UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE CONTADURIA PUBLICA
Y ADMINISTRACION
DIVISION DE POST-GRADO

AUDITORIA DE INFORMATICA
(UN ENFOQUE METODOLOGICO)

T E S I S

PARA OBTENER EL GRADO DE
MASTER EN INFORMATICA ADMINISTRATIVA

P R E S E N T A

LIC. ENRIQUE HERNANDEZ HERNANDEZ

MONTERREY, N. L. JULIO DE 1993.

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE CONTADURIA PUBLICA

Y ADMINISTRACION

DIVISION DE POST-GRADO

AUDITORIA DE INFORMATICA

(UN ENFOQUE METODOLOGICO)

T E S I S

PARA OBTENER EL GRADO DE

MASTER EN INFORMATICA ADMINISTRATIVA

P R E S E N T A

LIC. ENRIQUE HERNANDEZ HERNANDEZ

MONTERREY, N. L. JULIO DE 1993.

Agradecimientos :

A mi esposa Vicky : Por ser la mujer que me enseño el camino de la verdad y del amor, sin ella lo que soy hubiera tardado en ser o nunca hubiera sido, con ella el valor y la alegria encuentro al extender mi mano, gracias mi vida, por los hijos, comprensión y amor que me haz dado

A mis hijos : Enriquito, te dedico con todo mi corazón éste trabajo, muchas líneas, fueron impresas por la inspiración que me brindas cada día, seguiré luchando gracias al ejemplo que me diste, lo bueno de mi vida es para tí

Carlos Antonio y Erick Ivan : Cada mañana despierto pensando en la felicidad y fortaleza que me brindan, los admiro por su vitalidad, por ser como son, vale la pena recalcar que mi objetivo principal es y será darles cada día el mejor ejemplo, mi apoyo y mi amor incondicional.

A mi madre : Por iniciarme en los estudios, por motivarme a continuarlos y por ser fuerte y comprensiva para levantarme cuando me caí, por darme el valor y conciencia para terminarlos. Usted ha sido siempre ejemplo de rectitud, sencillez y honestidad, es támbien para usted dedicado el presente trabajo, con mucho amor y eterno agradecimiento

A mis hermanos: Me dieron siempre alegrias, sus recuerdos me siguen dando alegrias, ustedes me conocen y saben que mucho los quiero y los recuerdo

A mis amigos : ¿Recuerdan nuestros retos? sigamos luchando por cumplirlos

A mis maestros : Mucho de ustedes va en mi mente y mi trabajo, gracias por su ejemplo

A mis alumnos : Sin ustedes no existen escuelas ni maestros ni progreso, muchas gracias

A mis escuelas : Ahí creci, me eduque, me forme, lo malo lo tire y lo bueno a la práctica llevaré, opciones de vivir muchas encontré, pero siempre por los estudios me incliné, a mis hijos lo mismo inculcaré. Gracias.

A Dios : Por permitirme la oportunidad de vivir y dar mi granito de arena

T E S I S :

AUDITORIA DE INFORMATICA

(UN ENFOQUE METOLOGICO)

FACULTAD DE CONTADURIA PUBLICA Y DE ADMINISTRACION

DIVISION DE POSTGRADO

MAESTRIA DE INFORMATICA ADMINISTRATIVA

LIC. ENRIQUE HERNANDEZ HERNANDEZ

CONTENIDO : **Página**

INTRODUCCION

1. ANTECEDENTES

1.1. OBJETIVOS

INTRODUCCION

El presente trabajo fue elaborado debido a la gran inquietud y necesidad que existe en los medios educativos de nivel profesional y postgrado de contar con un proceso de Auditoría de Informática formal, práctico y eficiente para la evaluación de la Función de Informática en el planteamiento oportuno de las recomendaciones y cursos de acción requeridos para dar una solución integral a los negocios aprovechando las áreas de oportunidad que emergen de dicho proceso.

El proceso metodológico aquí planteado fué desarrollado en base a una extensa ejecución de la Auditoría de Informática de acuerdo a los estandares y procedimientos recomendados por las Asociaciones nacionales e internacionales de Auditoría, de Informática y de la conjunción de ambas, las de Auditoría de Informática.

Así mismo se realizo una investigación detallada del material existente en México y Estados Unidos relacionados con la Auditoría en Informática, Esta integrado tambien por cuestionarios y formatos prácticos, que brindarán a los Auditores en Informática elementos para cubrir de manera satisfactoria los tópicos de Auditoría, Seguridad y Control inherentes a la Función de Informática.

Cabe señalar que va inmerso en este trabajo una serie de experiencias asimiladas con el desempeño diario de la Auditoría de Informática y que han brindado a las empresas y centros educativos la facilidad de entender este proceso obteniendo del mismo grandes beneficios para el mejoramiento continuo de la Informática.

Deseo brindar a la institución, así como a sus alumnos y maestros un método derivado de mis conocimientos y vivencias profesionales un proceso formal para la planeación y/o ejecución de la Auditoría o Evaluación en las areas mas relevantes de la Función de Informática, para que pueda ser discutido en nuestras aulas.

Una gran cantidad de alumnos que he tenido el gusto de asesorar a traves de mi estancia en ésta escuela ha desarrollado proyectos de Auditoría en Informática en empresas de los diversos sectores concluyendo con acciones y recomendaciones de mejoramiento y reposicionamiento de la Función de Informática con una aprobación formal de cada uno de los estudios realizados por los estudiantes.

Los cuestionarios y formatos que aquí recomiendo son resultado de un analisis detallado, que busca simplemente hacer mas util y amigable el uso de los mismos.

1. ANTECEDENTES

Desde que el uso de la Informática se enfocó al apoyo de la sistematización de las áreas del negocio, se empezarón a implantar Aplicaciones administrativas como la Contabilidad, la Nómina, Etc. dando inicio a lo que se conocio como la Auditoría a Sistemas de Información.

Posteriormente, el uso de la Informática se extendio a todas las áreas de negocio en todos los niveles, con productos y servicios muy variados, proliferarón las minicomputadoras o equipos departamentales, despues las microcomputadoras o computadoras personales, entraron de lleno las Redes Locales, la Integración de las empresas a traves de las Telecomunicaciones y un gran número de componentes de tecnología que imposibilitaron materialmente al responsable de Informática y a los Auditores de Sistemas tradicionales a seguir evaluando este campo con métodos y procedimientos ordinarios.

Se hizo entonces necesario un replanteamiento del fondo y forma de la Auditoría de Informática, mi trabajo entre otros própositos busca darle una dimensión más realista y adecuada a la Auditoría de Informática.

Se espera de cada alumno interesado en el campo que hoy me ocupa a un auditor profesional, experto, pero sobre todo un ser flexiblemente humano que entienda el contexto real del negocio. Será su principal objetivo darle la dimensión justa a cada problemática conviertiendola en área de oportunidad y orientarla a una solución de negocio.

Debemos recordar que en los negocios existen objetivos cómunes para todas lás áreas respecto a los recursos de Informática, por ejemplo sería el relacionado con el logro del máximo uso y aprovechamiento de los Recursos de Informática mediante políticas, procedimientos y métodos apropiados, siendo la Función de Auditoría de Informática uno de los medios más importantes y especializados para apoyarnos en la obtención permanente de dicho fin.

Surgimiento de la Auditoría de Informática en el tiempo :

En los años cuarentas empezarón a darse resultados relevantes en el campo de la computación, con sistemas de apoyo para estrategias militares entre otros, posteriormente se vino incrementando el uso de las computadoras y sus aplicaciones.

Se diversifico el apoyo a otros sectores de la sociedad: Educación, Salud, Industrial, Politico, Banca, Aeronautica, Comercio, Etc.

En aquellos años la seguridad y control de ese medio ambiente se limitaba a dar custodia física a los equipos y a permitir el uso de los mismos por personal altamente calificado (no había un gran número de usuarios ya sea técnicos o administrativos).

Actualmente el medio ambiente de la Informática se ha extendido a todas las ramas de la sociedad, es tan factible controlar un vuelo espacial por medio de una computadora, como seleccionar las compras del hogar desde una microcomputadora.

Esta rapidez en el crecimiento de la Informática nos orilla a deducir que los beneficios se han incrementado con la misma velocidad, algunos con mediciones tangibles como reducción de costos e incremento porcentual en ventas y otros con aspectos intangibles como mejora en la imagen, obtención de productos de más calidad pero ambos con la misma importancia que permiten seguir impulsando la investigación y actualización constante de dicha Tecnología.

La idea de que se obtienen beneficios en mayor grado y magnitud que antes no está tan lejos de la realidad, sin embargo es tán valido afirmar que los costos han sido altos y en muchas ocasiones rebasado los límites esperados, ocasionando grandes perdidas y decepciones en las diferentes áreas usaurias de las empresas.

A pesar de lo anterior el futuro que se vislumbra a corto y mediano plazo, es que las empresas sigan invirtiendo en Informática, así como en la Seguridad requerida.

Las empresas y organismos interesados en que la Informática siga creciendo para beneficio de la humanidad (Educación, Productividad, Calidad, Ecología, Etc.) desean que dicho crecimiento sea controlado y orientado de una manera profesional, se debe obtener un resultado planeado y esperado de cada inversión en esta rama.

Asegurar que todas las inversiones y proyectos inherentes a la Función de Informática sean justificados y brinden los resultados esperados es una responsabilidad de todo aquel que administre dicha función.

Con el paso de los años la Informática y todos los elementos tecnológicos que la rodean han ido creando una necesidad en cada sector en la sociedad y se ha vuelto un requerimiento permanente para el logro de soluciones.

Por ejemplo la Manufactura, Finanzas, Ventas, así como las funciones internas de los sectores Educativos o Comerciales, se encuentran buscando la manera de integrar los diversos elementos de Informática, que se hayan diseminados a traves de toda la organización, además desean comunicarse con otras entidades externas, como proveedores, clientes y sectores de gobierno, lo que implica inversión de tiempo, recursos y una planeación y evaluación formal de dicho proceso de cambio.

