los requisitos técnicos exigidos por informática • No satisface los requerimientos de los usuarios • Leyó en el periódico las bondades y facilidades del nuevo modelo • Algún conocido le recomienda adquirir la nueva versión • El gerente o director de informática lo ha utilizado en las empresas donde ha trabajado y le ha funcionado de "maravilla" • La presión de los usuarios para instalar equipos modernos • Obedece a las nuevas estrategias de la empresa • Se lo prestó un proveedor y prefirió comprarlo que volver a usar el equipo viejo • Otros de carácter técnico, estratégico o sentimentales 13. Indique si cuenta con algún sistema computarizado que apoye el control del mantenimiento en aspectos como • Calendarización del mantenimiento (correctivo y preventivo) • Niveles de servicio • Costos del mantenimiento • Causas y soluciones del mantenimiento • Tareas, fechas y responsables del mantenimiento • Otros			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Sistemas de información 1. ¿Existe una lista de los sistemas de información en operación? 2. ¿Dichos sistemas fueron aprobados formalmente por los usuarios? 3. ¿Se cuenta con manuales de usuarios, técnicos y de operación para cada uno de los sistemas de información en producción? 4. ¿Dichos manuales están actualizados? 5. ¿Hay un procedimiento formal para el mantenimiento de los sistemas de información? 5.1 ¿Dicho procedimiento contempla lo siguiente? • Formalización y difusión del plan de mantenimiento (actualización)preventivo/correctivo • Medidas que garanticen la continuidad de las operaciones durante este proceso • Desarrollo de las actividades de mantenimiento (actualización) preventivo/correctivo • Identificación del tipo de mantenimiento (preventivo o correctivo) y las causas o razones de su realización • Identificación de los sistemas de información que recibirán mantenimiento o serán actualizados • Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento o actualización • Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática de la empresa, usuarios, entre otros) • Elaboración y análisis de estadísticas para fortalecer el mantenimiento o actualización preventivo 5.2 Indique si este procedimiento es válido para • Sistemas de información desarrollados con paquetes de software (procesadores de palabras, hojas electrónicas, otros) • Sistemas de información desarrollados con lenguajes de programación (tercera cuarta generación, bases de datos, CASE, etc.) • Sistemas de información comprados a externos (soluciones de mercado) 6. ¿Están identificados los sistemas de información comprados a externos?			

(Continúa)

Cuadro 6.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	7 ¿Se cuenta con el mismo procedimiento formal para dar mantenimiento o actualizar los sistemas de información instalados en micros, minis o mainframes? 7.1 Si no es así, indique si existe el siguiente procedimiento a) Definición de los responsables de dar mantenimiento o actualizar los sistemas de información b) Razones o causas que justifiquen el proceso de mantenimiento o actualización c) Identificación del tipo de mantenimiento o actualización (preventivo o correctivo) d) Calendario de programación (fechas, usuarios afectados, etc.) e) Identificar los módulos o componentes de los sistemas de información afectados por dicho mantenimiento o actualización f) Registro de los sistemas de información que recibirá mantenimiento o serán actualizados g) Los sistemas de información afectados por el mantenimiento debe ser alojado en el siguiente orden • Area de desarrollo (nuevos módulos) y prueba (durante la actualización) • Area de producción (instalación de cambios o adaptaciones aprobadas) h) Todo cambio ha de ser probado y autorizado por un responsable definido para este objetivo y) Seguridad (acceso para cambios y adaptaciones) j) Identificar los sistemas de información que "viven en mantenimiento correctivo" k) Otros 7.2 ¿Se actualiza la información de los manuales de usuarios, técnicos y de operación cuando así corresponda? (Verificar los últimos cambios) 8 Si el mantenimiento implica la inserción de un módulo, ¿se capacita a los usuarios? 9 ¿Existen controles para que únicamente personal actualizado dé mantenimiento a los sistemas de información en operación? 9.1 Si es así, ¿cuáles son esos controles? 10 ¿Se implantan controles y procedimientos en los sistemas de información que reciben mantenimiento con objeto de garantizar la integridad de la información? 10.1 Si es así, ¿con qué controles y procedimientos se cuenta?			

(Continúa)

Cuadro 6.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	11 ¿Está consciente el personal de informática de que un buen producto evita en gran medida los problemas típicos del mantenimiento tradicional? • Cargas de trabajo • Eliminación de sistemas que no cumplen la totalidad de los requerimientos del usuario • Sistemas que no contemplan controles y procedimientos que garanticen confiabilidad, oportunidad y calidad • Medidas de seguridad incompletas • Insatisfacción de la alta dirección por los bajos resultados de los sistemas • Falta de estandarización en el uso de 1 Metodología para el desarrollo 2 Técnicas (análisis, diseño, etc.) 3 Tareas 4 Productos terminados 5 Funciones y responsabilidades 6 Otros • Sistemas que no son flexibles (no se adaptan a los cambios de la empresa) • Otros 12. Señale si hay algún sistema computarizado que apoye el control del mantenimiento en aspectos como • Calendarización del mantenimiento preventivo • Seguimiento al mantenimiento (correctivo y preventivo) • Niveles de servicio Costos del mantenimiento • Causas y soluciones del mantenimiento • Otros Red de telecomunicaciones 1 ¿Hay una lista de los componentes de la red existente en el negocio, así como una ilustración gráfica de la distribución y cantidad de los mismos? 1 1 ¿Cómo se inventarió la red de telecomunicaciones (inventarios físicos, por software, con base en las compras, etc.)? (El auditor en informática debe validar esta información.) 2 ¿Está identificado el lugar físico de la red y los responsables de su uso y custodia? 3 ¿Existen manuales o procedimientos para el manejo de la red?			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4 ¿Dichos manuales o procedimientos están actualizados? 5 ¿Existe un procedimiento formal para el mantenimiento de la red? 5.1 ¿Este procedimiento contempla lo siguiente? • Formulación y difusión del plan de mantenimiento preventivo/correctivo • Medidas que garanticen la continuidad de las operaciones durante este proceso • Desarrollo de las actividades de mantenimiento preventivo/correctivo • Identificación del tipo de mantenimiento (preventivo o correctivo) y las causas o razones de su realización • Identificación de los recursos de la red que recibirán mantenimiento • Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo/correctivo • Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática de la empresa, usuarios, entre otros) • Elaboración y análisis de estadísticas para fortalecer el mantenimiento preventivo 5.2 ¿Este procedimiento es válido para? • Componentes de los enlaces por satélite • Componentes para los enlaces terrestres • Componentes para los enlaces internos en la(s) empresa(s) • Otro equipo 6 ¿Entre las acciones complementarias con que apoyan el proceso de mantenimiento y que registran algunos datos relacionados con el mismo tienen alguna(s) de las siguientes? • Registro de los componentes de la red de telecomunicaciones que reemplazarán al equipo que recibirá mantenimiento • Registro del costo originado por el mantenimiento preventivo o correctivo para los siguientes elementos • Componentes de los enlaces por satélite • Componentes para los enlaces terrestres • Componentes para los enlaces internos en la(s) empresa(s) • Otro equipo • Todo mantenimiento deberá ser autorizado por el responsable del equipo			

(Continúa)

Cuadro 5.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Procedimientos de seguridad (egreso e ingreso del equipo) • Elaborar estadísticas que ayuden a identificar las áreas de la empresa y los componentes de equipo que "viven en mantenimiento correctivo" • Otros 8 ¿Se actualiza la información de los manuales de alguno de los elementos de la red de telecomunicaciones cuando se libera una nueva versión tecnológica? 8.1 ¿Se capacita a los usuarios de la red de telecomunicaciones cuando sucede lo anterior? 9 ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los equipos de cómputo y periféricos? 9.1 Si es así, ¿cuáles son esos controles? 10 ¿Se implantan controles y procedimientos en los componentes de la red de telecomunicaciones que reciben mantenimiento con objeto de garantizar que la información alojada en estos componentes permanezca íntegra y correcta antes, durante y después de este proceso? 10.1 Si es así, ¿cuáles son esos controles y procedimientos? 10.2 ¿Quién es el responsable de dar seguimiento a dichos controles? 11 ¿Está consciente el personal de informática de que un buen equipo y la aplicación de las políticas y procedimientos de uso y cuidado del mismo evitan en gran medida los problemas típicos del mantenimiento tradicional? • Altos costos • Cargas de trabajo y tiempos de respuesta bajos • Caídas de la línea e interrupción de comunicaciones • Dificultad en el manejo de la red • Medidas de seguridad incompletas • Insatisfacción del usuario/informática • Otros 11.1 ¿Está consciente el usuario de la importancia de seguir de manera formal y oportunamente las políticas y procedimientos de uso y buen cuidado del equipo para evitar en gran medida los problemas mencionados en la pregunta 11? ¿Por qué? 12 ¿La actualización oportuna de la red es originada por sugerencias del proveedor o usted la sabe?			

(Continúa)

Cuadro 6.8. Programa de trabajo del área de Mantenimiento

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	12 Indique cuáles son las principales razones de la actualización de la red de telecomunicaciones • El equipo tiene mal desempeño (velocidad de transmisión, por ejemplo) • Capacidades de transmisión inadecuadas • El gerente o director de informática lo ha utilizado en las empresas donde ha trabajado y le ha funcionado de "maravilla" • Nuevas estrategias de la empresa • Otros de carácter técnico o estratégico 13 ¿Existe algún sistema computarizado que apoye la administración del mantenimiento en los siguientes aspectos? • Calendarización del mantenimiento preventivo • Seguimiento del mantenimiento correctivo y preventivo • Niveles de servicio • Costos del mantenimiento • Causas y soluciones del mantenimiento • Tareas, fechas y responsables del mantenimiento • Otros 14 Elaborar cédula de observaciones con las siguientes columnas: • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda.

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

REDES LOCALES Y TELECOMUNICACIONES

OBJETIVO: Conocer y verificar el nivel de eficiencia de las redes locales y las telecomunicaciones, a través de la revisión de la planeación, diseño, instalación, operación, mantenimiento y seguridad de las mismas.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
Redes locales: 1 Asegurar que exista una función formal de administración de la red local 2 Asegurar la existencia de procedimientos y controles que orienten a la satisfacción de: • La administración de las redes locales • La instalación de las redes locales • La operación y seguridad de las redes locales • El mantenimiento de las redes locales 3 Detectar el grado de confianza, satisfacción y desempeño que brindan al negocio las redes locales existentes 4 Confirmar que existan parámetros de medición del desempeño de las redes 5 Evaluar el grado de soporte que se brinda a los usuarios de la red en el uso de sistemas y software al que tienen acceso en la misma	**Redes locales** *Administración* 1 ¿La empresa cuenta con red(es) local(es)? 1.1 Si es así, ¿cuántas hay en dicha red, incluyendo el servidor?(Mencione las características básicas de aquéllas y de los periféricos.) 1.2 ¿Qué software (paquetes, lenguajes, sistemas de información, sistemas operativos, bases de datos, etc.) hay instalado(s)? ¿Cuáles son las versiones correspondientes? 1.3 Si no tiene una red local ¿con cuantas micros, periféricos, paquetes, etc. cuenta? 1.4 ¿Existe una administración formal de la red? 1.5 En caso de no tener una administración formal de la(s) red(es) o de las microcomputadoras no conectadas en red de la empresa ¿cómo se da seguimiento a los siguientes aspectos? • Planeación de nueva tecnología de información (hardware, software, etc.) para la red • Monitoreo de las actividades de la operación y mantenimiento de la red • Procedimientos de control y seguridad de la red • Aspectos legales del software instalado Capacitación y soporte a usuarios • Otros			

(Continúa)