A continuación se describen algunas consideraciones que podemos asegurar son ya una realidad.

* Todas las actividades de la sociedad buscan apoyarse de alguna forma con la Tecnología de Informática
* Se piensa que las Computadoras y Aplicaciones deben estar al alcance de todos
* Equipos de Cómputo de diferentes Marcas y capacidades, así como las Bases de Datos y los Sistemas de Información deben ser una solución integrada.
* La capacitación debe ser permanente en el uso de la Tecnología de Informática debido a su constante crecimiento y actualización
* Hardware, Software, Telecomunicaciones y otros medios electrónicos deben Integrarse para explotar al máximo las bondades que ofrecen y dar soluciones a todos los sectores de la sociedad.
* Integrar a la comunidad de manera permanente a las Asociaciones profesionales relacionadas con Informática
* Alta penetración de la Informática en todos los niveles del sector educativo, así como en los sectores sociales y culturales.
* El control y seguridad sobre todos los recursos de Informática es una necesidad.
* Se debe evaluar de manera formal y periodica a la Función de Informática
* El proceso de planeación de los negocios debe integrar de manera permanente a la Función de Informática.
* Otros.

El incremento permanente de las expectátivas y necesidades hacia Informática, al igual que la actualización continua de los elementos que componen dicha Tecnología orilla a los negocios a contar con controles, políticas y procedimientos que aseguren a la Alta Dirección que los Recursos involucrados sean debidamente protegidos y garantizar que se orienten a la contribución de la rentabilidad y competitividad del negocio.

Si la respuesta a alguna(s) de las siguientes preguntas es negativa es conveniente reafirmar o considerar la necesidad de asumir la responsabilidad de un control y seguridad permanente sobre los recursos de Informática :

* ¿Conocen los usuarios y Alta Dirección la situación actual de la Función de Informática en la empresa (Organización, Políticas, Servicios, Etc.) ?
* ¿Se aprueban formal y oportunamente el costo /beneficio de cada proyecto de Informática ?
* ¿Son las Areas críticas del negocio apoyadas por Informática ?
* ¿Conoce el Responsable de Informática los requerimientos actuales y futuros del negocio que deben apoyarse en los servicios y productos de su area ?
* ¿Existe un entendimiento de los problemas y causas existentes en Informática?

Cada una de esas preguntas encierra una importancia específica para el buen funcionamiento de Informática en cualquier negocio, sin embargo todas las preguntas estan interrelacionadas y la negación de alguna de ellas es una pequeña fuga de gas que con el tiempo y un pequeño chispazo pueden ocasionar graves daños a los negocios, sean estos traducidos en fraudes, proyectos cancelados con alto porcentaje de costos no recuperables, rechazo de los servicios de Informática por los usuarios claves del negocio, improductividad y baja calidad de los recursos de Informática, planes de Informática no orientados a las metas y estrategias de negocio, Pirateria de Software, Fuga de Información a la competencia o proveedores, etc.

1.1. Objetivos :

- Plantear a maestros y estudiantes un proceso metódico para el entendimiento de la planeación, el desarrollo e implementación de la Auditoría de Informática.

- Brindar a los estudiantes un método estructurado y práctico que permite el ejercicio práctico de dicho proceso metodológico en las aulas.

- Facilitar el procedimiento metodológico asimilado a lo largo de mis experiencias como consultor de empresas, catedrático y estudiante en diversas instituciones profesionales a los diferentes alumnos que lo requieran con fines académicos.

- Es una finalidad prioritaria del presente trabajo apoyar a los catedráticos en la actualización de sus temarios relacionados con el tema que hoy me ocupa, así mismo se busca impulsar en los estudiantes de las áreas relacionadas con la Informática un sentimiento conciente de la necesidad e importancia que tiene el control y la seguridad de los diferentes recursos humanos y financieros involucrados con Informática.

2. Terminología de la Auditoría de Informática

2.1. Informática

2.2. Auditoría

2.3. Auditoría de Informática

2. Terminología de la Auditoría de Informática

Las definiciones y conceptos mencionados a continuación corresponden a las experiencias y conocimientos adquiridos a traves del tiempo en el desarrollo de actividades profesionales y/o estudiantiles, seminarios, cursos, etc.

2.1. Informática :

La Informática se desarrolla en base a normas, procedimientos y técnicas definidas formalmente por Institutos establecidos a nivel nacional e internacional.

En base a lo anterior solo mencionaremos algunos aspectos de Informática necesarios para el entendimiento ya supuestamente asimilados por los usuarios de este libro, sin embargo recomendamos leer los libros sugeridos en la bibliografia, asi como la participación más directa y activa en los institutos o asociaciones relacionadas con el campo de la Informática.

A. Campo que se encarga del estudio y aplicación práctica de la Tecnología, Métodos, Técnicas y Herramientas relacionadas con las computadoras y manejo de la información por medios electrónicos.

B. Son aquellas Areas de la Tecnología de Información orientadas al buen uso y aprovechamiento de los Recursos Computacionales para asegurar que la información de las organizaciones fluya en las organizaciones (Entidades internas y externas de los negocios) de manera oportuna, veraz y confiable.

Hardware : ***Componentes físicos/tangibles de las computadoras,*** **generalmente clasificadas en CINCO grandes ramas :**

- Microcomputadoras - Redes (Locales, remotas, etc.)
- Minicomputadoras - Supercomputadoras (Mainframes) - Periféricos

Software : ***Parte no física de las computadoras, esto significa que es la porción no tangible de los equipos de computo, son un conjunto de programas con orientaciones especificas para la administración y uso eficiente de los recursos de computo.*** **Su clasificación generalizada podemos resumirla en los términos siguientes :**

- Software de Aplicaciones (Sistemas de Información) :
- Administrativos - Financieros - De Manufactura - Etc.

- Software de Paquetes Computacionales :
- Hojas Electrónicas - Procesadores de Palabras - Etc.

- Software de Programación :
- Lenguajes de Tercera Generación - Lenguajes de Cuarta Generación

- Software de Sistemas Operativos

- Productos CASE (Computer Aided Software Engenieering)

- Otros para própositos específicos :

Sistemas de Información : ***Conjunto de módulos computacionales y/o manuales organizados e interrelacionados entre si de una manera formal para la administación y uso eficiente de todos los recursos (Humanos, materiales, finacieros, tecnológicos, etc.) de una área específica del negocio (Manufactura, Administración, Dirección, etc.)*** **con la finalidad de orientar dichos recursos, así como los procedimientos, políticas y funciones inherentes a los mismos al logro de las metas y objetivos de negocio de una manera productiva.**

Los Sistemas de Información pueden orientarse a los siguientes aspectos :

- Apoyo a los niveles operativos, Tácticos y estratégicos del negocio

Sistemas de Información Estratégica (SIE) : Son aquellos que de manera permanente proporcionan a la Alta Dirección una oportuna serie de parametros y acciones encaminadas a la toma de decisiones que brindarán al negocio rentabilidad y alta competitividad respecto a la competencia y al mismo negocio respecto a periodos pasados en su historial como empresa formal.

Metodología : Es un conjunto de Etapas (fases / módulos) formalmente estructurados que se orienta a proporcionar una trayectoria secuencial y lógica para el logro de resultados.

Ejemplos de Metodologías :

- De Planeación de Sistemas - De Desarrollo de Sistemas - De Calidad
- De Auditoria de Informática (Como la propuesta en este libro) - Otras

Técnicas : Es el conjunto de procedimientos y pasos ordenados utilizados en el desarrollo de un proyecto con el fin de finalizar las etapas / fases / módulos definidas en el proceso metodológico.

Algunas de las Técnicas generalmente aceptadas son :

- Análisis estructurado- Diseño estructurado - Análisis Costo/Beneficio
- Pert - Gantt - Documentación - Entrevistas - Otras

Herramientas : Es el conjunto de elementos físicos utilizados para llevar a cabo de manera práctica las acciones y pasos definidos en la Técnica. Antes del auge de las computadoras, así como de otros elementos tecnolológicos relacionados con la ingenieria, arquitectura, etc. dichas herramientas eran simples máquinas o utencilios manuales que nos apoyaban en el desarrollo de las tareas de cada uno de los proyectos.

Herramientas de Productividad : Son aquellas orientadas a lograr la optimización del tiempo de los recursos en el desarrollo de un proyectos, asi mismo se encaminan a proporcionar resultados de alta calidad, por ejemplo :

- Procesadores de Palabras - Diagramadores - Graficadores
- Productos CASE - Impresoras - Microcomputadoras - Etc.

2.2. Auditoría :

La auditoría se desarrolla en base a normas, procedimientos y técnicas definidas formalmente por Institutos establecidos a nivel nacional e internacional.

A. Auditoría : Un proceso formal y necesario para las empresas con el fin de asegurar que todos sus activos sean protegidos permanentemente.

B. Auditoría : Es un conjunto de tareas llevadas a cabo por un especialista para la evaluación y/o revisión de Políticas y procedimientos relacionados con las siguientes áreas :

- Administrativas	- Financieras	- Operativas
- De Informática	- De Crédito	- Fiscales

C. Es un proceso formal que se efectua por requerimientos de las empresas y/o de gobierno en periodos establecidos previamente por los interesados con el objetivo de verificar el cumplimiento oportuno de las políticas y procedimientos relacionadas con cada una de las actividades existentes en la organización

Tareas principales de la Auditoría :

- Estudio y actualización permanente en las áreas susceptibles a revisar
- Apegarse en las tareas que desempeñe a las normas, políticas, procedimientos y técnicas de Auditoría establecidas por los organismos generalmente aceptados a nivel nacional e internacional
- Evaluación y verificación de las áreas requeridas por la Alta Dirección y/o responsables directos del negocio
- Elaboración del Informe de Auditoría (Debilidades y Recomendaciones)
- Otras recomendadas para el desempeño eficiente de la Auditoría

Nota : La Auditoría puede ser ejecutada en una organización por Auditores Internos Así como Auditores Externos.