Cuadro 6.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
6 Determinar si existen los suficientes controles y procedimientos de seguridad para la red de la empresa 7 Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes de las redes locales 8 Asegurar que solo se encuentre instalado software legalizado en las redes locales 9 Comprobar si se cuenta con algún software que apoye el monitoreo y la auditoría de los diferentes elementos que componen una red local Telecomunicaciones: 1 Asegurar que exista una función formal de administración de la red de comunicaciones 2 Asegurar la existencia de procedimientos y controles que orientan a la satisfacción de • La administración de la red de telecomunicaciones • La instalación de la red de telecomunicaciones • La operación y seguridad de la red de telecomunicaciones • El mantenimiento de la red de telecomunicaciones 3 Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio la red de comunicaciones existentes 4 Verificar que existan parámetros de medición del desempeño de la red de comunicaciones	1 6 Si la empresa tiene una administración de la(s) red(es) local(es) o microcomputadoras no conectadas en red, ¿cuáles de las funciones listadas a continuación realiza, con qué tareas efectua cada función y cómo les dan seguimiento sus coordinadores o jefes inmediatos? Planeación • Definir un plan formal que contemple • Evaluación del hardware actual – Análisis y evaluación de la red local actual (si existe) – Análisis y diagnóstico del número de microcomputadoras, características, usuarios, etc – Análisis y diagnóstico de periféricos – Otros • Evaluación del software actual Análisis y diagnóstico del software instalado en la red o computadoras aisladas graficadores, procesadores, hojas electrónicas, otros Lenguajes de programación, sistemas operativos, etc. – Cantidad de licencias, copias pirata, versiones, número de usuarios – Software por legalizar – Otros • Estudio de justificación de instalación o reemplazo de la red local – Hardware requerido computadores, periféricos, otros – Configuración de la red distribución física, interfase, etc – Software requerido aspectos legales, paquetes de cómputo, lenguajes de programación, sistemas operativos, otros – Evaluación costo/beneficio – Procedimientos de capacitación, seguridad, operación mantenimiento monitoreo, etc Organización • Elaboración de políticas y procedimientos para • La evaluación de hardware, software, etc de la red • Adquisición o instalación de hardware o software • Asignación y baja de usuarios • Administración de la red			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
5 Evaluar el grado de soporte que se brinda a los usuarios de la red de comunicaciones en el uso de sistemas y software al que tienen acceso en la misma 6 Determinar si existen los suficientes controles y procedimientos de seguridad para la red de comunicaciones de la empresa 7 Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes de la red de comunicaciones 8 Asegurar que sólo se encuentre instalado software legalizado en la red de comunicaciones 9 Verificar si se cuenta con algún software que apoye el monitoreo y la auditoría de los diferentes elementos que componen la red de comunicaciones	• Nivel de servicios para usuarios de la red – Desempeño - Tiempos de respuesta - Proceso - Atención a fallas - Otros – Capacitación, soporte, mantenimiento - Hardware - Software - Aplicaciones – Operación de - Equipo - Software - Aplicaciones - Seguridad – Datos - Software - Aplicaciones - Accesorios 2 ¿Algún personal externo interviene en las funciones de administración mencionadas? 2.1 Si es así, ¿en qué funciones participa y por qué? 3 ¿Existe la documentación formal que especifique qué hacer y cómo efectuar cada función administrativa de la red? 3.1 Si es así ¿Las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación? 4 En caso de que no exista esta documentación, ¿cómo se indica al personal responsable y a los usuarios lo referente a los puntos mencionados en la pregunta 1? 5 ¿Existe un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios? 6 ¿Cómo se canalizan las dudas, sugerencias y compromisos entre los usuarios y los responsables de la red? 7 ¿Qué garantiza que se está utilizando la tecnología de redes más adecuada para la empresa? 8 ¿Hay análisis costo/beneficio de las diferentes estrategias de redes implantadas? ¿Se han aprobado de manera formal?			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Instalación 1 ¿Existen procedimientos que aseguren la oportuna y adecuada instalación de los diferentes componentes de la red conforme se hayan realizado los contratos y compras formales de los mismos? 2 Mencione las actividades que se realizan durante el proceso de instalación de los componentes de la red local (hardware, software, procedimientos, etc.) 3 ¿Las compras de los diferentes elementos de la red, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla? 4 En caso de que las compras e instalación de componentes de la red (sea hardware, software u otros) no se hayan planeado formalmente, ¿cómo se justifica esto ante los responsables de informática y de las áreas usuarias? 5 En cuanto a la instalación de software, ¿cómo se asegura la compra legal? ¿Cómo aseguran que no sea instalado en otros equipos de la empresa sin licencia de uso? ¿Qué hacen cuando detectan anomalías del software? 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección del software? 6. Cuando son terceros (personal externo) los encargados de la instalación parcial o total de cualquiera de los elementos que componen la red, ¿cómo se asegura la empresa de que esto se haga a sus políticas y lineamientos de servicio, oportunidad y confidencialidad? 7 ¿Tienen alguna(s) sugerencia(s) que apoyen el proceso de instalación? Operación y seguridad 1 ¿Se cuenta con manuales de operación de la red? ¿Contemplan aspectos de seguridad? 1.1 Si es así, ¿el personal responsable de administrarla y operarla fue capacitado y preparado para el manejo de la misma? ¿Le da seguimiento a la seguridad? 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2 Indique si existen estándares relativos a la operación y administración de la red como • Estándares de desempeño • Tiempos de respuesta • Tráfico (volúmenes de información, velocidad) • Interrupciones • Tiempo de recuperación de la red • Equipos o terminales interconectados • Otros • Estándares de mantenimiento • Calendarios (fechas, horarios, etc.) • Responsables • Otros 2.1 Si existen, ¿son aplicados formalmente por los responsables de la red? 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos? 2.3 Una vez que se aplican estos estándares, ¿qué datos se envían a otras áreas (usuarios, auditoría en informática)? 2.4 ¿Los costos por el uso de la red se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios? 2.5 ¿Existe otro procedimiento para establecer los costos derivados por el uso de la red? Si es así, ¿cuál? 2.6 ¿El usuario aprueba formalmente este procedimiento de pago? 3 ¿Se desarrolló o adquirió algún cuestionario estándar que permita saber el nivel de servicios que brinda la red? 3.1 Si es así, ¿con qué periodicidad se distribuye este cuestionario a los usuarios o encargados de la red? 3.2 ¿Qué indicadores o parámetros importantes salen de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática? 4 ¿Hay procedimientos que protejan los datos transmitidos de una red local a otra(s)? 4.1 Si se tienen, ¿cuáles son? 4.2 ¿Se cuenta con un responsable o un software de comunicaciones que vigile de manera permanente que los datos sean transmitidos con los estándares de oportunidad, totalidad, exactitud y autorización de una red a otra s)? 4.3 ¿Existen registros con información relevante para el administrador de la red o el auditor en informática?			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4.4 Si es así, señale si éstos contienen información relativa a • Usuarios que accesaron a la red • Operaciones realizadas en la red (envío, recepción) • Tiempos de conexión • Interrupciones en el transcurso del uso de la red • Causas • Tiempo para reiniciar cada interrupción • Terminales o equipos conectados • Accesos invalidados a la red • Terminales donde se llevaron a cabo estos accesos no autorizados • Otros 4.5 ¿Estos registros son generados por algún software de la red o por los responsables de la misma? 5 Señale si se tiene identificada formalmente la siguiente información • Usuarios de la red • registros y niveles de acceso • Terminales conectadas a la red • Responsables de la red • Procedimientos de contingencia • Software • Periféricos conectados • Software original y pirata instalado • Software de las micros conectadas a la red (duplicidad o carencia de software en la red) • Tipos de unidades centrales de procesamiento (CPU) • Capacidad de discos o espacio libre por servidor y micros • Otros 5.1 ¿Estos registros son generados por algún software de la red o los elaboran por separado los responsables de la misma? 6 ¿Hay una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios de la red? 7. ¿Existe un procedimiento formal para dar servicio oportuno y eficiente a los requerimientos de los usuarios? 7.1 ¿Lo conocen los usuarios? 8. ¿La red tiene controles de acceso a personas no autorizadas (acceso a equipo, datos y software)? 8.1 En caso de contar con esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado?			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	8.2 Si es así ¿cuáles son estos controles y quiénes le dan seguimiento? 8.3 Verificar que los controles contemplen al menos • Protección de archivos • Protección a programas fuente de las aplicaciones en red • Protección a otro software alojado en la red • Métodos para prevenir el monitoreo no autorizado de la red • Detección inmediata y automatizada de accesos no autorizados • Contraseñas que autoricen el acceso a la red, sin permitir la entrada a archivos no autorizados • Otros 9. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red (tarjetas, terminales, manuales, software, documentación, etc.)? 9.1 En caso de contar con esos controles, ¿cómo se aseguran los responsables de darles seguimiento? 9.2 Verificar que estos controles cuenten con • Protección adecuada de los componentes de la red (cables, tarjetas, terminales, servidores, etc.) • Guardias o personal que vigile el acceso al centro de telecomunicaciones • Bitácoras de acceso a las áreas conectadas a la red • Métodos de control de acceso como pases, tarjetas de identificación, puertas de candados, monitores, etc. • Listado de personal autorizado con acceso a las terminales y controladores de la red • Otros 10. ¿Se tiene un seguro que proteja el software y el equipo de la red? 11. ¿Se cuenta con alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en la(s) red(es)? 12. ¿Estos convenios están formalizados? 13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento contínuo de la(s) red(es) local(es) de la empresa como las siguientes? • Evaluación periódica de la red: hardware, software, grado de satisfacción, grado de utilización, etc. • Acceso a la red de nuevos usuarios: niveles de acceso por perfil de usuario, asignaciones de software o datos para utilizar, consultar, modificar, borrar, etc.			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Aspectos administrativos administrador u operadores (tareas, sueldos, capacitación, vacaciones, reemplazos, otros) • Capacitación, planeación, ejecución y actualización • Crecimiento de la red periférico, memoria, usuarios, software, aplicaciones • Respaldo datos equipo periféricos, software, aplicaciones, etc • Seguridad controles, procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc • Otros que se consideren pertinentes **Telecomunicaciones** **Administración** 1 ¿La empresa cuenta con una RC? 1 1 Si es así, ¿qué tipo de enlaces tiene (satelitales, terrestres)? 1 2 ¿Qué software de comunicaciones utiliza para el manejo de la RC? ¿Cuáles son las versiones correspondientes? 1 3 Si no tiene una RC, ¿piensa integrar una a la empresa? ¿Cuándo? 1 4 ¿Existe una administración formal de la RC? 1 5 En caso de no tener una administración formal de la RC, indique cómo se da seguimiento a los siguientes aspectos • Planeación de nueva tecnología de información (hardware, software, etc) para la RC • Monitoreo de las actividades de la operación y mantenimiento de la RC • Procedimientos de control y seguridad • Aspectos legales del software instalado • Capacitación y soporte a usuarios, operadores y técnicos de la RC • Otros 1 6 Si la empresa tiene administración de la RC, ¿cuáles de las funciones mencionadas a continuación realiza, con qué tareas efectúa cada función y cómo les da seguimiento sus coordinadores o jefes inmediatos? Planeación • Definir un plan formal que contemple • Evaluación de la red de comunicaciones (si existe)			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	- Análisis y evaluación de la red de comunicaciones: diseño, uso, costo/beneficio - Análisis y diagnóstico de módems, controladores, cables medios de transmisión, etc - Otros • Evaluación del software actual de la red de comunicaciones - Análisis y diagnóstico del software instalado para el uso de la red de comunicaciones - Software de monitoreo - Cantidad de licencias, copias pirata, versiones, número de usuarios - Software por legalizar - Otros • Estudio de justificación de instalación o reemplazo de la red de comunicaciones local - Hardware requerido módems, multiplexores, antenas, etc - Configuración de la red de comunicaciones distribución física, interfaces, etc - Software requerido operación, seguridad, monitoreo, etc - Evaluación costo/beneficio - Procedimientos de capacitación, seguridad, operación mantenimiento, monitoreo, etc Organización • Elaboración de políticas y procedimientos para • La evaluación de hardware, software, etc. de la red de comunicaciones • Adquisición o instalación de hardware o software de la red de comunicaciones • Asignación y baja de usuarios en la red de comunicaciones • Administración de la red de comunicaciones • Nivel de servicios para usuarios de la red de comunicaciones - Desempeño en tiempos de respuesta, proceso, atención a fallas, otros - Capacitación, soporte, mantenimiento del hardware, software y aplicaciones • Operación de equipo, software y aplicaciones • Seguridad de datos, software, aplicaciones y accesorios 2 ¿Algún personal externo interviene en la administración de la RC mencionada? 2.1 Si es así, mencione cuál y por qué			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	- Análisis y evaluación de la red de comunicaciones: diseño, uso, costo/beneficio - Análisis y diagnóstico de módems, controladores, cables, medios de transmisión, etc - Otros • Evaluación del software actual de la red de comunicaciones - Análisis y diagnóstico del software instalado para el uso de la red de comunicaciones - Software de monitoreo - Cantidad de licencias, copias pirata, versiones, número de usuarios - Software por legalizar - Otros • Estudio de justificación de instalación o reemplazo de la red de comunicaciones local - Hardware requerido: módems, multiplexores, antenas, etc - Configuración de la red de comunicaciones: distribución física, interfaces, etc - Software requerido: operación, seguridad, monitoreo, etc - Evaluación costo/beneficio - Procedimientos de capacitación, seguridad, operación mantenimiento, monitoreo, etc Organización • Elaboración de políticas y procedimientos para • La evaluación de hardware, software, etc. de la red de comunicaciones • Adquisición o instalación de hardware o software de la red de comunicaciones • Asignación y Baja de usuarios en la red de comunicaciones • Administración de la red de comunicaciones • Nivel de servicios para usuarios de la red de comunicaciones - Desempeño en tiempos de respuesta, proceso, atención a fallas, otros - Capacitación, soporte, mantenimiento del hardware, software y aplicaciones • Operación de equipo, software y aplicaciones • Seguridad de datos, software, aplicaciones y accesorios 2. ¿Algún personal externo interviene en la administración de la RC mencionada? 2.1 Si es así, mencione cuál y por qué			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	3 ¿Hay documentación formal que especifique qué hacer y cómo realizar cada una de las funciones de administración de la RC? 3.1 De ser así, ¿las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación? 4 En caso de que no exista esta documentación, ¿cómo se indica al personal responsable de la RC y a los usuarios lo referente a los puntos mencionados en la pregunta 1? 5 ¿Se cuenta con un plan vacacional y de remplazo de personal que asegure el servicio continuo a los usuarios? 6 ¿Cómo se canalizan las dudas, sugerencias y compromisos entre los usuarios y los responsables de la RC? 7 ¿Qué garantiza que se está utilizando la tecnología de RC más adecuada para la empresa? 8 ¿Existen análisis costo/beneficio de las diferentes estrategias de la RC implantada? ¿Son aprobados de manera formal? Instalación 1 ¿Existen procedimientos que aseguren la oportuna y adecuada instalación de los diferentes componentes de la RC conforme se hayan realizado los contratos y compras formales de los mismos? 2 Mencione las actividades que se realizan durante el proceso de instalación de los componentes de la RC (hardware, software, procedimientos, etc.) 3 ¿Las compras de los diferentes elementos de la RC, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla? 4 En caso de que las compras e instalación de componentes de la red sea hardware, software u otros no se hayan planeado formalmente, ¿cómo se justifica esto ante los responsables de informática y de las áreas usuarias en el uso de dicha RC? 5 En cuanto a la instalación de software, ¿cómo se asegura la compra legal? ¿Cómo aseguran que no sea instalado en otros equipos de la empresa sin licencia de uso? ¿Qué hacen cuando detectan anomalías del software? 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección del software?			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	6 Cuando son terceros (personal externo) los encargados de la instalación parcial o total de cualquiera de los elementos que componen la RC, ¿cómo se asegura la empresa de que esto se haga a sus políticas y lineamientos de servicio, oportunidad y confidencialidad? 7 ¿Tienen alguna(s) supervisora(s) que apoyen el proceso de instalación? Operación y seguridad 1 ¿Se cuenta con manuales de operación de la RC? ¿Contemplan aspectos de seguridad? 1.1 Si es así, ¿el personal responsable de administrar y operar la RC fue capacitado y preparado para el manejo de la misma? ¿Le da seguimiento a la seguridad? 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa? 2 ¿Existen estándares relativos a la operación y administración?, por ejemplo • Estándares de desempeño • Tiempos de respuesta • Tráfico (volúmenes de información, velocidad) • Interrupciones • Tiempo de recuperacion • Equipos o terminales interconectados • Otros • Estándares de mantenimiento • Calendarios (fechas, horarios, etc.) • Responsables • Otros 2.1 Si existen, ¿los responsables de la RC los aplican de manera formal? 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos? 2.3 Una vez que se aplican estos estándares, ¿qué datos se envían a otras áreas (usuarios, auditoría en informática)? 2.4 ¿Los costos por el uso de la RC se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios? 2.5 ¿Existe otro procedimiento para establecer los costos derivados por el uso de la RC? Si es así, ¿cuál es?			