2.3. Auditoría de Informática

La Auditoría de Informática se desarrolla en base a normas, procedimientos y técnicas definidas formalmente por Institutos establecidos a nivel nacional e internacional.

Auditoría de Informática :

A. Es un proceso formal ejecutado por especialistas del Area de Auditoría y de Informática, que se orienta a la verificación y aseguramiento de que las Políticas y procedimientos establecidos para el manejo y uso adecuado de la Tecnología de Informática en la Organización se lleven a cabo de una manera oportuna y eficiente.

B. Son aquellas actividades llevadas a cabo por profesionales del Area de Informática y de Auditoría encaminadas a evaluar el grado de cumplimiento de las Políticas, Controles y Procedimientos inherentes al uso de los Recursos de Informática por el personal de la empresa (Usuarios, Informática, Alta Dirección, etc.).

C. Es un conjunto de acciones que realiza el personal especializado en las áreas de Auditoría y de Informática para el aseguramiento permanente de que todos los Recursos de Informática operen bajo un ambiente de seguridad y control eficientes.

Nota : La Auditoría puede ser ejecutada en una organización por Auditores Internos Así como Auditores Externos.

3. La Auditoria de Informática y su Medio Ambiente :

3. La Auditoria de Informática y su Medio Ambiente :

Las actividades de un negocio u organización tienen un efecto directo sobre sectores especifícos de la sociedad, de igual manera los eventos y actividades externos al negocio tienen un grado de impacto en el mismo.

No han sido pocos los negocios que han fracasado al mantenerse estáticos ante los movimientos que se presentan a su alrededor, así mismo una gran cantidad de ellos que se han adaptado oportunamente a los cambios sufridos por los elementos externos obtienen ventajas competitivas de dichas variaciones para lograr el liderazgo o al menos mantenerse en el mercado.

El medio Ambiente marca regularmente las pautas y caminos estratégicos a seguir en los diferentes aspectos que contemmpla un negocio y los factores que lo afectan pueden ser :

- Económicos - Políticos - Culturales - Tecnológicos
- Organizacionales - Ecológicos - Etc.

Es importante para los negocios el evaluar de manera constante cada factor externo que predomine o afecte de manera trascendente el medio ambiente externo, con la finalidad de llevar a cabo las acciones necesarias para minimizar o sacar ventaja estratégica del mismo.

Las estrategias de los negocios son definidas formalmente en un proceso de planeación de negocios mediante reuniones o juntas en las que se involucran los Accionistas, Alta Dirección y en algunas ocasiones Consejeros o Consultores expertos en una actividad tan relevante como es la definición de el plan estratégico para cualquier ente organizacional.

Una de las tareas básicas de este proceso es el de determinar los factores internos y externos que pueden afectar y/o facilitar de manera directa o indirecta las estrategias emanadas de dicho plan.

La Auditoría en Informática siendo un proceso básico de validación y control del uso de los Recursos Tecnológicos utilizados en el logro de las estrategias, debe tambien contemplar como parte de sus actividades primarias el entendimiento del entorno que rodea al negocio, así como de la estructura y tiempos del Plan estratégico de Negocios.

En ocasiones la Función de Auditoría en Informática se ve relacionada de manera directa o indirecta con las acciones definidas por la Alta Dirección, ya sea porque será el responsable de llevarlas a cabo o porque será el responsable de darle seguimiento formal a su cumplimiento, a continuación se dará una explicación a manera de ejemplo en la Figura 3-1.

MEDIO AMBIENTE (FACTORES EXTERNOS)			
Factor Externo	**Acciones de la Empresa**	**Responsabilidad del Auditor de Informática**	**Comentario**
Redución a las cifras monetarias en tres dígitos (por ejemplo, antes 5,000 ahora 5)	Es política de la empresa que todos los documentos y/o transacciones reflejen esa reducción de tres dígitos	Verificar que todos los Sistemas de Información, contemplen esta disposición de manera formal y oportuna	Emana como un decreto Gobierno
Auge en el uso de la Tecnología de comunicaciónes Vía Satelite	Se define como estratégico que exista un enlace entre empresas/entidades de la organización por este medio Se proyecta a futuro enlazar clientes y proveedores con la empresa	Verificar y/o Recomendar que exista un proyecto de Análisis Costo/Beneficio para la Adquisición de los permisos de Gobierno, así como la Tecnología que se requiere para la Implantación de dicha Estrategía Verificar su Implantación Adecuada y oportuna.	Se obtiene con esta acción una ventaja competitiva Permite una integración más eficiente entre las entidades de un negocio
Tratado de Libre Comercio con uno o más paises	Se define como política de empresa que cada área o entidad de negocio impulse la calidad y la eficiencia en cada individuo,actividad y producto terminado	Recomendar políticas y procedimientos que aseguren la Calidad y eficiencia en cada una de las funciones de Informática, así como en los productos y Servicios de esta área.(-) (-) Aplica para la Función de Auditoría de Informática	Algunas Sugerencias de Auditoría: - Capacitar a personal - Uso de Métodos y Técnicas Estandar - Etc.
Legalización del Software mediante Derechos de Autor	Es una política en todos los niveles de la organización el contar con Software en la empresa que solo sea original (con licencia de uso)	Establecer una serie de Controles y Procedimientos que aseguren y verifiquen que solo Software Original se encuentre instalado en el equipo de computo del negocio	Acciones : - Inventariar el Softare de la empresa - Comprar e Instalar solo Software Legal

Figura 3-1

Medio Ambiente de Informática :

Son aquellas características dominantes del mercado en cada una de las ramas o criterios relacionados con la Tecnología de Informática, que definen el rumbo y estrategías de Implementación y operación de la misma en los negocios.

La Función de Informática debe estructurar sus servicios, funciones y proyectos en base a los requerimientos específicos del negocio, apoyandose en gran parte en la Tecnologia de Vanguardia que domina el mercado, considerando las tendencias de la misma. El grado de apoyo que se buscará en el medio ambiente Tecnológico depende en gran medida de la orientación y justificación que se le asigne al enfocarlo a cada estrategía de la empresa.

No todo lo que ofrece el mercado como estandares y soluciones Tecnológicas en caso de adoptarlos nos garantizará el desempeño eficiente de la Función de Informática en una Organización, el Auditor de Informática deberá verificar la existencia de un Análisis Costo/Benefico en cada proyecto de Inversión orientado a la Adquisicón de Nueva Tecnología o Estandares para el uso y manejo de la misma. Además Auditória de Informática mantendra un proceso permanente de seguimiento al uso de los Recursos de Tecnología, Metodologías, Técnicas, Procedimientos y Políticas inherentes a Informática que Asegure Calidad y Productividad en esta área, no con el fin de ser 'un policia informático' sino un punto de apoyo.

El medio ambiente de Informática sufre de manera continua cambios en algunos de sus elementos, ya sea en Hardware, Software, Telecomunicaciónes, Etc. debido a la busqueda constante de soluciones más eficientes en aspectos relativos al Desempeño, Costo, etc.

En consecuencia, cualquier área que tenga como objetivo el operar, manejar y /o evaluar (Que es el caso que nos interesa) debe estar dispuesta a llevar las acciones pertinentes que nos aseguren su debido entendimiento y aprovechamiento para brindarle a la Organización resultados de Alta Calidad y la confianza de que la Información seguirá cumpliendo con los requisitos de control esperados : Exactitud, Totalidad, Autorización, Actualización, etc.

En las últimas decadas el medio ambiente de Informática ha sido uno de los campos que ha registrado un mayor ritmo de crecimiento en todas sus áreas de acción, traduciendose esto en :

a) Mejores equipos de cómputo, ya que cuentan con características dificilmente encontradas anteriormente, tales como conectividad, escalabilidad, etc.

b) Lenguajes de programación y paquetes de software más flexibles y dinámicos que permiten actualmente a los desarrolladores de aplicaciones ser más productivos, dando un alto grado de participación a los usuarios en el proceso de Desarrollo e Implantación de Soluciones de Negocio.

c) Innovaciones Tecnológicas en Telecomunicaciones, ya que se pueden transmitir voz, datos, imagen y video, Así mismo se ha logrado enlazar a diferentes empresas con clientes y proveedores a traves de Redes Locales (LAN), Redes Metropolitanas (MAN) y Redes Abiertas (WAN) (Iniciales derivadas de su significado en ingles), la capacidad de volumenes de información, la velocidad de transmisión y la protección de los datos ha venido obteniendose con la aparición del cable coaxial y la Tecnología de Redes Digitales Integradas por ejemplo.

d) En el campo de la Tecnología Vanguardista se encuentran en proceso de Implantación y Formalización en la mayoria de las empresas :

- Código de Barras
- Multimedia (Integración de Video, Televisión, Computadora, Etc.)
- C.A.S.E. (Ingenieria de Software Asistida por Computadora)
- E.D.I. (Intercambio Electrónico de Datos)
- Automatización de Oficinas (el enfoque del 'paper less' / 'sin papel')
- Ambientes orientados a Objetos

e) Metodologías, técnicas y herramientas para la Administración de la Función de Informática, la Planeación y Desarrollo de Sistemas han venido formalizandose y apegandose a los estandares comunmente aceptados a nivel nacional e internacional, lo que ha sido un factor de suma utilidad para el desempeño eficiente de las tareas y servicios inherentes a la Informática y de la misma Auditoría de Informática.

f) La integración de especialidades profesionales (Ingenieria, Auditoría, Informática, etc.) en Asociaciones Profesionales reconocidas formalmente a nivel Nacional e Internacional, como la EDP Auditors Association, Inc. (Asociación Mexicana de Auditores en Informática, A.C. en México) entre otras, brindan la oportunidad a las instituciones y organizaciones privadas y de gobierno tener un contacto directo y oportuno con los conocedores y/o impulsadores de las tendencias dominantes del medio ambiente en sus areas economicas, sociales, tecnologicas, etc.

La Figura 3-2 ilustra de manera general algunos comentarios relevantes sobre las características y aportaciones que han surgido en la Tecnología de Informática y de las cuales los negocios deben estar evaluando para su posible implantación y lograr el máximo de beneficios.

En la Figura 3-2 se comenta tambien de manera somera, la contribución e impacto que ha tenido la Tecnología de Informática en su campo de acción.

Concepto	Características	Impacto en la Auditoría de Informática
Hardware : - Mainframes - Minicomputadoras - Microcomputadoras - Portatiles - Impresoras - Dispositivos de Almacenamiento - Otros **Comunicaciones :** - Voz - Datos - Imagen - Video	-Elementos físicos y tangibles de la Tecnología de Informática - Por ellos es posible alimentar, Procesar, Generar , transmitir y Almacenar los datos de los Sistemas de Información (Estratégicos, Tácticos y Operativos del negocio) - El Hardware sufre cambios de manera dinámica , hoy en día su tamaño Físico ha disminuido y sus caracteristicas de desempeño y portabilidad han mejorado de manera sorprendente : - Almacenamiento - Procesamiento - Portabilidad - Escalabilidad - Conectividad - Etc.	- Al surgir las primeras computadoras y se trasladarón a ellas los Sistemas Financieros Y Contables, el Auditor utilizo los Equipos de Cómputo para Consulta, Captura, Proceso y Generación de Reportes para Evaluar la Situación que guardaban dichos sistemas. -Actualmente los equipos de Cómputo brindan más facilidades al Auditor de Informática que se pueden Evaluar Sistemas de Información y otros aspectos de Interes a traves de accesos remotos y en línea, - Se pueden utilizar equipos portables que permiten auditar tareas en el lugar de los hechos. - Las facilidades que brindan las comunicaciones y los equipos de Computo, permiten al Auditor registrar y minitorear una gran cantidad de actividades inherentes al uso de las computadoras y equipos de Teleccomunicaciones.
Software : - **Procesadores de Palabras** - **Hojas de Cálculo** - **Graficadores** - **Diagramadores** - **Presentadores** - **Especializado :** - Auditoria - Seguridad - Desempeño - **Case :** - Método - Técnica - Herramienta	Son los Elementos Lógicos de la Computadora. Es por medio de este elemento que se ha logrado con el paso del tiempo la Sistematización Computacional de los Procesos de negocio(tareas operativas, tácticas y estratégicas) En un nivel más especializado, se ha logrado con la Ingenieria de Software la Sistematización a Traves de las Computadoras de las actividades del Desarrollo de Sistemas y en gran medida de la Planeación de Sistemas a traves del CASE (Ingenieria de Software Asistida por Computadora).	- Al surgir la necesidad de evaluar Sistemas Computacionales que guardaban datos de los estados Financieros y Contables de la empresa, el Auditor se apoyo en personal con especialización en Informática, ya que la programación (en lenguajes como COBOL) y el manejo de los equipos de Computo requeria de conocimientos específicos. El apoyo que se le brindo al Auditor fué el de programar rútinas control y evaluación de procesos en los Sistemas Computacionales, o para generar reprocesos y respaldos de la Información a ser auditada. - Al surgir el Auditor de Informática, éste se perfilo como el individuo que domina ambos campos la Auditoría y La Informática, siendo este el enlace ideal para la Evaluación, no solo de Sistemas de Información, sino tambien del uso eficiente de todos los Recursos, Servicios y Productos de Informática en el negocio

Figura 3-2

Objetivo del Auditor de Informática al estudiar el Medio Ambiente y su impacto en el negocio :

Es definir el grupo de proyectos de Auditoría de Informática que serán ejecutados en un plazo determinado con el fin de apoyar directa o indirectamente a las estrategias del negocio, considerando los diversos factores internos y externos que se relacionan con la organización. Es conveniente señalar que cada uno de estos proyectos deberá estar enmarcado en los límites definidos para la función, esto es debe enfocarse al control, seguridad y auditoría de los diferentes elementos que tengan impacto directo o indirecto con la Tecnología de Informática.

4. Planeación

4. PLANEACION :

La Función de Auditoría de Informática debe generar al igual que todas las áreas del negocio, un plan de proyectos que justifiquen su trabajo durante un cierto periodo, de igual manera deberán de contemplar cada uno de esos proyectos un Análisis Costo/Beneficio y la estructura de los mismos con un enfoque metodológico , lo anterior con la finalidad de que tambien dicha función pueda ser evaluada en base a su desempeño, con parametros que sean lo más tangibles y medibles posibles.

Cada proyecto de Auditoria en Informática soporta en un bajo o alto grado a los objetivos y requerimientos de tres entidades del negocio :

A. Alta Dirección

- Seguimiento a proyectos relacionados con la Tecnología de Informática
- Verificación y Aseguramiento en el cumplimiento de Políticas inherentes a la Tecnología de Informática
- Otros aspectos de Interes para la Alta Dirección

B. Auditoria

- **Apoyo en la Definición, Implantación y Seguimiento en :**
  - Políticas, Controles y Procedimientos de Auditoría Financiera, Operativa, de Créditos, Fiscal, etc. Relacionadas directa o Indirectamente con la Tecnología de Informática (Sistemas de Información, Equipos de Cómputo, Comunicaciones, Etc.)
- Planes de capacitación en el uso y entendimiento de :
  1. Software de Auditoría
  2. Herramientas de Productividad (Hojas Electrónicas, Procesadores de Palabras, Graficadores, Diagramadores, etc.)
  3. Bases de Datos (Consulta de Información por ejemplo)
  4. Equipos de Cómputo (Micros, terminales, portátiles, etc.)
  5. Otros de Interes para los Auditores

- Otros de interes para el desarrollo eficiente de los auditores cuando evaluan áreas del negocio que se apoyan en Informática.

C. Informática :

- Apoyo en la Definición, Implantación y Seguimiento en :

- Políticas, controles, procedimientos y Estandares relativos a :

1. Organización y Administración de Informática
2. Proceso de Planeación de Informática
3. Evaluación y Adquisición de nueva Tecnología
4. Evaluación y Adquisición de Servicios
5. Desarrollo e Implantación de Soluciones (EDI, CASE, Base de Datos, Telecomunicaciones, Sistemas Estratégicos, Multimedia, etc.)
6. Etc.

- Otros de Interes para Informática

Lo anterior nos lleva a concluir que es muy importante que exista una permanente comunicación entre la Función de Auditoría de Informática y la Alta Dirección, así como con las Direcciones y/o Gerencias de Auditoría o Informática.

A continuación se mencionarán algunos puntos a considerar para obtener un Plan Maestro de Auditoria en Informática que asegure un apoyo permanente y eficiente a las entidades del negocio antes mencionadas :

1. Crear o formalizar un cómite de control y seguimiento integrado por :
   - Alta Dirección
   - Responsable directo de Auditoría
   - Responsable directo de Informática
   - Responsable directo de Auditoría de Informática

2. Analizar los proyectos de Negocio, Informática, Auditoría y Auditoría de Informática de manera conjunta, con el objetivo de ver la relación o impacto que tienen entre si y facilitarse de manera formal los compromisos que aseguren el cumplimiento de los mismos.

Nota : Los proyectos de cada área pueden ser desarrollados y planeados de manera independiente.

3. Establecer fechas de reuniones formales e informales para dar seguimiento a los planes de compromiso conjunto.

4.1. El Proceso de Planeación de Auditoría de Informática

Son las actividades desarrolladas por el Auditor en Informática que tienen como objetivo principal elaborar y presentar un conjunto de Proyectos inherentes a la Función de Auditoría de Informática a la Alta Dirección, y que estarán orientados primordialmente al aseguramineto de la Calidad, Seguridad y Control de los diferentes elementos que se encuentran relacionados directa o indirectamente con los Recursos de Informática.

Para un entendimiento de las tareas críticas de un proceso de planeación de Auditoría de Informática ver la **Figura 4-1.**

Tareas Básicas del Proceso de Planeacón de Auditoría de Informática y Responsabilidades			
Actividad	**Responsable de Ejecusión**	**Responsable del seguimiento**	**Comentarios**
Determinación de las áreas a Auditar en el Negocio	Coordinador y/o Supervisor de Auditoría de Informática	Director y/o Gerente de Auditoría de Informática	Se efectua un Diagnóstico actual de la Función de Informática (Desde el punto de vista de negocio y desde el punto de vista del negocio) con el fin de detectar áreas de riesgo o debilidades de la Función de Informática.(Ver mátriz de Riesgos)
Elaboración del Plan de Auditoría de Informática	Coordinador y/o Supervisor de Auditoría de Informática	Director y/o Gerente de Auditoría de Informática	Las fechas y periodos en que se auditaran las áreas puede obedecer a solicitud expresa de la Alta Dirección o a requerimientos de la Función de Auditoría de Informática
Presentación del Plan a la Alta Dirección	Director y/o Gerente de Auditoría de Informática	Alta Dirección del Negocio	Se recomienda que se haga de manera oportuna (Al iniciar el periodo fiscal por ejemplo) y que se autorize formalmente
Ejecución del Plan de Auditoría de Informática	Supervisor y/o Auditores de Informática (Externos o Internos)	Gerente y/o Supervisores de la Función de Auditoría de Informática	Algunas empresas consideran que es recomendable utilizar personal de Auditoría externo, esto para darle independencia al Informe o para aligerar las cargas de trabajo.

Figura 4-1

Proceso Detallado de la Planeación de Auditoría de Informática :

Es importante aclarar que este proceso de planeación depende en gran medida del Diagnostico Previo que haga el Auditor de Informática de la Situación que guarda en ese momento cada una de las áreas o servicios de la Función de Informática, Así como tambien es de suma relevancia el considerar las necesidades o prioridades que tenga la Alta Dirección de auditar o evaluar una área específica de Informática.

Consideraciones para el Proceso elaboración, Documentación, Autorización y Difusión formal del Plan de Auditoría de Informática.