(Continúa)

Cuadro 6.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2.6 ¿El usuario aprueba formalmente este procedimiento de pago? 3 ¿Se desarrolló o adquirió algún cuestionario estándar que permita medir el nivel de servicios que brinda la RC? 3.1 Si es así, ¿con qué periodicidad se distribuye este cuestionario a los usuarios o encargados de la RC? 3.2 ¿Qué indicadores o parámetros importantes salen de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática? 4 ¿Se tienen procedimientos que protejan los datos transmitidos de una RC propia local a otra(s)? 4.1 Si se tienen, ¿cuáles son? 4.2 ¿Existe un responsable o un software de comunicaciones que revise de manera permanente que los datos sean transmitidos con los estándares de oportunidad, totalidad, exactitud y autorización de una RC a otra(s)? 4.3 ¿Existen registros con información relevante para el administrador de la RC o el auditor en informática? 4.4 Si es así, señale si contienen la siguiente información • Usuarios que accesaron a la RC • Operaciones realizadas en la RC (envío, recepción) • Tiempos de conexión • Interrupciones en el transcurso del uso de la RC • Causas • Tiempo para reiniciar cada interrupción • Terminales o equipos conectados • Accesos invalidados a la RC • Terminales donde se llevaron a cabo estos accesos no autorizados • Otros 4.5 ¿Estos registros son generados por algún software de la RC o los elaboran de manera independiente los responsables de la administración de la misma? 5 Indique si se tiene identificada formalmente la siguiente información • Usuarios de la RC • registros y niveles de acceso • Terminales conectadas a la RC • Responsables • Procedimientos de contingencia • Software • Periféricos conectados			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Componentes • Otros 5.1 ¿Estos registros son generados por algún software de la RC o por los responsables de su administración? 6 ¿Existe una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios de la RC? 7 ¿Hay un procedimiento formal para dar servicio oportuno y eficiente a los requerimientos de los usuarios? 7.1 ¿Lo conocen los éstos? 8 ¿La RC tiene controles de acceso a personas no autorizadas (acceso a equipo, datos y software)? 8.1 En caso de contar con esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado a la RC? 8.2 Si es así, ¿cuáles son estos controles y quiénes son los responsables de darles seguimiento? 8.3 Verificar que los controles contemplen al menos • Protección a datos transmitidos a través de la RC • Protección a los componentes de la RC • Métodos para prevenir el monitoreo no autorizado de la RC • Detección inmediata y automatizada de accesos no autorizados a la RC • Contraseñas que autoricen el acceso a la RC y eviten la entrada a archivos no autorizados • Otros 9 ¿Existen controles relativos a la seguridad física de los diversos componentes de la RC (tarjetas, terminales, manuales, software, documentación, etc.)? 9.1 En caso de contar con esos controles, ¿cómo se aseguran los responsables de darles seguimiento? 9.2 Verificar que estos controles cuenten con • Protección adecuada de los componentes de la RC (cables, tarjetas, terminales, servidores, etc.) • Guardias o personal que vigile el acceso al centro de telecomunicaciones • Bitácoras de acceso a las áreas conectadas a la RC • Métodos de control de acceso como pases, tarjetas de identificación, puertas de candados, monitores, entre otros • Listado de personal autorizado con acceso a las terminales y controladores de la RC • Otros			

(Continúa)

Cuadro 5.9. Programa de trabajo del área de Redes Locales y Telecomunicaciones

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	10 ¿Se tiene un seguro que proteja el software y el equipo de la RC? 11 ¿Hay alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en la RC 12 ¿Estos convenios están formalizados? 13 ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la RC de la empresa como las siguientes? • Evaluación periódica de la RC hardware, software, grado de satisfacción, grado de utilización etc • Acceso a la RC nuevos usuarios, niveles de acceso por perfil de usuario, asignaciones de software o datos para utilizar, consultar, modificar, borrar etc • Aspectos administrativos administrador u operadores (tareas, sueldos, capacitación, vacaciones, reemplazos, otros) • Capacitación, planeación, ejecución y actualización • Crecimiento de la RC multiplexores, enlaces, usuarios, módems y medios de transmisión • Respaldo datos, equipo medios de transmisión, software, por mencionar algunos • Seguridad controles, procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc • Otros que se consideren pertinentes 14 Elaborar cédula tipo de observaciones con las siguientes columnas: • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.10. Programa de trabajo del área de Hardware

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

HARDWARE

OBJETIVO: Conocer y verificar el nivel de uso del hardware de la empresa, a través de la revisión de la adquisición, instalación, operación, administración, mantenimiento y seguridad del mismo.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Asegurar que exista una función formal de administración del hardware 2 Asegurar la presencia de procedimientos y controles para • La administración del hardware • La instalación del hardware • La operación y seguridad del hardware • El mantenimiento del hardware 3 Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio el hardware existente 4 Comprobar que existan parámetros de medición del desempeño del equipo 5 Evaluar el grado de soporte que se brinda a los usuarios del equipo en el uso de sistemas y software al que tienen acceso 6 Determinar si existen los suficientes controles y procedimientos de seguridad para el hardware de la empresa	Administración 1 ¿La empresa cuenta con microcomputadoras, minicomputadoras o mainframes? 1.1 Si es así, ¿cuántos tipos de equipo tiene?(Mencionar sus características básicas, periféricos y atributos básicos de éstos) 1.2 ¿Qué software (paquetes, lenguajes, sistemas de información, sistemas operativos, bases de datos, etc.) hay instalados? ¿Cuáles son las versiones correspondientes? 1.3 ¿Existe una administración formal de equipo? 1.4 En caso de no tener una administración formal de equipo de cómputo, ¿con qué cuenta la empresa, esto es, cómo se da seguimiento a los siguientes aspectos? • Planeación de nueva tecnología de información (hardware, software, etc.) • Monitoreo de las actividades de la operación y mantenimiento del equipo • Procedimientos de control y seguridad del equipo • Aspectos legales del software instalado en los equipos • Capacitación y soporte a usuarios • Otros			

(Continúa)

Cuadro 5.10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
7. Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes del hardware 8. Asegurar que sólo se encuentre instalado software legalizado 9. Verificar si se cuenta con algún software que apoye el mantenimiento preventivo y correctivo de los diferentes elementos que componen el hardware del negocio 10. Evaluar el grado de compatibilidad e integridad entre microcomputadoras, minicomputadoras, mainframes y supercomputadoras de la empresa 6. Determinar si existen los suficientes controles y procedimientos de seguridad para la red de la empresa	15. Si no se cuenta con administración del hardware, ¿cuáles de las funciones a continuación mencionadas realiza, con qué tareas efectúa cada función y cómo les dan seguimiento sus coordinadores o jefes inmediatos ? Planeación • Defina un plan formal que contemple • Evaluación del hardware actual - Análisis y evaluación del equipo - Análisis y diagnóstico del número de equipos (por tipo), características, usuarios, etc. - Análisis y diagnóstico de periféricos - Otros • Evaluación del software actual - Análisis y diagnóstico del software instalado en los equipos de cómputo como graficadores, procesadores, etc. - Lenguajes de programación, sistemas operativos, etc. - Cantidad de licencias, copias pirata, versiones, número de usuarios - Software por legalizar - Otros • Estudio de justificación de instalación o reemplazo del equipo de cómputo - Hardware requerido: micro, periféricos, etc. - Configuración del equipo: distribución física, interfase, etc. - Software requerido: aspectos legales, lenguajes de programación, sistemas operativos, etc. - Evaluación costo beneficio - Procedimientos de capacitación, seguridad, operación mantenimiento, monitoreo, etc. Organización • Elaboración de políticas y procedimientos para • La evaluación de hardware, software, etc. del equipo • Adquisición o instalación de hardware o software • Asignación y baja de usuarios del hardware • Administración del equipo			

(Continúa)

Cuadro 5.10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Nivel de servicios para usuarios del equipo – Desempeño en tiempos de respuesta, proceso, atención a fallas y otros – Capacitación, soporte, mantenimiento del hardware, software y aplicaciones – Operación de equipo, software y aplicaciones – Seguridad de datos, software, hardware, aplicaciones y accesorios 2 ¿Algún personal externo interviene en la administración del equipo? 2.1 Si es así ¿quién y por qué? 3 ¿Existe la documentación formal que especifique qué hacer y cómo hacer cada una de las funciones de administración del equipo? 3.1 Si es así ¿Las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación? 4 En caso de que no exista esta documentación, ¿cómo se indica al personal responsable y a los usuarios lo referente a los puntos mencionados en la pregunta 1? 5 ¿Existe un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios? 6 ¿Cómo se canalizan las dudas, sugerencias y compromisos entre los usuarios y los responsables del equipo? 7 ¿Qué garantiza que se esta utilizando la tecnología del hardware más adecuada para la empresa? 8 ¿Hay análisis costo/beneficios de las diferentes estrategias de hardware implantadas? ¿Son aprobados de manera formal?			

(Continúa)

Cuadro $ 10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Instalación 1 ¿Existen procedimientos que aseguren la oportuna y adecuada instalación de los diferentes componentes del equipo conforme se realicen los contratos y compras formales de los mismos? 2 Mencione las actividades que se realizan durante el proceso de instalación de los componentes de la tecnología adquirida (hardware, software, procedimientos, etc.) 3 ¿Las compras de los diferentes elementos del equipo, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se asegura de que esto se cumple? 4 En caso de que las compras e instalación de componentes del equipo (sean microcomputadoras, minicomputadoras, software etc.) no hayan planeados formalmente, ¿cómo se justifican ante los responsables de informática y de las áreas usuarias involucradas en el uso de dicha tecnología? 5 En cuanto a la instalación de software, ¿cómo se asegura que haya sido comprado legalmente? ¿Cómo aseguran que no sea instalado en otros equipos de la empresa sin tener licencia de uso? ¿Qué hacen cuando detectan anomalías al respecto? 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección de dicho software? 6 Cuando la instalación parcial o total de cualquiera de los elementos que componen el equipo de cómputo es realizada por personal externo, ¿cómo se asegura la empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confidencialidad? 7. ¿Tienen alguna(s) referencia(s) que apoyen el proceso de instalación? Operación y seguridad 1. ¿Se cuenta con manuales de operación del equipo? ¿Contemplan aspectos de seguridad? 1.1 Si es así, ¿el personal responsable de administrarlo y operar el equipo fue capacitado y preparado para el manejo de la misma? ¿Da seguimiento a la seguridad? 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?			