1. Es importante identificar el nivel de riesgo de cada uno de los Elementos que integran la Función de Informática en el negocio a traves del **Diagnostico de la situación actual de Informática** (Los cuestionarios y formatos sugeridos para su desarrollo serán contemplados en un capitulo posterior).

Las áreas que serán diagnosticadas pueden variar de acuerdo al tamaño y estructura del negocio, pueden ser empresas que dependan de un corporativo o 'Holding', el giro de la empresa y el número de sucursales o subsidiarias originan en ocasiones que el Auditor de Informática tenga que evaluar productos y servicios de Informática con un enfoque centralizado o descentralizado según sea el caso.

Algunos de los siguientes servicios serán mencionados de manera ilustrativa, sin embargo no son limitativos o totalitarios para ninguna empresa, ya que será el perfil y característica propia la que defina el alcance de la Función de Informática :

- Sistemas de Información en Operación
- Administración de Hardware y Software
- Desarrollo de Sistemas de Información
- Soporte a usuarios (Capacitación, Asesoria, etc.)
- Administración de Telecomunicaciones
- Investigación y Desarrollo Tecnológico
- Etc.

2. El Auditor deberá utilizar todos los parametros de medición y evaluación posibles, sin caer en un análisis detallado, ya que aquí solo se trata de detectar la problematica principal de cada una de las áreas.

Si este proceso mostrará anomalías de considerable importancia, en alguno de sus elementos evaluados, se deben tomar acciones inmediatas orientadas a minimizar y/o eliminar la anomalía.

3. Determinar el nivel de Riesgo que existe en cada una de las áreas de la Función de Informática : Cada área, producto o servicio de Informática es susceptible de evaluación y control para el aseguramiento de que se desarrolle de acuerdo a los estandares, políticas y procedimientos especificos que le han sido asignados de acuerdo a su función.

Actividades para el Proceso elaboración, Documentación, Autorización y Difusión formal del Plan de Auditoría de Informática

1.- Diagnóstico de la Situación Actual de los Sistemas de Información en Operación.

1.1. Sistemas de Información en Operación : Por ser este un elemento crítico dentro del funcionamiento formal de cualquier negocio (Aquí se manejan los datos de las áreas financieras, productivas y administrativas para la toma de decisiones) haremos énfasis en las consideraciones y criterios más importantes que debe tomar en cuenta el Auditor de Informática (de las demás áreas, como desarrollo de Sistemas, Telecomunicaciones, etc. haremos referencia más detallada en los siguientes capitulos).

El Diagnóstico general de esta área se puede llevar a cabo de la siguiente manera :

A.1) Obtener una lista de los principales Sistemas de Información, los Usuarios Principales de cada uno (Determinar cuales fuerón desarrollados por la empresa y cuales fuerón comprados a terceros, esto con el fin de que si se llegase a determinar que algunos de estos deben ser evaluados con más detalle, sepamos cual será la fuente principal de estudio).

A.2) Tomando como base los comentarios positivos y negativos de los principales usuarios de cada sistema de información que se encuentre en operación, determinará con ellos los volumenes de transacciones promedio.

A.3) Las fallas y/o regularidades más comunes que presenta el Sistema y/o Equipo de Computo donde se encuentra, prioridades de operación.

A.4) Informes del desempeño hechos con anterioridad a los usuarios principales, a los analistas del sistemas y personal de producción.(Oportunidad, Calidad, Confiabilidad).

Debilidades que pueden motivar a que se lleve a cabo la Auditoría a un Sistema de Información :

Primero : Que el Sistema no haya sido liberado formalmente, lo que puede traer como consecuencia el desconocimiento real por parte de los usuarios y del personal de Auditoría de las debilidades y fortalezas del Sistema.

Segundo : Que el sistema nunca haya sido auditado, esto sugiere la alternativa de auditarlo de manera inmediata, sobre todo, si es un sistema crítico para Alta Dirección (Un Sistema de Cheques en un banco, un Sistema de Ventas en una empresa comercial o un Sistema de Manufactura en una empresa de giro Industrial); en caso de no ser un Sistema crítico para el negocio, programar una revisión al mismo en los proyectos intermedios o finales de Auditoría de Informática..

2. Clasificar el nivel de riesgo que representa el uso Hardware y Software dentro de la organización. Lo que se desea determinar en este punto es que los Sistemas de Información Computarizados y datos sean procesados en un ambiente tecnológico confiable, seguro y eficiente. Aquí se pueden auditar aquellos equipos o paquetes de software que dan soporte a los Sistemas críticos del negocio, o se podra auditar de manera periodica el mantenimiento.

2.1 Evaluar así mismo la capacidad de los equipos, cantidad de unidades (Discos, Cintas, Terminales,etc.),los Tipos (Micros, Redes, Minis, Mainframes), Distribución física de los mismos, reportes de Desempeño de los mismos son datos que pueden ayudar a determinar la secuencia y grado de intensidad con que se auditará el Hardware.

El uso y propósito de los paquetes de software, la existencia de procedimientos y políticas en la evaluación y adquisición de Software, así como la estandarización de paquetes, apoyan al auditor en la programación de los proyectos de Auditoría.

3 Otros aspectos a clasificar : Administración del Centro de Computo, Organización de Informática, Servicios y Productos (Externos o Internos) de Informática, Telecomunicaciones, EDI(Intercambio Electrónico de Datos por sus siglas en Ingles), Automatización de Procesos, CASE,Etc.

Estos deben ser evaluados en base a estandares comunmente aceptados a nivel nacional e internacional y en base a la proyección de uso que piensa darle el negocio en el corto, mediano y largo plazo. Además deben considerarse los comentarios y/o asesorias de personal especializado en esta área, siendo gente externa o de la misma Función de Informática de la empresa que se está evaluando.

4.- Clasificación de los riesgos en base a criterios establecidos por la Función de Auditoría de Informática, tales como :

- Cumplimiento de Estandares comunmente aceptados a nivel nacional e internacional
- Cumplimiento formal de Políticas y Procedimientos
- Grado de Satisfación de la Alta Dirección y del Personal Usuario
- Etc.

Nota : El Auditor deberá utilizar todos los parametros de medición y evaluación posibles, sin caer en un análisis detallado, ya que aquí solo se trata de detectar la problematica principal de cada una de las áreas.

Si este proceso mostrará anomalías de considerable importancia, en alguno de sus elementos evaluados, se deben tomar acciones inmediatas orientadas a minimizar y/o eliminar la anomalía.

Consideraciones a tomar en cuenta al hacer el Diagnostico de la Situación Actual para la obtención de la Matriz de Riesgos: *Es importante señalar que el Auditor de Informática, debe conocer de manera suficientemente aceptable los aspectos relativos a Auditoría e Informática que debe tener cada una de las áreas de Informática,* **lo anterior es un requisito indispensable, ya que será en base a su experiencia y dominio de la Auditoría de Informática en lo que hará un Diagnóstico objetivo y contundente**, ademas se apoyará en la visión de los principales usuarios del negocio y del responsable de Informática.

Consideraciones a tomar en cuenta al hacer el Diagnostico de la Situación Actual para la obtención de la Matriz de Riesgos: *Es importante señalar que el Auditor de Informática, debe conocer de manera suficientemente aceptable los aspectos relativos a Auditoría e Informática que debe tener cada una de las áreas de Informática,* **lo anterior es un requisito indispensable, ya que será en base a su experiencia y dominio de la Auditoría de Informática en lo que hará un Diagnóstico objetivo y contundente**, ademas se apoyará en la visión de los principales usuarios del negocio y del responsable de Informática.

5.- Elaborar una matriz de Riesgos que muestre las Areas de la Función de Informática, que serán susceptibles de una revisión por parte de Auditoría en el siguiente periodo.

Dicha matriz muestra resultados en un orden descendente. Esto implica que el Area que muestre el valor más alto es la entidad con mayor riesgo, por lo tanto deberá ser la primera en evaluarse por parte de Auditoría y así sucesivamente hasta conocer las Areas de menor riesgo.

6.- Elaborar un plan consolidado de Proyectos que tenga al menos la siguiente información :

- Fechas de Inicio y Terminación de cada Auditoría
- Etapas de cada Auditoría
- Tareas Principales de Cada Etapa
- Equipo de Trabajo (Auditor(es), Representante de Informática y Representante de las áreas Usuarias
- Requerimientos (Recursos, Apoyo de la Dirección, Capacitación, Material de Auditoría en Informática,etc)

7.- Revisar con la Gerencia o Dirección a la que reporta directamente la Función de Auditoría Informática, la Matriz de Riesgos y el Pronostico de Proyectos de Auditoría de Informática .

Debe ser llevada a cabo de manera oportuna y formal con el fin de que se de el visto bueno o se lleven a cabo las adaptaciones o mejoras que se consideren pertinentes, **antes de presentarlo a la Alta Dirección de la Organización.**

8. Elaborar formalmente el plan, cubriendo al menos los siguientes aspectos :

- Area a Auditar - Prioridad - Fechas de Inicio y Término
- Involucrados - Responsables
- Fechas de Revisión formales e Informales
- Otros de interes particular del Auditor de Informática en el momento de efectuar esta tarea

9.- Presentar a la Alta Dirección el Plan de Proyectos de la Función de Auditoría en Informática. Lo anterior es con los siguientes propositos :

- Que conozcan antes de que inicie el año fiscal los proyectos de Auditoría en Informática
- Verificar que las Areas que ellos consideran críticas para el buen funcionamiento del negocio, hayan sido contempladas en el Plan de Auditoría de Informática y en la Matriz de Riesgos, para su debida reorganización antes de que sea autorizado.
- Otros

10.- Llevar a cabo cada uno de los proyectos de acuerdo al Plan de Auditoría en Informática.

10.1 ejecutar actividades de Seguimiento y Revisión formal a cada uno de los proyectos

11.- Integrar y formalizar equipos de trabajo formados por:

a) Gerente(s) de las Areas Usuarias a Evaluar
b) Gerente de la Función de Informática
c) Lider del Proyecto de la Función de Auditoría en Informática
d) Otros que sean necesarios

12.- Obtener la aprobación formal de la Alta Dirección del Informe Final de la Auditoría de Informática Realizada

13 Aplicar este proceso de Planeación de Auditoría de Informática de manera permanente.

5. Metodología para el Desarrollo e Implantación de la Auditoría de Informática :

5.1 Proceso Metodológico de la Auditoría de Informática

5. Metodología para el Desarrollo e implantación de la Auditoría de Informática :

La Auditoría de Informática debe ser respaldada por un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Al igual que otras funciones en el negocio la Auditoría de Informática debe efectuar sus tareas y actividades mediante una Metodología Formal (Ver **Figura 5-1**).

No es recomendable que se fomente en las organizaciones la dependencia en el desempeño de tan importante función solo en base a la experiencia, habilidades, criterios y conocimientos sin una referencia metodológica, el contar con un método nos garantiza que todas las cualidades de cada Auditor de Informática sean orientadas a trabajar en equipo para la obtención de productos de calidad estandarizados.

La Función de Auditoría de Informática debe contar támbien con un desarrollo de activades basadas en un método de trabajo formal, que sea entendido por todos los Auditores de Informática y complementado con Técnicas y Herramientas propias de la Función.

Lo anterior se facilita si los Auditores de Informática cuentan con una metodología que oriente cada proyecto a una ejecución armoniosa y planeada en cada una de las tareas y actividades involucradas.

Un alto porcentaje de los especialistas en Areas de Investigación, Planeación Financiera o de Informática, en Desarrollo de Sistemas, en Manufactura y otras más se apoyan en gran medida en tareas, actividades, productos terminados, revisiones, roles y responsabilidades, etc. definidas previamente en un documento formal llamado Métodología, donde lo que se busca es brindarle a los responsables de dichas áreas un camino estructurado por donde llegar a los resultados esperados por la empresa.

Es importante señalar que el uso de la metodología no garantiza por si sola el éxito de los proyectos de Auditoría de Informática, se requiere además un buen dominio y uso constante de los siguientes aspectos complementarios :

- Técnicas y Herramientas de productividad
- Habilidades personales
- Conocimientos técnicos y administrativos
- Experiencia en el campo de Auditoría y de Informática
- Concocimiento de los factores del negocio y del medio ambiente
- Actualización permanente
- Involucración y comunicación constante con Asociaciones Nacionales e Internacionales relacionadas con este campo
- Otras

EL PROCESO METODOLOGICO GENERAL DE LA AUDITORIA DE INFORMATICA : UN ENFOQUE METODICO				
Etapa	**Productos Terminados**	**Requerimientos**	**Responsables**	**Involucrados**
PRELIMINAR (DIAGNOSTICO)	1. DIAGNOSTICO DE NEGOCIO	+ INVOLUCRACION DE LA DIRECCION	L.P.	A.D. / .A.I.
	2. DIAGNOSTICO INFORMATICA	+ INFORMACION VERAZ	L.P.	R.I. / R.A.I.
JUSTIFICACION	1. MATRIZ DE RIESGOS	+ ANALISIS DE RIESGOS Y AREAS DE OPORTUNIDAD	L.P.	R.A.I. / R.I.
	2. PLAN DE AUDITORIA DE INFORMATICA	+ DEFINIR RESPONSABLES Y TIEMPOS	L.P.	R.A.I.
ADECUACION	1. PLAN Y METODOLOGIA DE ACUERDO AL CLIENTE	+ ENTENDIMIENTO DEL NEGOCIO Y DE LA FUNCION DE INFORMATICA	L.P.	R.I. / R.A.I. / P.U.
	2. PLAN DETALLADO	+ DETALLAR TAREAS Y TIEMPOS	A.I.	R.I. / R.A.I. / P.U.
FORMALIZACION	1. PLAN APROBADO	+ APROBACION FORMAL (FIRMAS)	A.D.	R.I. / R.A.I. / P.U.
	2. COMPROMISO EJECUTIVO	+ RESPALDO Y APOYO AL PROYECTO	A.D.	R.I. / R.A.I. / P.U.
DESARROLLO	1. AUDITAR AREAS SELECCIONADAS	+ APROBACION DE LA DIRECCION	L.P.	R.I. / P.U. / A.I.
	2. INFORME DE AUDITORIA DE INFORMATICA	+ ASIGNAR RESPONSABLES Y TIEMPOS PARA CADA ACCION RECOMENDADA	A.D. / P.I. / P.U.	R.A.I. / L.P. / A.I.

NOMENCLATURA : A.D. = ALTA DIRECCION P.U. = PERSONAL USUARIO R.I. = RESPONSABLE DEL AREA DE INFORMATICA
P.I. = PERSONAL DE INFORMATICA R.A.I. = RESPONSABLE DEL AREA DE AUDITORIA DE INFORMATICA
L.P. = LIDER DEL PROYECTO DE AUDITORIA DE INFORMATICA A.I. = AUDITOR DE INFORMATICA

Figura 5-1

5.1 Proceso Metodológico de la Auditoría de Informática

Las ventajas de usar un proceso de trabajo metodológico y estandar dentro de la Función de Auditoría de Informática por todo el personal de la función genera al ménos las siguientes ventajas :

- Se elimina el proceso informal de trabajo
- Los recursos orientan sus esfuerzos a la obtención de productos de calidad, con características y requisitos comunes para todos los responsables
- Las tareas y productos terminados de los proyectos se encuentran definidos y formalizados en un documento al alcance de todos los Auditores de Informática
- Se facilita en un alto grado la administración y seguimiento de los proyectos, debido a que la metodología obliga a la planeación detallada de cada proyecto bajo criterios estandares.
- Trabaja sobre tareas y productos terminados perfectamente definidos.
- Otros

La Figura 5-1 nos muestra una descripción general de las Etapas de la Metodología de Auditoría de Informática así como los Datos generales relacionados con cada una de ellas.

Esta visión será de gran utilidad tanto para el Auditor de Informática como para los demás involucrados en el Proyecto.

El Responsable de la Función de Auditoría de Informática puede valerse de la información consolidada contenida en la Tabla de descripción general de la Metodología de Auditoría de Informática, para darle un seguimiento oportuno y estructurado a cada uno de los proyectos, debido a que todas las tareas y productos terminados (Salvo algunas tareas y resultados)

En los cápitulos posteriores cada una de las etapas será explicada de manera detallada

Tal como se ha venido comentado en capitulos anteriores, el desarrollo exitoso de la Auditoría de Informática depende de un conjunto de factores interrelacionados entre si. El conjuntar y coordinar de manera eficiente los siguientes factores nos brindará el aseguramineto de resultados satisfactorios por parte del desempeño de la Función de los Auditores de Informática :

- Dominio de los conceptos Técnicos y Administrativos relacionados con Auditoría de Informática
- Habilidades Inherentes a la Auditoría de Informática
- Normas personales
- Entendimiento de la Auditoría de Informática y sus tendencias
- Adaptación y/o Actualización de acuerdo al Medio Ambiente dominante
- **Entendimiento satisifactorio de Métodos, Técnicas y Herramientas necesarias para auditar las áreas seleccionadas en el proceso de Planeación de Auditoría de Informática**
- Otros que dependen de las características de cada organización donde se desarrolle la Función de Auditoría de Informática

Uno de los factores que son críticos para el Auditor de Informática en el desempeño eficiente de su trabajo es el conocimiento y/o aplicación de los Métodos, Técnicas y Herramientas comunmente aceptados para Informática en los Negocios o Asociaciones.

En medida que el Auditor de Informática tenga experiencia y conocimientos actualizados sobre los diferentes aspectos que evaluará, tendrá resultados pobres o exitosos dentro de la Organización donde trabaja.

En la **Figuras 5-2, 5-3** se muestran un conjunto de elementos metodológicos, técnicos y operativos recomendados para apoyar a la Función de Auditoría de Informática en la revisión y evaluación de áreas específicas de Informática y los demás componentes relacionados con ella.

GRADO DE IMPORTANCIA DE METODOS, TECNICAS Y HERRAMIENTAS EN LAS ETAPAS DEL PROCESO METODOLOGICO DE AUDITORIA DE INFORMATICA			
CONCEPTO	**ETAPA PRELIMINAR**	**ETAPA DE JUSTIFICACION**	**ETAPA DE ADECUACION**
Métodología :			
- Planeación de Informática	**CRITICO**	**CRITICO**	**CRITICO**
- Implantación de sistemas	**NO REQUERIDO**	**NO REQUERIDO**	**CONVENIENTE**
Técnicas :			
- Análisis :			
- Organizacional	**CRITICO**	**CRITICO**	**CRITICO**
- Sistemas	**NO REQUERIDO**	**CONVENIENTE**	**CONVENIENTE**
- Computacional	**NO REQUERIDO**	**NO REQUERIDO**	**NO REQUERIDO**
- Diseño :			
- Conceptual	**NO REQUERIDO**	**CONVENIENTE**	**CRITICO**
- Computacional	**NO REQUERIDO**	**NO REQUERIDO**	**NO REQUERIDO**
- Costo/Beneficio	**CONVENIENTE**	**CRITICO**	**CRITICO**
- Modelo de Datos y Procesos	**CONVENIENTE**	**CRITICO**	**CRITICO**
- Documentación :			
- Detallada	**NO REQUERIDO**	**CONVENIENTE**	**CONVENIENTE**
- Entrevistas	**CRITICO**	**CRITICO**	**CRITICO**
- Cuestionarios	**CONVENIENTE**	**CRITICO**	**CRITICO**
- Otras Técnicas (&)	**(&)**	**(&)**	**(&)**
- Controles, Políticas y Estandares Nacionales e Internacionales	**NO REQUERIDO**	**CONVENIENTE**	**CONVENIENTE**
- Areas de Especialización :			
- Comunicaciones (&)	**(&)**	**(&)**	**(&)**
- Otros (&)	**(&)**	**(&)**	**(&)**
- Habilidades y/o Virtudes :			
- Creatividad	**NO REQUERIDO**	**CONVENIENTE**	**CONVENIENTE**
- Abstracción	**CRITICO**	**CRITICO**	**CRITICO**
- Otros (&)	**(&)**	**(&)**	**(&)**