(Continúa)

Cuadro 5.10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2 Indique si existen estándares relativos a la operación y administración como: • Estándares de desempeño • Tiempos de respuesta • Tráfico (volúmenes de información, velocidad) • Interrupciones • Tiempo de recuperación del equipo • Equipos o terminales interconectados • Otros • Estándares de mantenimiento • Calendarios (fechas, horarios, etc.) • Responsables • Otros 2.1 Si existen, ¿son aplicados formalmente por los responsables del equipo? 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos? 2.3 Una vez que se aplican estos estándares, ¿qué datos se envían a otras áreas (usuarios, auditoría en informática)? 2.4 ¿Los costos por el uso del equipo se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios? 2.5 ¿Existe otro procedimiento para definir los costos derivados por el uso del equipo? Si es así, ¿cuál es? 2.6 ¿El usuario aprueba formalmente este procedimiento de pago? 3 ¿Se desarrolló o adquirió algún cuestionario estándar que permita establecer el nivel de servicios que brindan las microcomputadoras, minicomputadoras o mainframes? 3.1 Si es así, ¿con qué periodicidad se distribuye este cuestionario a los usuarios o encargados del equipo? 3.2 ¿Qué indicadores o parámetros importantes salen de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática? 4 ¿Se tienen procedimientos que protejan los datos transmitidos de un equipo de cómputo a otro(s)? 4.1 Si se tienen, ¿cuáles son? 4.2 ¿Hay un responsable o un software de comunicaciones que vigile de manera permanente que los datos sean transmitidos con los estándares de oportunidad, fidelidad, exactitud y autenticación de un equipo a otro(s)? 4.3 ¿Se tienen registros con información relevante para el administrador del equipo o el auditor en informática?			

(Continúa)

Cuadro 5.10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4.4 Si es así, ¿contienen información relativa a los puntos siguientes? • Usuarios que accesaron los diferentes equipos de cómputo • Operaciones realizadas en el equipo (envío, recepción) • Tiempos de conexión • Interrupciones durante el uso del equipo • Causas • Tiempo para reiniciar cada interrupción • Terminales o equipos conectados • Accesos invalidados a los diferentes equipos • Terminales donde se llevaron a cabo estos accesos no autorizados • Otros 4.5 ¿Estos registros son generados por algún software o los producen de manera independiente los responsables de la misma? 5 ¿Se tiene identificada formalmente la siguiente información? • Usuarios del equipo • registros y niveles de acceso • Terminales conectadas en los diferentes equipos • Responsables del equipo • Procedimientos de contingencias • Software del equipo • Periféricos conectados a los equipos • Software original y pirata instalado en los equipos • Software duplicado de las micros • Tipos de CPU • Capacidad de discos o espacio libre por servidor y micros • Otros 5.1 ¿Estos registros son generados por algún software o por los responsables de la administración misma? 6 ¿Existe una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios del equipo? 7 ¿Se tiene un procedimiento formal para dar un servicio oportuno y eficiente a los requerimientos de los usuarios del equipo? 7.1 ¿Lo conocen los usuarios? 8 ¿Los equipos poseen controles de acceso a personas no autorizadas (equipo, datos y software)? 8.1 En caso de contar con esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado a los equipos?			

(Continúa)

Cuadro 5.10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	8.2 Si es así, ¿cuáles son estos controles y quiénes son los responsables de darles seguimiento? 8.3 Verificar que los controles contemplen al menos • Protección de archivos • Protección a programas fuente de las aplicaciones que están en los equipos • Protección a otro software alojado en los equipos • Métodos para prevenir el monitoreo no autorizado de la red • Detección inmediata y automatizada de accesos no autorizados a los equipos • Contraseñas que autoricen el acceso a los equipos, sin permitir la entrada a archivos no autorizados • Otros 9 ¿Existen controles relativos a la seguridad física de los diversos componentes del equipo (tarjetas, terminales, manuales, software, documentación, entre otros)? 9.1 En caso de contar con esos controles, ¿cómo se aseguran los responsables de darles seguimiento? 9.2 Verificar que estos controles cuenten con • Protección adecuada de los componentes del equipo (tarjetas, terminales, manuales, software, documentación entre otros) • Guardias o personal que vigile el acceso al centro de telecomunicaciones • Bitácoras de acceso a las áreas conectadas al equipo • Métodos de control de acceso como pases, tarjetas de identificación, puertas de candados, monitores, etc • Listado de personal autorizado con acceso a las terminales y controladores del equipo • Otros 10 ¿Se cuenta un seguro que proteja el software y el equipo? 11 ¿Se tienen alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en algunos de los equipos? ¿Tienen convenios con otras empresas? 12 ¿Estos convenios están formalizados? 13 Indique si se ha tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo del hardware instalado en la empresa como los siguientes • Evaluación periódica del equipo hardware, software grado de satisfacción grafo de riesgos, etc • Acceso a los equipos de nuevos usuarios niveles de acceso por perfil de usuario, asignar rutas de software o datos para utilizar, consultar, modificar, borrar etc			

(Continúa)

Cuadro 5.10. Programa de trabajo del área de Hardware

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Aspectos administrativos administrador u operadores, tareas sueldos, capacitación, vacaciones, reemplazos, entre otros • Capacitación, planeación, ejecución y actualización • Crecimiento del equipo periférico, memoria, usuarios software y aplicaciones • Respaldo datos, equipo, periféricos, software, aplicaciones, entre otros • Seguridad controles procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc • Otros que se consideren pertinentes 14 Elaborar cédula tipo de observaciones con las siguientes columnas: • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.11. Programa de trabajo del área de Software

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

SOFTWARE

OBJETIVO: Conocer y verificar el nivel de uso del software de la empresa, a través de la revisión de la adquisición, legalización, instalación, operación, capacitación, administración, mantenimiento y seguridad del mismo.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Asegurar que exista una función formal de administración del software 2 Asegurar la presencia de procedimientos y controles para • La administración del software • La instalación del software • La operación y seguridad del software • El mantenimiento del software 3 Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio el software existente 4 Investigar si hay políticas que aseguren un proceso formal de • Evaluación y selección del software por comprar • Contratos que aseguren la legalización, instalación, capacitación y actualización oportuna del software adquirido por la empresa • Seguimiento a las normas de utilización del software legal, no de copias • Evaluación permanente del software existente en el mercado	Administración 1 ¿La empresa cuenta con microcomputadoras, minicomputadoras o mainframes 1.1 ¿Existe un documento que muestre la distribución del equipo y sus usuarios? 1.2 ¿Qué software (paquetes, lenguajes, sistemas de información, sistemas operativos, bases de datos, etc.) hay instalados)? ¿Cuáles son las versiones correspondientes? 1.3 ¿Existe una administración formal del software? ¿Quién es el responsable? 1.4 En caso de no tener una administración formal, indique como se da seguimiento a los siguientes aspectos • Planeación de nueva tecnología de información (hardware, software, etc.) • Monitoreo de las actividades de manejo y actualización del software • Procedimientos de control y seguridad • Aspectos legales del software instalado • Otros			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
• Evaluación permanente de nuevos requerimientos de software en el negocio 5. Evaluar el grado de soporte que se brinda a los usuarios en el uso del software al que tienen acceso en los equipos de la empresa 6. Determinar si existen los suficientes controles y procedimientos de seguridad para el software de la empresa 7. Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes del software 8. Asegurar que sólo se encuentre instalado software legalizado 9. Verificar si se cuenta con algún sistema o paquete computacional que apoye el monitoreo y auditoría de los diferentes elementos que componen el software instalado en los equipos del negocio 10. Evaluar el grado de compatibilidad e integridad entre los diferentes tipos de software instalado en las computadoras del negocio	1.5 Si se tiene tal administración, ¿cuáles de las funciones listadas a continuación realiza, con que tareas efectúa cada función y como les da seguimiento sus coordinadores o jefes inmediatos? Planeación • Definir un plan formal que contemple • Evaluación del software actual – Análisis y diagnóstico del software instalado en los equipos de cómputo (graficadores, procesadores, etc.) – Lenguajes de programación, sistemas operativos, etc. – Cantidad de licencias, copias pirata, versiones, número de usuarios – Grado de satisfacción de los usuarios – Requerimientos no satisfechos – Costo beneficio del software actual – Software por legalizar – Otros • Evaluación del hardware actual – Distribución y ubicación del equipo donde está instalado el software (microcomputadoras, red, minis, mainframes) – Características (memoria, RAM, etc • Estudio de justificación de instalación o reemplazo del software – Software requerido (aspectos legales, paquetes de cómputo, lenguajes de programación, sistemas operativos, etc.) – Hardware requerido (micros,periféricos, etc.) – Evaluación costo beneficio – Procedimientos de capacitación, seguridad, operación mantenimiento, monitoreo, etc Organización • Elaboración de políticas y procedimientos para • La evaluación del software • Adquisición o instalación • Autorización de usso • Administración del software • Soporte a usuarios capacitación, soporte y actualización • Manejo de software • Seguridad: acceso al software, modificación o destrucción			•

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2 ¿Hay personal externo que intervenga en las funciones de administración mencionadas? 2.1 Si es así, mencione su especialización y por qué participa 3 ¿Existe la documentación formal que especifique qué hacer y cómo llevar a cabo cada una de las funciones de administración del software? 3.1 Si es así ¿Las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación? 4 En caso de que no exista esta documentación, ¿cómo se invica al personal responsable y a los usuarios lo referente a los puntos mencionados en la pregunta 1? 5 ¿Existe un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios? 6 ¿Como se canalizan las dudas, sugerencias y compromisos entre los usuarios y los responsables de la administración del software? 7 ¿Qué les garantiza que se está utilizando el software idóneo? 8 ¿Existen análisis costo/beneficio de las diferentes estrategias de software implantadas? ¿Se han aprobado formalmente?			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Legalización e instalación 1 ¿Existen procedimientos que aseguren la oportuna y adecuada instalación del software conforme se hayan realizado los contratos y compras formales del mismo? 2 Mencione las actividades que se realizan durante el proceso de instalación de la tecnología adquirida (hardware, software, procedimientos etc.) 3 ¿Las compras del software, así como su instalación, se derivan de un proceso de planeación y evaluación formal ? ¿Cómo se aseguran de que esto se cumpla? 4 En caso de que las compras e instalación del software no hayan sido planeadas formalmente, ¿cómo se justifica esto ante los responsables de informática y de las áreas usuarias? 5 En cuanto a la instalación de software, ¿cómo se aseguran de que éste haya sido comprado legalmente? ¿Cómo previenen que no sea instalado en otros equipos de la empresa sin licencia de uso? ¿Qué hacen cuando detectan anomalías al respecto? 5.1 ¿Quien es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección dicho software? 6 Cuando son terceros (personal externo) los encargados de la instalación del software, ¿cómo se asegura la empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confidencialidad? 7 ¿Tienen alguna(s) sugerencia(s) que apoyen el proceso de instalación? **Operación y seguridad** 1 ¿Se cuenta con manuales de operación? ¿Contemplan aspectos de seguridad? 1.1 Si es así, ¿el personal responsable de administrar o manejar el software fue capacitado y preparado para el manejo del mismo? ¿Se da seguimiento a la seguridad? 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Legalización e instalación 1 ¿Existen procedimientos que aseguren la oportuna y adecuada instalación del software conforme se hayan realizado los contratos y compras formales del mismo? 2 Mencione las actividades que se realizan durante el proceso de instalación de la tecnología adquirida (hardware, software, procedimientos, etc.) 3 ¿Las compras del software, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla? 4 En caso de que las compras e instalación del software no hayan sido planeadas formalmente, ¿cómo se justifica esto ante los responsables de informática y de las áreas usuarias? 5 En cuanto a la instalación de software, ¿cómo se aseguran de que éste haya sido comprado legalmente? ¿Cómo previenen que no sea instalado en otros equipos de la empresa sin licencia de uso? ¿Qué hacen cuando detectan anomalías al respecto? 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección dicho software? 6 Cuando son terceros (personal externo) los encargados de la instalación del software, ¿cómo se asegura la empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confidencialidad? 7 ¿Tienen alguna(s) sugerencia(s) que apoyen el proceso de instalación? **Operación y seguridad** 1 ¿Se cuenta con manuales de operación? ¿Contemplan aspectos de seguridad? 1.1 Si es así, ¿el personal responsable de administrar o manejar el software fue capacitado y preparado para el manejo del mismo? ¿Se da seguimiento a la seguridad? 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2 Indique si existen estándares relativos a la operación y administración como • Programas de capacitación ◦ Calendario de cursos ◦ Costo de los cursos ◦ Material empleado en los cursos ◦ Lugares donde se impartirán los cursos ◦ Evaluación de los cursos ◦ Otros • Estándares de actualización ◦ Calendarios (fechas, horarios, etc.) ◦ Software por actualizar o reemplazar ◦ Responsables ◦ Otros 2.1 Si existen estos estándares, ¿son apegados formalmente por los responsables del software? 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos? 2.3 Una vez que se aplican estos estándares, ¿qué datos relativos a los resultados de los mismos se envían a otras áreas (usuarios, auditoría en informática, entre otros)? 2.4 ¿Los costos por el uso del software se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios? 2.5 ¿Existe otro procedimiento para establecer los costos derivados por el uso del software? Si es así, ¿cuál es? 2.6 ¿El usuario aprueba formalmente este procedimiento de pago? 3 ¿Se desarrolló o adquirió algún cuestionario estándar que permita saber el grado de utilización o satisfacción relativos al software? 3.1 Si es así, ¿con qué periodicidad se distribuye este cuestionario a los usuarios o encargados del software? 3.2 ¿Qué indicadores o parámetros importantes salen de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática? 4 ¿Se tienen procedimientos que protejan los datos transmitidos de un equipo de cómputo a otro(s) generados por el uso del software? 4.1 Si se tienen ¿cuáles son? 4.2 ¿Hay un responsable o un software de comunicaciones que revise permanentemente que los datos sean transmitidos con los estándares de oportunidad, totalidad, exactitud y autorización de un equipo a otro(s)? 4.3 ¿Existen registros con información relevante para el administrador del equipo o el auditor en informática?			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4.4 Si es así, señale si contienen información relativa a • Usuarios que accesaron a los diferentes tipos del software (usuarios, programadores, otros) • Operaciones realizadas en la red (envío, recepción) • Interrupciones en el uso del equipo donde está instalado el software • Causas • Tiempo para recuperar cada interrupción • Accesos invalidados a los diferentes tipos de software • Terminales donde se llevaron a cabo estos accesos no autorizados • Usuarios que intentaron estos accesos • Otros 4.5 ¿Estos registros son generados por algún software o por los responsables de la misma? 5. Informe si se tiene identificada formalmente la siguiente información • Usuarios • Registros y niveles de acceso • Equipos donde se encuentra instalado cada tipo de software • Periféricos conectados a dichos equipos • Software original y pirata instalados en los equipos • Otros 5.1 ¿Estos registros son generados por algún software o los responsables del mismos? 6. ¿Se cuenta con una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios ? 7. ¿Existe un procedimiento formal para dar servicio oportuno y eficiente a los requerimientos de los usuarios? 7.1 ¿Lo conocen los usuarios? 8. ¿Los equipos tienen controles de acceso a personas no autorizadas (equipo, datos y software)? 8.1 En caso de contar con esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado a los diferentes tipos de software?			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	8.2 Si es así, ¿cuáles son estos controles y quienes le dan seguimiento? 8.3 Verificar que los controles contemplen al menos • Protección de archivos • Protección a programas fuente de las aplicaciones que están en los equipos • Protección a otro software alojado en los equipos • Métodos para prevenir el monitoreo no autorizado del equipo • Detección inmediata y automatizada de accesos no autorizados a los equipos • Contraseñas que autoricen acceso a los equipos y eviten el acceso a archivos no autorizados • Otros 8.4 Verificar que estos controles cuenten con • Bitácoras de acceso a las áreas donde se encuentre el equipo y el software • Métodos de control de acceso como pases, tarjetas de identificación, puertas con candados, monitores, etc. • Listado de personal con acceso autorizado a las terminales y controladores del equipo • Otros 9 ¿Se tiene un seguro que proteja el software y el equipo? 10 ¿Se tienen alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en algunos de los equipos? ¿Cuenta con convenios con otras empresas? 12 ¿Estos convenios están formalizados? 13 Indique si se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo del software instalado en la empresa como las siguientes • Evaluación periódica del software y el equipo donde está instalado hardware, software, grado de satisfacción, grado de utilización, etc. • Acceso a los equipos nuevos usuarios, niveles de acceso por perfil de usuario, asignaciones de software o datos por utilizar, consultar, modificar, borrar, entre otros			

(Continúa)

Cuadro 5.11. Programa de trabajo del área de Software

NO.	OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
		• Aspectos administrativos administrador u operadores (tareas, sueldos, capacitación, vacaciones, reemplazos, otros) • Capacitación planeación, ejecución y actualización • Crecimiento del equipo periféricos, memoria, usuarios, software y aplicaciones • Respaldo datos equipo medios de transmisión, software, por mencionar algunos • Seguridad controles procedimientos, software de auditoría, niveles de acceso, planes de contingencia plan de reinicialización y recuperación etc • Otros que se consideren pertinentes 14 Elaborar cédula tipo de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.12. Programa de trabajo del área de Seguridad

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

SEGURIDAD

OBJETIVO: Conocer y verificar el nivel de seguridad de los recursos informáticos de la empresa, a través de la revisión de las medidas de seguridad implantadas referentes a respaldos de información, sistemas, plan de contingencias, políticas y procedimientos.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Verificar que existan los planes, políticas y procedimientos relativos a la seguridad dentro de la organización 2 Confirmar que exista un análisis costo/beneficio de los controles y procedimientos de seguridad antes de ser implantados 3 Comprobar que los planes y políticas de seguridad y de recuperación sean difundidos y conocidos por la alta dirección 4 Evaluar el grado de compromiso por parte de la alta dirección, los departamentos usuarios y el personal de informática con el cumplimiento satisfactorio de los planes, políticas y procedimientos relativos a la seguridad 5 Asegurar la disponibilidad y continuidad del equipo de cómputo el tiempo que requieran los usuarios para el procesamiento oportuno de sus aplicaciones	Hardware 1 ¿Hay políticas y procedimientos relativos al uso y protección del hardware de la organización? 1.1 Si existen, indique si están formalmente identificados los siguientes aspectos de seguridad • Administración del hardware • Micros, minis y supercomputadoras (mainframes) • Tecnología de comunicaciones, redes, etc • Cuantificación del hardware • Descripción del hardware • Distribución del hardware • Áreas de informática, departamentos usuarios y áreas locales y remotas • Registro del hardware instalado, dado de baja, en proceso de adquisición, etc • Uso del hardware: desarrollo, operación, mantenimiento, monitoreo, toma de decisiones • Funciones responsables del control del hardware • Otros • Procedimientos y controles de seguridad para la evaluación, selección y adquisición de hardware • Políticas enfocadas a computar que el software adquirido cubra los siguientes puntos			

(Continúa)

Cuadro 5.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
6 Asegurar que las políticas y procedimientos brinden confidencialidad a la información manejada en el medio de desarrollo, implantación, operación y mantenimiento 7 Verificar que exista la seguridad requerida para el aseguramiento de la integridad de la información procesada en cuanto a totalidad y exactitud 8 Constatar que se tiende la seguridad necesaria a los diferentes equipos de cómputo que existen en la organización 9 Comprobar que existan los controles de seguro necesarios para el hardware y software de la empresa 10 Confirmar la presencia de una función responsable de la administración de la seguridad en: • Recursos humanos, materiales y financieros relacionados con la tecnología de información • Recursos tecnológicos de información	• Módulos de seguridad acceso al hardware (llaves de seguridad), uso del hardware(facilidades de monitorear la operación) y bitácoras de uso del hardware (quién, cuando), para que, entre otros puntos) • La actualización del hardware • Políticas orientadas a confirmar que el hardware actualizado cubra los siguientes puntos • Autorización del hardware por medio de la justificación de la actualización • Impacto de la implantación del hardware en el medio de informática aplicaciones, software y costos • Implicaciones de control en la implantación y uso del hardware actualizado • Reemplazo del hardware. • Políticas para verificar que el hardware reemplazado cubra los siguientes puntos • Autorización por medio de la justificación del reemplazo • Impacto de la implantación en el medio de informática aplicaciones, hardware y costos • Implicaciones de control en la implantación y uso del hardware nuevo 2 En cuanto al equipo de soporte, se han de tener los siguientes datos: • Localización física de • Aire acondicionado • Equipo No-Break • Equipos contra incendios • Otros 3 ¿La ubicación física del equipo de cómputo en el edificio es la más adecuada pensando en los diversos desastres o contingencias que se pueden presentar (manifestaciones o huelgas, inundaciones, incendios, otros) 4 ¿Hay procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de desastres o contingencias? 5 Indique si se cuenta con controles y procedimientos para: • Clasificación y justificación del personal con acceso a los centros de cómputo del negocio y a las oficinas donde se encuentra papelería o accesorios relacionados con informática • Restringir el acceso a los centros de cómputo sólo al personal autorizado • Definición y difusión de las horas de acceso al centro de cómputo.			

(Continúa)

Cuadro 5.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Uso y control de bitácoras de acceso a los centros de cómputo • Definir la aceptación de la entrada a visitantes • Manejo de bitácoras especiales para los visitantes a los centros de cómputo 6 ¿Existe personal de seguridad encargado de la salvaguarda de los equipos de cómputo de la empresa? 6.1 ¿Fue capacitado el personal para este trabajo? 6.2 Si no se cuenta con tal personal ¿A que área o función pertenecen los responsables de proteger físicamente el equipo? 7 Mencione si existen políticas relacionadas con el ingreso y salida del hardware que aseguren al menos lo siguiente - • Que la entrada y salida del hardware sea • Revisada • Justificada • Aprobada por el responsable de información a que va a resultarlo • Registrada • Devuelta • Devuelta en las mismas condiciones de entrada • Devolución autorizada por medio de un responsable de informática 8 ¿Existe alguna función de investigación, auditoría o seguridad que se dedique a la evaluación permanente de software, métodos, procedimientos, etc., sugeridos en el mercado para la implantación de nuevas acciones relativas a la seguridad que brinden continuidad en la operación y cuidado de los recursos relacionados con informática? 8.1 Si es así ¿Cuáles son las actividades principales que se asignan a esta área? 8.2 En caso de que lo anterior no ocurra ¿Qué acciones garantizan la adecuación de los controles y procedimientos de seguridad en el momento de implantar nuevas tecnologías? Aplicaciones del software. 1 ¿Se tienen políticas y procedimientos relativos al uso y protección del software existente? 1.1 Si existen, indique si están formalmente identificados los siguientes aspectos de seguridad • Administración del software • Sistemas operativos, utilerías, paquetes, etc. etc • Cuantificación del software			

(Continúa)

Cuadro 5.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Descripción del software (por original) • Distribución del software (en que equipos o dispositivos de almacenamiento secundario se encuentra, en que lugar físico se localizan) • Registro del software instalado, dado de baja, en proceso de adquisición, etc • Uso del software tipo de uso, responsables de su uso, entre otros puntos • Procedimientos y controles de seguridad para la evaluación, selección y adquisición de software • Políticas enfocadas a comprobar que el software adquirido cubra los siguientes puntos • Módulos de seguridad acceso al software), uso del software y bitácoras de uso del software (quién, cuándo, para qué, entre otros puntos) • La actualización del software • Políticas orientadas a confirmar que el software actualizado cubra los siguientes puntos • Autorización del software por medio de la justificación de la actualización • Impacto de la implantación del software en el medio de informática: aplicaciones, hardware y costos • Implicaciones de control en la implantación y uso del software actualizado • Reemplazo del software actual por otro • Políticas para asegurar que el software reemplazado cubra con los siguientes puntos • Autorización por medio de la justificación del reemplazo. • Impacto de la implantación en el medio de informática: aplicaciones, hardware y costos • Implicaciones de control en la implantación y uso del software nuevo 2 Diga si poseen políticas relacionadas para el ingreso y salida del software que aseguren al menos lo siguientes • Que el software que salga de la empresa sea • Revisado (contenido, cantidad, destino) • Esté registrado formalmente en la empresa • Justificado • Aprobado por el responsable de informática que va a recibirlo • Registrado (quién y a qué hora lo sacó)			

(Continúa)