Figura 5-2

GRADO DE IMPORTANCIA DE METODOS, TECNICAS Y HERRAMIENTAS EN LAS ETAPAS DEL PROCESO METODOLOGICO DE AUDITORIA DE INFORMATICA		
CONCEPTO	**ETAPA DE FORMALIZACION**	**ETAPA DE DESARROLLO**
Métodología :		
- Planeación de Informática	**CRITICO**	**CRITICO**
- Implantación de Sistemas	**NOREQUERIDO**	**CRITICO**
Técnicas :		
- Análisis :		
- Organizacional	**CRITICO**	**CRITICO**
- Sistemas	**CONVENIENTE**	**CRITICO**
- Computacional	**NO REQUERIDO**	**CRITICO**
- Diseño :		
- Conceptual	**CONVENIENTE**	**CRITICO**
- Computacional	**NO REQUERIDO**	**CRITICO**
- Costo/Beneficio	**CRITICO**	**CRITICO**
- Modelo de Datos y Procesos	**CONVENIENTE**	**CRITICO**
- Documentación :		
- Detallada	**NO REQUERIDA**	**CRITICO**
- Entrevistas	**CRITICO**	**CRITICO**
- Cuestionarios	**NO REQUERIDO**	**CRITICO**
- Otras Técnicas (&)	**(&)**	**(&)**
- Controles, Políticas y Estandares Nacionales e Internacionales	**NO REQUERIDO**	**CRITICO**
- Areas de Especialización :		
- Comunicaciones (&)	**(&)**	**(&)**
- Otros (&)	**(&)**	**(&)**
- Habilidades y/o Virtudes :		
- Creatividad	**CONVENIENTE**	**CRITICO**
- Abstracción	**CRITICO**	**CRITICO**
- Otros (&)	**(&)**	**(&)**

Figura 5-3

(&) Es importante aclarar que las tablas anteriores no buscan limitar el buen desarrollo de la Auditoría de Informática. Se recomienda analizar de manera objetiva, la Tecnología y tipo de Organización para definir la magnitud y el énfasis que debe darsele a cada uno de los conceptos señalados.

6. Etapa Preliminar (Diagnóstico de la Situación Actual) :

6.1. Diagnóstico de Negocio (Alta Dirección y Usuarios de Informática)

6.1.1. Conocimiento del Negocio
6.1.2. Apoyo al negocio

6.2. Diagnóstico de Informática (Responsables de la Función)

6.2.1. Conocimiento de la Función de Informática
6.2.2. Servicios
6.2.3. Aspectos de Control

6. Etapa Preliminar (Diagnóstico de la Situación Actual) :

6.1. Diagnóstico de Negocio (Alta Dirección y Usuarios de Informática)

Este es el primer paso que de manera práctica inica el Auditor de Informática dentro de las empresas o Instituciones al efectuar un proyecto de Auditoría de Informática, se busca una opinión de la Alta Dirección para estimar el grado de satisfacción y confianza que se tiene hacia los productos, servicios y recursos de informática en el negocio, así mismo es posible detectar en esta etapa las fortalezas, aciertos y apoyo que brinda dicha función desde la perspectiva de los directivos del negocio.

Un punto importante que debe quedar plasmado en esta fase o etapa preliminar son las áreas de oportunidad que tiene Informática para hacer más competitivo y rentable al negocio, sea este soporte directo o indirecto, en alto o menor grado.

Es conveniente aclarar que esta etapa no debe ser tratada como un conjunto de tareas que requieren muchos recursos involucrados ni un tiempo considerable, es simplemente un aspecto necesario y generalizado para entender los puntos debiles y fuertes de la Función de Informática desde un punto de vista de los usuarios claves y la Alta Dirección.

TAREAS, PRODUCTOS TERMINADOS, RESPONSABLES E INVOLUCRADOS :

Todas las actividades del Auditor de Informática deben estar claramente definidas en todos los componentes formales que integran cualquier trabajo dentro de una organización, en la **Figura 6-1** tenemos toda la información detallada que guiara al Auditor de Informática en esta etapa.

los aspectos a evaluar son al menos los tres mencionados a continuación, más si el Auditor considera que la complejidad del negocio, la fusión o compra de la empresa, la informalidad palpable de Informática o alguna consideración específica para el Lider de Proyectos y/o a petición de la Alta Dirección requieren más puntos a considerar y un tiempo más prolongado, se recomienda que lo apliquen, ya que aquí se detectan los primeros sintomas de Informática y pueden ser a la postre los más relevantes.

EL PROCESO METODOLOGICO DE LA AUDITORIA DE INFORMATICA : UN ENFOQUE METODICO				
Etapa	***Productos Terminados***	**Requerimientos**	**Responsables**	**Involucrados**
PRELIMINAR : DIAGNOSTICO DE LA SITUACION ACTUAL	**1. DIAGNOSTICO DE NEGOCIO**	1.1.MISION Y OBJETIVOS DE NEGOCIO	L.P. / R.A.I.	A.D.
		1.2. ORGANIZACION DE INFORMATICA	L.P. / R.A.I.	A.D.
		1.3. GRADO DE APOYO AL NEGOCIO	L.P. / R.A.I.	A.D. / P.U.
	2. DIAGNOSTICO DE INFORMATICA	2.1. MISION Y OBJETIVOS DE LA FUNCION DE INFORMATICA	L.P. / R.A.I.	R.I.
		2.2. ORGANIZACION DE INFORMATICA	L.P. / R.A.I.	R.I.
		2.3. CONTROL (FORMALIDAD)	L.P. / R.A.I.	R.I. / P.I.
		2.4. PRODUCTOS Y SERVICIOS	L.P. / R.A.I.	R.I.
JUSTIFICACION:	**1. HACER MATRIZ DE RIESGOS**	1.1. MATRIZ DE RIESGOS	L.P. / A.I.	R.A.I.
	2. HACER PLAN DE AUDITORIA DE INFORMATICA (GLOBAL)	2.1. PLAN DE INFORMATICA GENERAL	L.P.	R.A.I. / A.I.

NOMENCLATURA :	A.D. = ALTA DIRECCION P.U. = PERSONAL USUARIO R.I. = RESPONSABLE DEL AREA DE INFORMATICA
	P.I. = PERSONAL DE INFORMATICA R.A.I. = RESPONSABLE DEL AREA DE AUDITORIA DE INFORMATICA
	L.P. = LIDER DEL PROYECTO DE AUDITORIA DE INFORMATICA A.I. = AUDITOR DE INFORMATICA

Figura 6-1

6.1.1. Conocimiento del Negocio

El Auditor de Informática debe conocer el tipo de organización, la misión, estrategías, planes (de ser posible al menos sus proyectos globales), nivel jerárquico que tiene la Función de Informática, los procesos básicos de negocio, así como las entidades externas al negocio que se relacionan con cada área de negocio.

Los aspectos relevantes que debe solicitar el Auditor de Informática para su análisis preliminar y que emanan de este punto son :

- Misión del Negocio
- Areas o Proceso del negocio
- Organigrama del Negocio (Detectar ubicación de Informática)
- Relación entre las diversas áreas del negocio
- Relación del Negocio con áreas externas (Clientes, Proveedores, por ejemplo)
- Organigrama
- Políticas referentes a Informática
- Otros de Interes para el Auditor de Informática de acuerdo a las características propias del proyecto

6.1.2. Apoyo al negocio

El Auditor de Informática **debe obtener una concepción inicial del grado de apoyo y satisfacción** que existe en el negocio, debe ubicar al menos una estimación de hacía donde se orienta el soporte de la Función de Informática :

- Apoyo a la Alta Dirección (Sistemas de Información Estratégica, Tecnología, Etc.)
- Apoyo a las Gerencias (Sistemas de Información Integrales, Tecnología, etc.)
- Apoyo a Niveles Operativos (Sistemas de Información básicos, Tecnología, Etc.)

Debe conocer de manera general los siguientes aspectos :

- Involucración de la Función de Informática en los proyectos claves del negocio
- Difusión de las Políticas y Planes de Informática en los niveles Estratégico, Táctico y Operativos del Negocio
- Imagén de Informática que tiene la Alta Dirección y Responsables de cada área del Negocio
- Grado de Satisfacción que existe por cada servicio prestado por la Función de Informática
- Expectátivas que tiene el negocio por Informática
- Fortalezas de Informática y debilidades de Informática
- Areas de Oportunidad (Propuestas ya sea por la Alta Dirección, Usuarios o Informática)
- Otros de Interes específico del Auditor de Informática

6.2. Diagnóstico de Informática (Responsables de la Función)

6.2.1. Conocimiento de la Función de Informática

En este parte de la etapa Preliminar el Auditor de Informática pretende conocer :

- La estructura interna de Informática
- Funciones
- Objetivos
- Estrategías
- Planes
- Políticas
- De manera general la Tecnología de Software y Hardware en que se apoya para llevar a cabo su Función dentro del negocio.
- Otros de interes específico para el Auditor de Informática

Se busca tambien obtener la Información relacionada con algunos aspectos que han sido indagados con los usuarios y la Alta dirección con el objetivo de encontrar la consistencia o en su defectos las discrepancias entre una opinión y la otra.

Las entrevistas deben efectuarse con el responsable de Informática y ocasionalmente con los encargados directos de las funciones claves de esta área. La importancia de concientizarlos en la necesidad y provecho que brinda su apoyo a este tipo de proyectos es indispensable, el Auditor de Informática debe ser profesional y ético en su trabajo para brindarles la seguridad de que al final todo redundará en beneficios para todos los involucrados (la dirección, los usuarios e Informática).