Cuadro 5.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Devuelto (comparar con fecha estimada de devolución) • Devuelto en las mismas condiciones en que salió • El personal esté comprometido formalmente a no hacer mal uso del mismo (copiarlo, dañarlo, modificarlo, etc.) • Que el software que ingrese a la empresa sea • Revisado (contenido, cantidad, destino) • Justificado (evaluación, prueba o respaldo de las aplicaciones del negocio) • Aprobado por el responsable de informática • Registrado (quien y a qué hora lo metió) • Devuelto (comparar con fecha estimada de devolución) • Devuelto en las mismas condiciones en que salió • El personal esté comprometido formalmente a no hacer mal uso del mismo (copiarlo, dañarlo, modificarlo, etc.) 3 En cuanto a las aplicaciones (sistemas de información) que se desarrollan en la empresa, ¿se tienen los controles y procedimientos necesarios para garantizar la seguridad mínima requerida? 3.1 En caso de que existan ¿Al menos contemplan lo siguiente? • Procedimientos de llenado de documentos fuente • Procedimientos de uso de la computadora • Encendido e inicialización del equipo • Reinicialización del equipo en caso de fallas • Manejo de bitácoras de uso de la computadora • Monitoreo de uso de la computadora • Niveles de acceso a los módulos de • Captura • Actualización • Consulta • Generación de reportes • Respaldos • Otros • Procedimientos de uso de los módulos de: • Captura • Actualización • Consulta • Generación de reportes • Respaldos • Otros			

(Continúa)

Cuadro 5.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	4 ¿Existen procedimientos que verifiquen que la construcción (programación), prueba e implantación de los controles y procedimientos de seguridad sean formalmente aprobados antes de que se utilice el sistema? 5 ¿Participan funciones de control o evaluación de sistemas, como auditores o consultores, en la aprobación de los controles de seguridad de los sistemas antes de que sean formalmente aprobados por los usuarios? 6 Mencione si los controles aseguran que el sistema contemple los procedimientos necesarios para que la información manejada en el mismo sea total exacta, autorizada, mantenida y actualizada 6.1 ¿Existen procedimientos para comprobar que los totales de los reportes de validación del usuario concuerden con los totales de validación del sistema computarizado? 6.2 ¿Los documentos fuente por capturar llevan preimpresos sus números consecutivos o se los asigna el usuario? Si ocurre lo último, ¿hay alguno de los controles mencionados a continuación dentro del sistema que valide la no repetición o exclusión de algún número consecutivo? • Control de disquetes, cintas, papelería, etc. • Control de todos los movimientos o transacciones rechazadas por el sistema (comprobar que los datos erróneos para el sistema sean registrados, corregidos, alimentados correctamente y actualizados) • Entendimiento y buen uso de los mensajes del sistema, como manejo de errores • Uso de bitácoras por parte de usuarios y personal de informática como pistas para auditoría 6.3 ¿Cómo se aseguran que durante la operación del sistema se den los controles mencionados en el punto 6? 6.4 ¿Cómo se aseguran que al estar el sistema en operación se cumplan formal y oportunamente los procedimientos de seguridad contemplados en el desarrollo del mismo? a) Con una auditoría de sistemas b) Con revisiones de consultores externos c) Con revisiones del personal de informática 6.5 ¿Cómo se aseguran de que los manuales de usuario, técnicos y de operación cumplan con los estándares de la metodología de CVDS y de que sean completos? 6.6 ¿Cómo se aseguran de que el personal que va a utilizar estos manuales se encuentre capacitado en el uso de los mismos?			

(Continúa)

Cuadro 6.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	6.7 ¿Se documentan todas las debilidades derivadas de la revisión del cumplimiento de controles y procedimientos de seguridad durante la operación de los sistemas? 6.8 Si es así, indique si los clasifican en: • Debilidades en los procedimientos de entrada, proceso o salida • Entendimiento o manejo del equipo donde se encuentran los sistemas • Dificultades en la comunicación usuarios-informática para el manejo de nuevos requerimientos o cambios a los sistemas • Otros 7. En cuanto al mantenimiento de sistemas señale si se cuenta con un procedimiento formal para asegurar que los cambios efectuados en los sistemas sean: • Justificados (ejemplo a los requerimientos de usuarios) • Descritos (objetivos, función, etc.) • Probados en el área de desarrollo antes de ser trasladados al área de producción • Revisados por funciones de control (auditoría de sistemas, consultores entre otros) • Aprobados por los responsables correspondientes • Registrados en bitácoras de cambios • Actualizados en la documentación correspondiente, como manuales de usuario, técnicos y de operación • Implantados los controles de seguridad de dichos cambios 8. ¿Hay un procedimiento formal para asegurar que los requerimientos de los departamentos usuarios sean registrados, justificados, programados, probados e implantados de acuerdo con los estándares de la metodología del CVDS? 9. ¿Cómo se da seguimiento a los cambios de los sistemas sugeridos por la función de informática? 10. ¿Existen procedimientos que permitan identificar con claridad las responsabilidades en cuanto al uso del sistema y equipo de cómputo donde será implantado y operado? 11. ¿Qué procedimiento se utiliza para liberar formalmente el sistema? 11.1 Indique si se registran todos los sistemas liberados y aprobados formalmente por los usuarios, auditores, función de informática, consultores, etc. 12. Una vez que el sistema está en operación, ¿Qué funciones verifican que los controles y procedimientos relativos a la seguridad se cumplan de manera satisfactoria?			

(Continúa)

Cuadro 5.12. Programa de trabajo del Área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	13 ¿Los responsables de modificar los programas fuente del sistema en operación están bien definidos? 13.1 Si es así, ¿cómo se aseguran de que sólo ellos tengan acceso a dichos programas? 13.2 ¿Cómo se aseguran que sólo se modifiquen programas autorizados en términos formales y que se documenten en los manuales correspondientes? 13.3 ¿Cómo se aseguran los responsables de estos cambios de incluir los controles de seguridad? 14 ¿Hay un registro de los archivos existentes en cada sistema en operación (maestros y de movimientos)? 14.1 Si es así, ¿existe un procedimiento que asegure que sólo sean accesados por personal autorizado? 14.2 ¿Se tiene algún procedimiento para especificar cuáles funciones se actualizarán, consultarán o eliminarán información de los archivos de los sistemas en operación? 14.3 ¿Están clasificados los procedimientos para actualizar archivos en línea o lote? 15 ¿Se cuenta con procedimientos de respaldo de los programas fuente, de la documentación y de los archivos en operación? 16 ¿El respaldo de la información se encuentra en el mismo edificio? 17 ¿Sucede lo mismo con el equipo de cómputo?			

(Continúa)

Cuadro 6.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	18 ¿Se tienen controles para que sólo el personal autorizado tenga acceso a dichos respaldos? **Plan de contingencia y de recuperación.** 1 ¿Considera que tanto la alta dirección, usuarios como el personal de informática están conscientes de que todos los recursos relacionados con la informática son activos del negocio y deben protegerse de una manera formal y permanente? ¿Por qué? 1.1 ¿Cuáles de los siguiente recursos vinculados con informática son más importantes para la organización y cuáles tienen más y mejores métodos de protección para seguir operando y apoyando los objetivos del negocio en condiciones óptimas? • Humanos • Materiales • Financieros • Tecnológicos • De información 1.2 ¿Existen planes de contingencia y de recuperación de operaciones para casos de contingencia o desastres? 1.3 Indique si dichos planes contemplan los siguientes aspectos: • Red de comunicaciones (RC) • Hardware • Software, aplicaciones, datos • Recursos Humanos • Lugares físicos donde se localizan los recursos anteriores • Otros 1.4 Si es así, ¿fueron difundidos formalmente en toda la organización? 1.5 ¿Fueron elaborados por terceros, personal de informática, usuarios o se trato de un proyecto donde intervinieron varias áreas del negocio? 2 En el proceso de planeación de contingencias y recuperación y de su implantación en la empresa, indique cuáles fueron las tareas realizadas, cuáles están pendientes, cuáles en desarrollo y quiénes son sus responsables 2.1 ¿ Se han presentado contingencias que hayan sido enfrentadas con el plan de contingencias y de recuperación diseñado para la empresa?, ¿con que resultados?			

(Continúa)

Cuadro 5.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	2.2 Si no tienen este plan, ¿qué acciones han tomado para enfrentar tales eventualidades y quiénes han sido los responsables de ejecutarlas? 3 Señale si poseen una función responsable de seguridad que verifique y de seguimiento a los siguientes puntos • Actualización formal de los planes • Capacitación a los usuarios y personal de informática en cuanto a la aplicación de los procedimientos contemplados en los planes • Supervisión y orientación en la ejecución de simulacros • Asignación de los responsables de la ejecución de las actividades contempladas en los planes para • Prevención de contingencias • Apoyo a la empresa en casos de desastres o de contingencias con el fin de reducir en lo posible las pérdidas humanas, equipos, datos, etc • Reanudo inmediato o en el tiempo mínimo posible de las operaciones de la empresa 4 ¿Las funciones involucradas en dichos planes los han probado? 5 ¿Contemplan todas las contingencias o desastres probables en la localidad donde tienen instalaciones la organización (huelgas, diluvios, robos, incendios, otros)? 6 ¿Los planes cubren los procedimientos necesarios para prevenir los elementos causales o restaurar los primordiales? 7 ¿Se clasifican el orden en que reiniciará la operación de cada aplicación de acuerdo con las prioridades y estrategias del negocio? 8 ¿Existen acuerdos con empresas o proveedores que tengan la misma tecnología o que sea compatible? 9 Mencione si se cuenta con contratos legales que aseguren los siguientes elementos de la función de informática y de los departamentos usuarios • Personal (de informática y usuarios), equipos de cómputo, software, aplicaciones, telecomunicaciones, edificios o instalaciones, entre otros 10 ¿Existe algún procedimiento formal para efectuar todo el proceso de evaluación, selección y contratación de los seguros? ¿Cuáles son dichos procedimientos? 10.1 ¿ Quiénes llevaron o están llevando a cabo la negociación de los seguros? 10.2 ¿En este proceso intervienen expertos en la evaluación de riesgos (administrador, responsables de seguridad, auditores en informática, especialistas o expertos financieros)?			

(Continúa)

Cuadro 6.12. Programa de trabajo del área de Seguridad

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	10.3 ¿Qué plazos de cobertura marcan estos seguros? 10.4 ¿Se tienen previstas acciones legales para proceder posibles incumplimientos por parte de las compañías aseguradoras? 11 ¿Existe una clasificación de los elementos prioritarios para que la operación de los sistemas básicos no se interrumpa por un desastre o contingencia? 11.1 Indique si la clasificación contempla los siguientes elementos equipo de cómputo, archivos, programas fuentes, lenguajes de desarrollo, sistemas operativos, documentación, personal, entre otros 12 Elaborar cédula tipo de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.13. Programa de trabajo del área de Planeación

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

PLANEACION

OBJETIVO: Conocer y verificar los planes, procedimientos y estrategias para el desarrollo de la infraestructura informática de la empresa, a través de la revisión de métodos, técnicas y herramientas de planeación y aceptación de proyectos.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1. Detectar la existencia, formalización y conocimiento de la planeación de informática en las áreas claves del negocio 2. Verificar que la planeación de informática haya sido evaluada y aprobada por la alta dirección 3. Comprobar que la planeación de informática se enfoque en el soporte de los objetivos, planes, políticas y estrategias de la empresa 4. Evaluar el grado de compromiso por parte de la alta dirección con informática para determinar si el apoyo que brinda a la planeación de informática es el adecuado 5. Confirmar la existencia de una metodología en informática 6. Investigar si existen técnicas y herramientas de productividad para el desarrollo del plan 7. Comprobar que exista un proceso formal de capacitación para el entendimiento y manejo satisfactorio de la metodología de planeación en informática	Metodología 1. ¿Existe en su área una metodología para la planeación de informática? 1.1 ¿Esta metodología contempla que hacer, quién debe hacerlo y cuándo debe hacerse durante los proyectos de planeación de informática? 1.2 Si es así, indique si también abarca los pasos y lineamientos requeridos para la siguiente clasificación de proyectos • Planeación de sistemas de información por desarrollar e implantar (corto, mediano y largo plazos) • Desarrollo e implantación de sistemas de las diferentes áreas del negocio • Compra e implantación de aplicaciones de mercado • Adaptación de aplicaciones adquiridas a externos • Proyectos de telecomunicaciones • Proyectos de investigación tecnológica • Proyectos de evaluación y selección de proveedores de productos y servicios • Proyectos de desarrollo e implantación de sistemas estratégicos de información para toma de decisiones • Proyectos de auditoría y evaluación de informática • Proyectos de desarrollo e implantación de planes de contingencia y recuperación • Proyectos de capacitación o actualización ejecutiva, técnica y de usuarios			

(Continúa)

Cuadro 5.13. Programa de trabajo del área de Planeación

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
8 Evaluar el grado de cumplimiento de la metodología, técnicas y herramientas en el proceso de planeación de informática 9 Comprobar si la alta dirección, los responsables de las áreas usuarias y los responsables de informática se han involucrado en el proceso de planeación de informática 10 Verificar si se da cumplimiento a los proyectos surgidos del plan de informática 11 Evaluar el grado de dominio que tiene el personal de informática sobre la metodología , técnicas y herramientas de productividad que utilizan para el desarrollo del plan de informática 12 Valorar el nivel de estandarización que tiene la metodología de planeación de informática con respecto a las aceptadas comunmente en el mercado	• Rediseño de sistemas existentes • Desarrollo e implantación de sistemas integrales en el negocio • Aseguramiento de calidad • Otros relacionados con la función de informática 1.3 ¿Está documentada formalmente dicha metodología? 1.4 Si es así, indique si cubre cada uno de los siguientes puntos • Un panorama general de la metodología • Equipos de trabajo sugeridos según el tipo de proyecto • Etapas de la metodología • Tareas de cada etapa • Secuencia de las etapas y tareas • Responsables e involucrados en cada etapa y tarea • Productos terminados por cada etapa o tarea • Requerimientos técnicos y administrativos para el cumplimento de cada tarea • Revisiones formales e informales sugeridas para cada etapa • Duraciones estimadas de cada etapa del proyecto • Consideraciones para proyectos especiales 2 ¿Cómo se aseguran un compromiso formal, un desarrollo y seguimiento eficientes, así como la aprobación final de los proyectos si no se cuenta con una metodología que contenga lo mencionado en las preguntas 1.3, 1.4, y 1.5? 3 En caso de contar con una metodología de planeación de informática, ¿Está fue desarrollada por personal de informática de la empresa, se compró o se tenía cuando se requiere? 3.1 ¿Se capacitó al personal de desarrollo en el entendimiento y uso práctico de la misma? 3.2 Indique si la capacitación fue impartida de manera formal por grupos de trabajo o individualmente y con casos prácticos o proyectos piloto 3.3 ¿Se evaluó el grado de asimilación de la metodología? ¿Cómo? 3.4 Si no se capacitó al personal en el uso de la metodología, ¿cómo se asegura su entendimiento y uso eficiente durante los proyectos? 3.5 ¿Desde cuándo están usando dicha metodología? 3.6 ¿Se capacita al personal de desarrollo de reciente ingreso a la empresa en el entendimiento y uso de la metodología? ¿Se contemplan los puntos mencionados en la pregunta 3.2? 3.7 ¿Se actualiza la metodología cuando es necesario?			

(Continúa)

Cuadro 5.13. Programa de trabajo del área de Planeación

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CEDULA DE REF.	INVOLUCRADOS
	3.8 ¿Que actividades de investigación o consulta se realizan para formular cambios o adaptaciones en la metodología? 3.9 ¿Se documentan formalmente estos cambios? 3.10 ¿Quien aprueba los cambios a la metodología? 3.11 ¿Capacitan formalmente al personal en lo referente a la actualización de la metodología? 4 ¿Existe una congruencia de la metodología de planeación de informática con las metodologías recomendadas como estándares en el mercado? 5 ¿Cómo se aseguran de que las metodologías de planeación de informática compradas o rentadas a externos satisfagan los requerimientos del negocio? 6 Mencionar cuales son las etapas, tareas, productos y los responsables del proceso de planeación de informática, que se lleva en la empresa 6.1 Las etapas mencionadas deben cubrir al menos los siguientes aspectos • Estudio de la situación actual y tendencias de los aspectos culturales, tecnológicos y económicos, entre otros • Análisis de la competencia: fortalezas, debilidades, imagen, aspectos financieros, etc • Expectativas y grado de satisfacción de los clientes: productos, servicios, expectativas, oportunidades • Evaluación de la situación actual del negocio: aspectos culturales, tecnológicos y económicos, sistemas de información, fortalezas y debilidades • Análisis de los planes del negocio: metas, objetivos, planes tácticos y estratégicos, etc • Evaluación de cada una de las áreas del negocio en aspectos relativos a sistemas de información, tecnología, proyectos estratégicos, entre otros • Elaboración y formulación del plan de informática • Proyectos tácticos y estratégicos que cubran los siguientes puntos: ▪ Sistemas de información, administración de la función, equipos de cómputo, telecomunicaciones, auditoría de informática, evaluación y adquisición de productos y servicios, proyectos conjuntos alta dirección -informática, proyectos conjuntos entre usuarios e informática, etc.			

(Continúa)

Cuadro 5.13. Programa de trabajo del área de Planeación

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	Técnicas 1. ¿El personal de informática sabe cuáles son las técnicas requeridas para el desarrollo seguimiento y documentación de las etapas de planeación de informática? 1.1 ¿Existen dichas técnicas para la planeación de informática en la empresa? 1.2 ¿Se capacita formalmente al personal de desarrollo de sistemas en el uso y aplicación de estas técnicas? 1.3 ¿Se capacita al personal recien contratado en el manejo de las mismas? 1.4 ¿Qué procedimiento utilizan para la capacitación del personal de desarrollo en el uso de metodologías y técnicas? 2 Explique cuáles de las técnicas siguientes son usadas en el desarrollo de sistemas por su empresa • Listas de verificación • Entrevistas • Listas de verificación de aseguramiento de calidad • Control de proyectos • Análisis organizacional (sistemas de negocio) • Análisis costo / beneficio • Documentación • Diagramación • Modelación de datos y procesos • Investigación • Manejo de equipos de trabajo • Otros (especifique) 3 ¿Quiénes y cómo determinaron cuáles eran las técnicas requeridas para el desarrollo e implantación de sistemas de información del negocio? 3.1 ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique? **Herramientas** 1. ¿Existe una clasificación de las herramientas de productividad (hardware, software, manuales) utilizadas por su empresa en la planeación de informática? 1.1 Si es así, ¿Podría indicar cuáles de los siguientes utilizan en su empresa?			

(Continúa)

Cuadro 5.13. Programa de trabajo del área de Planeación

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Procesadores de palabras • Hojas electrónicas • Graficadores • Diagramadores • Presentadores • Generadores de Aplicaciones • Generadores de bases de datos • Ingeniería de software • Indicadores de productividad (benchmarking) • Otros (especifique) 1.3 ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique? **Capacitación/actualización** 1. Mencione si existen procedimientos formales para capacitar al personal de planeación de informática (o puestos equivalentes) en • Entendimiento y aplicación de metodología de planeación de informática • Técnicas para efectuar las etapas de la planeación de informática • Herramientas de productividad requeridas en la planeación de informática 1.2 ¿Se documentan dichos procedimientos? 1.3 ¿Hay un responsable directo de elaborar, actualizar, documentar y definir estos procedimientos de capacitación? 1.4 ¿Cómo se asegura el cumplimiento oportuno de tales procedimientos? 1.5 Si existen ¿Al menos contemplan lo siguiente? • Calendarios de los cursos • Responsables de impartir los cursos • Puestos o funciones que requieren dichos cursos • Costos estimados de los cursos • Beneficios esperados de cada curso • Parámetros de medición para asistentes y expositores • Material requerido para cada curso • Responsables de la organización de los cursos 2. Si no se tienen un proceso formal de capacitación ¿Cómo se da seguimiento al entendimiento, uso y actualización oportuna de la metodología, técnicas y herramientas de productividad requeridas por parte del personal durante la planeación de informática?			

(Continúa)

Cuadro 5.13. Programa de trabajo del área de Planeación.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	• Procesadores de palabras • Hojas electrónicas • Graficadores • Diagramadores • Presentadores • Generadores de Aplicaciones • Generadores de bases de datos • Ingeniería de software • Indicadores de productividad (benchmarking) • Otros (especifique) 1.3 ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique? Capacitación/actualización 1. Mencione si existen procedimientos formales para capacitar al personal de planeación de informática (o puestos equivalentes) en • Entendimiento y aplicación de metodología de planeación de informática • Técnicas para efectuar las etapas de la planeación de informática • Herramientas de productividad requeridas en la planeación de informática 1.2 ¿Se documentan dichos procedimientos? 1.3 ¿Hay un responsable directo de elaborar, actualizar, documentar y definir estos procedimientos de capacitación? 1.4 ¿Cómo se asegura el cumplimiento oportuno de tales procedimientos? 1.5 Si existen ¿Al menos contemplan lo siguiente? • Calendarios de los cursos • Responsables de impartir los cursos • Puestos o funciones que requieren dichos cursos • Costos estimados de los cursos • Beneficios esperados de cada curso • Parámetros de medición para asistentes y expositores • Material requerido para cada curso • Responsables de la organización de los cursos 2. Si no se tienen un proceso formal de capacitación ¿Cómo se da seguimiento al entendimiento, uso y actualización oportuna de la metodología, técnicas y herramientas de productividad requeridas por parte del personal durante la planeación de informática?			

(Continúa)

Cuadro 5.13. Programa de trabajo del área de Planeación

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
	3 ¿El responsable de informática está consciente de la importancia que tienen la actualización y mejoramiento continuos del personal de desarrollo de sistemas de información para la implantación de soluciones del negocio? 4 Cuando intervienen terceros (personal externo) en proyectos de planeación de información ¿Cómo se aseguran de que la metodología, técnicas y herramientas de productividad que usan cubran por lo *menos* los estándares (o normas) mínimos de la empresa? ¿Qué se hace si la organización no tiene dichos estándares definidos? 5 Elaborar cédula tipo de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener: encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

Cuadro 5.14. Programa de trabajo del área de Investigación

	FIRMA	FECHA
ELABORÓ		
REVISÓ		
EMPRESA		

INVESTIGACION

OBJETIVO: Conocer y verificar el nivel de investigación tecnológica en la empresa, a través de la revisión del seguimiento que se da a los proyectos de actualización de área de informática, su aprobación, justificación y documentación.

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
1 Verificar si existe una función formal de investigación tecnológica dentro del área de informática 2 Detectar el grado de confianza satisfacción y respaldo que brinda al negocio la función de investigación tecnológica 3 Verificar que exista una clasificación y entendimiento de los servicios y productos que proporciona al negocio la función de investigación tecnológica 4 Determinar las acciones emprendidas por la función de investigación tecnológica para que la tecnología de información se encuentre al alcance de las diferentes áreas de la empresa que así lo requieran 5 Comprobar que exista un análisis costo beneficio de los proyectos propuestos por la función de investigación tecnológica que justifiquen su aprobación antes de ser implantados 6 Constatar que los proyectos de investigación tecnológica sean resultado del plan de informática	1. ¿Existe una clasificación de los principales productos y servicios proporcionados por el área de investigación tecnológica? 1.1 Si es así ¿Cuáles son? 1.2 Si no tienen esta clasificación ¿Cómo justifican su función ante el responsable de informática y la alta dirección? 1.3 ¿Cómo estiman los proyectos futuros en • Tipo de proyectos tareas, tiempos • Recursos • Responsables 2 ¿Existe una descripción formal de la función de investigación tecnológica? 2.1 Si es así, ¿Dicha descripción contempla tareas, actividades, responsabilidades, entre otros? 2.2 Si no se tiene esta descripción, ¿Cómo se administra la función? 3 ¿Existe un proceso metodológico para desempeñar la función de investigación? ¿Cuáles? 3.1 ¿Está dicho método de trabajo documentado formalmente? 3.2 Si no existe un método específico de trabajo, ¿Cómo se desarrolla esta función? 4 ¿Existen políticas y procedimientos específicos para las tareas y actividades de investigación? ¿Se cuenta con técnicas y herramientas para el desarrollo de las mismas? ¿Cuáles son? 5 Indique si los proyectos de investigación están contemplados en el plan de informática Si no es así, ¿Cómo los justifican?			

(Continúa)

Cuadro 6.14. Programa de trabajo del área de Investigación

OBJETIVOS	CUESTIONARIO DE EVALUACIÓN	COMENTARIOS	CÉDULA DE REF.	INVOLUCRADOS
7 Evaluar el grado de compromiso de la alta dirección con los proyectos de investigación que informática considera estratégicos para el negocio	6 Elaborar cédula tipo de observaciones con las siguientes columnas • Referencia • Observación • Consecuencia • Sugerencia • Comentado con			

NOTA: Todas las cédulas deberán contener encabezado, índice, significado de marcas, cruces con cédulas analíticas, programa de trabajo y cédula de observaciones, objetivo, conclusión y observación en caso que proceda

CONCLUSIONES

Como resultado de nuestra investigación, nos dimos cuenta de que una parte muy importante en la labor de un informático, es la de cuidar el uso de los recursos de cómputo de una organización. Actualmente esta función ha tomado mucha importancia, ya que día con día salen modelos nuevos de equipos y la competencia en cómputo entre las empresas de software, manejadores de bases de datos, equipo portátil, equipo propietario, servidores, etc., se hace globalmente más fuerte. Asimismo podemos hablar de que el fenómeno de penetración de las computadoras en las empresas, dado principalmente por la automatización de procesos y el surgimiento de las computadoras personales, comenzó hace poco más de 20 años, de una manera acelerada y vertiginosa, provocando en muchos de los casos que las organizaciones obtuvieran buenos equipos, pero no buenas soluciones.

Estas mismas empresas otorgaron su confianza a personal que por su experiencia y desarrollo profesional, conocían, en ese preciso momento, como utilizar una computadora. La experiencia (muchas veces empírica) de estas personas, les daba la capacidad de ofrecer a sus organizaciones, opciones de desarrollo prácticas, pero incompletas. ¿Qué queremos decir con "incompletas"?, pues bien, la falta de una formación administrativa, en lo que se refiere al manejo de los recursos informáticos, hacía que los objetivos del negocio se lograran con práctica y errores, más que con una planeación y metodología formal.

Pero aún con esto, el fenómeno de automatización de empresas ha continuado hasta llegar a nuestros días en los cuales sigue siendo factor determinante el conocer qué soluciones implantar y cómo evaluar su utilidad final. Lo que sucede, es que en realidad son muchos los aspectos que se deben cuidar para dar verdaderas soluciones de negocio a las empresas; recursos materiales, equipos, administración de proyectos, estándares, plataforma, procedimientos internos, sólo son algunos ejemplos; en la realidad es enorme la labor de un encargado de sistemas.

Es por esto que el informático debe apoyarse ampliamente en la auditoría en informática, ya que le permitirá darse cuenta de qué errores se cometen en la administración de recursos humanos, materiales y financieros dentro de la organización. Todo es tan simple como pensar ¿qué deseo como empresario?, ¿un área de informática que tenga el mejor equipo de cómputo, pero que haga los procesos más tardados a que si fueran manuales?, ¿que cause igual o más costos que la misma área de producción y en la cual no pueda prescindir del personal de informática porque se han convertido en "Gurus" de los sistemas de la empresa y si se van ellos, mueren las aplicaciones?, o ¿prefiero un área con organización y procedimientos bien definidos, un uso formal de estándares, difusión en las labores y servicios del área, planeación de soluciones a corto y largo plazo y sobre todo que los recursos humanos, materiales y financieros se usen para lograr los objetivos de la organización de manera controlada y organizada para convertir el área de informática en un área de apoyo pleno a la toma de decisiones y generadora de verdaderas soluciones de negocio?.

Pero la importancia de la auditoría en informática no recae sólo en esto, también el uso incorrecto de los recursos es algo que nos brinda un área de oportunidad para que, como gente de informática, logremos hacer comprender a las empresas que la computación es una herramienta que necesita planeación y organización y no es únicamente, la magias del sonido, los modelos futuristas, las impresionantes imágenes fotográficas y la comunicación virtual.

En los últimos años la evolución que ha sufrido todo lo relacionado a cómputo ha provocado dos fenómenos. Por un lado los fabricantes de hardware han logrado disminuir los costos de equipos, se han especializando en desarrollo de microcomputadoras y piezas de hardware cada vez más pequeñas logrando que las industrias, comercios, organizaciones y entidades públicas se inunden de pequeños equipos llamados PC's.

Estos proveedores proponen en el mercado soluciones corporativas basadas en redes LAN con servidores y muchas PC's conectadas a ellos. Los servidores son capaces de trabajar como servidores de Web al mismo tiempo que alojan las bases de datos y los sistemas más grandes de la compañía. Las soluciones ahora están encaminadas a tener plataformas pequeñas y consistentes que permitan a casi cualquier compañía mediana contar con la suya.

El segundo fenómeno, ligado en muchos aspectos al primero, consiste en los desarrollos cada vez más variados y polimorfos, de hardware, software y aditamentos de multimedia. Los juegos, la realidad virtual, el software educativo, las aplicaciones disponibles en internet, las videoconferencias, el software de diseño profesional y arquitectónico y el software para desarrollo artístico, provocan que se vea al cómputo como la herramienta más versátil, lujosa y atractiva de nuestros días.

En ningún momento tratamos como exagerados estos avances que indiscutiblemente son útiles y permiten que cada día más gente desarrolle de mejor manera su actividad profesional. Pero veamos que ha provocado este desarrollo

Por experiencia propia, nos hemos dado cuenta que usuarios faltos de una visión informática, aseguran cien por ciento que siempre es mejor una computadora multimedia a una que no lo es, ¿por qué?, sólo por los sonidos, los movimientos al ingresar a los sistemas, los colores, etc. Además ¿mejor en qué?, la gente de desarrollo por ejemplo, sabe que los sonidos y adornos que agrega a un sistema son sólo eso, impactos a la vista de un usuario incauto que preferirá ese sistema a uno que tal vez optimise mejor los recursos pero no sea tan vistoso. Por ejemplo, no es la misma utilidad la que se le da a una unidad lectora de CD-ROM en un servidor donde se necesitan sistemas imposibles de instalar con disquetes, a la de una PC que lo usa para cargar juegos y tocar CD de música y video para la recreación familiar.

El fenómeno se puede identificar mejor de la siguiente manera, los proveedores de soluciones agregan a sus equipos las mayores posibilidades de recursos multimedia para hacerlos doblemente atractivos al mercado y crear un impacto a la gente en cuanto a lujosidad y exclusividad, en equipos que realmente deben ser vistos como herramientas de trabajo. Ahora junto al estéreo, a la televisión y la videocasetera, se tiene una PC para acompletar la diversión.

Una problemática real se origina cuando esto es visto así no en una casa, sino en una empresa, la cual invierte millones de pesos para adquirir equipos que podrán tocar 4 CD y presentar videos e imágenes excelentemente nítidas, pero que se usan para hacer documentos simples en Word tan sólo de 9 de la mañana a 3 de la tarde. ¿Qué paso con la inversión?, ¿Se justifica?, ¿Es mejor una máquina multimedia que una que no lo es, tan sólo para hacer un documento?

Si no se hacen estudios de costos, de factibilidad, de recuperación de inversión y no se entiende que debe existir una reglamentación de adquisiciones de cómputo, será fácil que las empresas se preocupen más por tener lo "último" , que por tener lo más útil.

De aquí surge la verdadera oportunidad que vimos en proponer una metodología de trabajo que permita al informático verificar el verdadero cumplimiento de objetivos del negocio por medio de la adecuada aplicación de los recursos informáticos. Por lo anterior, nuestro trabajo es una propuesta formal del trabajo que se debe seguir en la revisión de una unidad de informática de cualquier empresa, sin intentar decir que esta propuesta sea universal y para todos los casos, es realmente una metodología moldeable a las características de:

- El medio informático en el que se desarrolle la auditoría
- Las innovaciones tecnológicas de la empresa
- El tamaño de la empresa
- Los alcances del contrato de prestación de servicios y el addendum
- El giro de la empresa

Una aportación del presente trabajo que, a consideración nuestra, resulta relevante destacar, es el manejo que proponemos del desarrollo de una auditoría en informática. No se puede negar el origen contable de la auditoría en informática, igualmente es inegable la liga que se tiene entre los procedimientos, métodos y objetivos de la auditoría tradicional y ésta. Pero ¿a qué grado debemos "conectar" las dos disciplinas?, creemos que esto puede ser tema de todo un tratado en informática, pero en este trabajo de investigación proponemos aspectos importantes al respecto. Para nosotros, que contamos ya con una formación profesional y conocemos el trabajo que generalmente desarrolla un informático, nos es factible proponer una metodología para el desarrollo de la auditoría en informática.

En nuestra propuesta de una metodología de desarrollo de la auditoría en informática, logramos, una metodología de desarrollo de una auditoría en informática que tiene sus bases en dos partes: la metodología de investigación y la metodología de desarrollo de sistemas. Para nosotros, fundamentar nuestra metodología en estos dos aspectos, fundamentales en la formación de un informático, unido a los ya existentes procedimientos para realizar auditorías tomados de algunos organismos, hacen que el objetivo de nuestro trabajo sea cumplido perfectamente.

Es también importante destacar que el manejo de áreas de oportunidad, que proponemos en nuestra investigación es el que encontramos más adecuado al ámbito de desarrollo de un informático en una organismo de talla comercial, productora, bancaria y de fines sociales. Con esto no afirmamos que sean las únicas y que siempre serán igual de adaptables a los formatos propuestos y a los conceptos evaluados por nosotros, acentuamos únicamente que el informático no debe perder su panorama administrativo-contable y técnico, no podemos decir que un informático deba conocer la estructura interna de un sistema operativo, pero si su uso; planeación de su adquisición, ventajas que aporta al negocio y administración de los usuarios que utilizan sus recursos, en conclusión, no debemos tomar al informático como el técnico, ni como el desarrollador y mucho menos como el experto en aplicaciones de oficina. El informático es la persona ideal para la administración de los recursos y proyectos, que de manera automática con el uso del computador, brinde a las compañías que lo contraten, soluciones de negocio a corto, mediano y largo plazo.

BIBLIOGRAFÍA

Aguirre Martínez, Eduar.?. Segundad Integral en las Organizaciones // Eduardo Aguirre Martinez -- México: TRILLAS, 1986.-- 222p.

Alcalde Lancharro, Eduardo y otros autores Informática Básica // Eduardo Alcalde Lancharro -- México: McGRAW-HILL, 1992 -- 247p.

Baena Paz, Guillermina. Instrumentos de Investigación. Manual para elaborar trabajos de investigación y tesis profesionales // Guillermina Baena Paz -- México. Editores Mexicanos Unidos S.A., Doceava Edición, 1984.-- 134p.

Defliese, Philip L. Auditoría Montgomery // Philip L. Defliese. Versión en español: Ricardo Calvet Pérez.-- México: LIMUSA GRUPO NORIEGA EDITORES, Segunda Edición, 1991 -- 1008p.

Echenique García, José A. Auditoría en Informática // José A. Echenique García.-- México: McGRAW-HILL INTERAMERICANA, 1990 -- 203p

Fine, Leonard H. Seguridad en centros de cómputo. Políticas y procedimientos // Leonard H. Fine.-- México: Trillas, 1988 -- 130p.

Freeman, Alan. Diccionario de Computación.// Alan Freeman.-- México: McGRAW-HILL, 1993.--

Hernández Hernández, Enrique Auditoría en Informática. Un Enfoque Metodológico y Práctico // Enrique Hernández Hernández -- México. COMPAÑÍA EDITORIAL CONTINENTAL, 1996.--

Hernández Jiménez, Ricardo. Administración de Centros de Cómputo // Ricardo Hernández Jiménez.-- México: TRILLAS, --

Instituto Mexicano de Contadores Públicos. Normas y procedimientos de auditoría // Instituto Mexicano de Contadores Públicos.-- México: IMCP, Decimosexta Edición, 1996

Levine Gutiérrez, Guillermo. Introducción a la Computación y la Programación Estructurada // Guillermo Levine Gutiérrez -- México: McGRAW-HILL , 1984 -- 284p

Mendivil Escalante, Victor M. Elementos de Auditoría // Victor M. Mendivil Escalante.-- México: ECASA, Cuarta Edición, Duodécima Reimpresión, 1993 -- 199p.

Meigs, Walter B. Principios de auditoría // Walter B. Meigs. Traducción: Gabriel Heffes.-- México: DIANA, 1971 -- 974p

Orilia, Lawrence S. Las Computadoras y la Información // Lawrence S. Orilia.-- México: McGRAW-HILL, --

Radlow, James Informática: las computadoras en la sociedad // James Radlow. Traducción: María de Lourdes Fournier G.-- México: McGRAW-HILL, 1988 -- 510p.

Ruiz de Velasco, Luis y otros autores. Auditoría Práctica // Luis Ruiz de Velasco.-- México: EDITORIAL BANCA Y COMERCIO, Decimoprimera Edición, 1995.-- 585p.

Sánchez Alarcón, Fco. Javier. Programas de Auditoría // Fco. Javier Sánchez Alarcón.-- México: ECASA, Séptima Edición, 1995 -- 202p.

Sanders, Donald H. Informática: Presente y Futuro.// Donald H. Sanders. Traducción. Roberto Luis Escalona.– México: McGRAW-HILL, 1988.– 887p.

Sanders, Donald H. Informática: Presente y Futuro // Donald H. Sanders. Traducción: María de Lourdes Fournier G.-- México: McGRAW-HILL, 1983.-- 670p.

Secretaría de la Presidencia, Dirección General de Estudios Administrativos. Metodología de Investigación en Organización y Métodos.// Secretaría de la Presidencia, Dirección General de Estudios Administrativos.-- México: Secretaría de la Presidencia, Segunda Edición, 1973 -- 58p.

Willingham, John J. Auditoría Conceptos y Métodos // John J. Willingham. Traducción. Jesús Villamizar Herrera.-- México: McGRAW-HILL, 1988.-- 466p.

HEMEROGRAFÍA

Díaz Llorca, Carlos La Auditoria Informática: un Diagnóstico. //Carlos Díaz Llorca -- Economía y Desarrollo.-- México: Vol. 70, Septiembre- Octubre 1982.-- pág. 108-121

Ibarra Zavala, Alonso y Media García, Gabriel Importancia del Equipo de Infraestructura en el Funcionamiento de un Centro de Cómputo.// Alonso Ibarra Zavala y Gabriel Media García.-- Comunidad Informática.-- México: INEGI, Vol. 10, No. 31, Año X, Octubre-Diciembre 1987.-- pág. 21-26.