El hacer un equipo de trabajo unido es un aspecto muy positivo en cualquier proyecto, los de Auditoría de Informática no son la excepción, se requiere que el Lider del Proyecto desarrolle en la etapa preliminar una buena comunicación con el personal de Informática, lo que podrá ser logrado en gran medida si entiende satisfactoriamente los logros, debilidades y fortalezas tecnológicas, humanas y organizacionales del personal que integra la Función de Informática.

En caso de que el Auditor de Informática revise vaga e informalmente la información aqui recomendada o simplemente omita su busqueda, corre el riesgo de planear o sugerir proyectos que no tengan el alcance requerido para asegurar que todas las áreas de oportunidad y aspectos de riesgo sean contemplados o evaluados.

6.2.2. Servicios

Un aspecto clave a considerar en la Etapa Preliminar es la evaluación general de los servicios que presta Informática a las diferentes áreas del negocio y en los diferentes niveles organizacionales.

El Auditor de Informática puede ya formarse un juicio inicial de la congruencia que existe entre las áreas usuarias y el responsable de Informática, aqui se detecta por lo general que servicios ya son aceptados formalmente en el negocio como estratégicos y cuales son meramente operativos o necesarios para llevar a cabo tareas que no producen valor agregado.

El objetivo de conocer su opinión respecto a esto es encontrar una consistencia entre lo que es su función y lo que dice la Alta Dirección que debe ser. No se busca crear controversias, ni de encontrar fallas personales.

El Auditor de Informática tiene la responsabilidad moral de darle un sentido crítico y práctico para orientar los esfuerzos de todas las áreas del negocio a 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 del negocio involucradas en este tipo de proyectos.

Los servicios que brinda generalmente Informática son :

- Implantación de Soluciones de Información :
  - Desarrollo de Sistemas de Información :
  - No integrados - Integrales - Estratégicos
  - Compra y adecuación de Aplicaciones hechas por externos
  - Bases de Datos :
    - Centralizadas - Descentralizadas
- Evaluación, Adquisición, Instalación y Reemplazo de :
  - Equipo de Computo
  - Paquetes de Software (Procesadores de palabras, Hojas de Cálculo, etc.)
  - Equipos de Telecomunicaciones
  - Lenguajes de Programación
- Mantenimiento :
  - Sistemas de Información
  - Base de Datos
  - Equipos de Computo y de Telecomunicaciones
  - Redes Locales
- Soporte a Usuarios
  - Capacitación y Asesoria
- Investigación :
  - Tecnología (Equipos de Computo, Comunicaciones, CASE, EDI, etc.)
- Otros de acuerdo al tipo de negocio

6.2.3. Aspectos de Control

Otra actividad de la Etapa preliminar para el Auditor de Informática **es el evaluar el Grado de Formalidad y Cumplimiento que se le da a las Políticas, Controles y Procedimientos relativos a cada una de las áreas de Informática.**

Una manera de obtener dicha información es a traves de la entrevista que concede el responsable de Informática al Lider de Proyector o una manera más directa es entrevistar a cada uno de los encargados de cada una de las áreas que conforman la Función de Informática, evitando caer en el detalle y ocupar mucho tiempo en las entrevistas.

Algunos aspectos que deben ser considerados, son al menos los siguientes :

- Políticas y Procedimientos de Organización de la Función de Informática :
  - Descripción de Puestos y Funciones - Evaluación de Desempeño
- Políticas y Procedimientos para el Desarrollo e Implantación de Sistemas
- Políticas y Procedimientos de Evaluación de Hardware y Software
- Políticas y Procedimientos de Seguridad
- Políticas y Procedimientos de Mantenimiento
  - Preventivo - Detectivo - Correctivo
- Plan de Contingencias
- Otros de Interes específico del Auditor de Informática

La actividad inicial de la siguiente Etapa, que es la de Justificación, depende en alto grado de los resultados y observaciones relativos al control emanados de los puntos de control mencionados anteriormente.

7. Etapa de Justificación :

7.1. Matriz de Riesgos / Justificación por Area de revisión

7.2 Plan General del Proyecto de Auditoría de Informática

7. Etapa de Justificación :

Una vez que se ha concluido la **Etapa Preliminar** (Cuando todas las tareas se han terminado satisfactoriamente y se obtuvierón los Productos Terminados para esa fase) se procede a continuar con la Etapa de Justificación (**Figura 6-1**), la cual se explicará a continuación.

Etapa Preliminar
(Terminada)

Etapa de Justificación
(En ejecusión)

Etapa de Adecuación
(Posterior)

Nota : Es Factible que el Lider del Proyecto de Auditoría de Informática desee realizar algunas actividades en paralelo, lo cual es muy valido y justificado si se cuenta con los recursos necesarios y la experiencia en este tipo de proyectos.

Volviendo a la descripción de la **Etapa de Justificación** diremos concretamente que es aquí donde se justifica la Revisión o Evaluación de las áreas o funciones críticas relacionadas con Informática.

Los Productos terminados más importantes de la etapa son tres :

1. Matriz de Riesgos 2. Plan General de Auditoría de Informática 3. Vo. Bo. por escrito

Cada uno de ellos forma parte escencial del Proceso Metodológico, el primero porque define las Areas que serán auditadas, el segundo porque establece las tareas, tiempos, responsables, etc. del Proyecto y el tercero debido a que le da el visto bueno al Lider de proyecto para continuar con las siguientes etapas contempladas en el Plan general.

7.1. Matriz de Riesgos / Justificación por Area de revisión

La siguiente tarea a realizar por el Auditor de Informática en la presente étapa (Justificación) es elaborar la Matriz de Riesgos, cuyo objetivo principal es detectar las áreas de mayor riesgo que existene en relación a Informática y que requieren una revisión de manera formal y oportuna.Las tareas, productos terminados, responsables e involucrados vienen en la **Figura 6-1**

En las **Figuras 7-1, 7-2** se muestra el contenido que debe tener **la Matriz de Riesgos**

MATRIZ DE RIESGOS

EMPRESA : **GERENCIA :** **FECHA DE ELABORACION :**
REPRESENTANTE USUARIO : **REPRESENTANTE INFORMATICA:** **LIDER DEL PROYECTO :**

AREAS SUSCEPTIBLES DE AUDITAR	APECTOS O COMPONENTES A EVALUAR DEL AREA	RIESGO POR COMPONENTE	CLASIFICACION DEL RIESGO POR AREA(TOTAL)	AREAS A AUDITAR SEGUN CLASIFICACION
ADMINISTRACION DE INFORMATICA	1. Misión y Objetivos	%	%	
USUARIOS DE INFORMÁTICA	1.Comunicación e Integración	%	%	
CONTROL INTERNO	1. Políticas y Procedimientos	%	%	
METOLODOLOGIA DE DESARROLLO (CDISI)	1. Metodología	%	%	
SISTEMAS DE INFORMACION	1. Operación	%	%	
MANTENIMIENTO	1. Hardware 2. Sistemas de Información	% %	%	
REDES LOCALES	1. Administración	%	%	

Figura 7-1

MATRIZ DE RIESGOS

EMPRESA : **GERENCIA :** **FECHA DE ELABORACION :**
REPRESENTANTE USUARIO : **REPRESENTANTE INFORMATICA:** **LIDER DEL PROYECTO :**

AREAS SUSCEPTIBLES DE AUDITAR	APECTOS O COMPONENTES A EVALUAR DEL AREA	RIESGO POR COMPONENTE	CLASIFICACION DEL RIESGO POR AREA(TOTAL)	AREAS A AUDITAR SEGUN CLASIFICACION
SOFTWARE : **(Paquetes de uso generalizado, Lenguajes de Programación, Sistemas Operativos, Paquetes de uso específico)**	1. Administración 2. Legalización	% %	%	
SEGURIDAD	1. Hardware 2. Software / Aplicaciones 3. Plan de contingencias y de Recuperación	% % %	%	(Secuencia Sugerida para Auditar cadaComponente y cada Area según el Nivel de Riesgo Estimado)
OTROS DE INTERES ESPECIFICO PARA EL AUDITOR DE INFORMATICA				

Figura 7-2

Nota : Las áreas de Revisión y los componentes de cada área mencionados en las Tablas anteriores son sugerencias que tratan de orientar a los Auditores de Informática, el orden y los aspectos mencionados no son estrictamente los que deben aplicarse, se pueden adecuar y/o agregar y/o eliminar de acuerdo al criterio y características propias del negocio que afecten al proyecto.

7.1. Matriz de Riesgos / Justificación por Area de revisión

Si de aquí emanan anomalías de considerable importancia, en alguno de sus elementos evaluados, se deben tomar acciones inmediatas orientadas a minimizar y/o eliminar la anomalía (Se plantearán en el Plan de Auditoría de Informática como acciones Inmediatas).

Se debe determinar el nivel de Riesgo que existe en cada una de las áreas de la Función de Informática : *Cada área, producto o servicio de Informática es susceptible de evaluación y control para el aseguramiento de que se desarrolle de acuerdo a los estandares, políticas y procedimientos especificos que le han sido asignados de acuerdo a su función.*

7.2. Plan General del Proyecto de Auditoría de Informática

Una vez elaborada, revisada y documentada la **Mátriz de Riesgos** de acuerdo a los riesgos más relevantes se procede a la Formulación del Plan General de Informática, el cual consiste basicamente en plantear las tareas más importantes que se llevarán durante un cierto periodo al efectuar la Auditoría de Informática (**Ver Figura 7-3**).

Las actividades principales a ejecutar por el Auditor de Informática o por el Lider del Proyecto para la elaboración del Plan General son al menos las siguientes :

* Estimar el tiempo que le llevará el auditar cada área determinada en la Matriz de Riesgos y en las tareas de apoyo para lograr las Areas de Oportunidad planteadas.

* Analizar y definir cuales serán los aspectos o componentes más relevantes a evaluar

* De ser necesario verificar su importancia y validez con los involucrados sin llevarse mucho tiempo y tecnisismos en las entrevistas (Puede ser via telefónica, fax o personalmente)

* Asignar prioridades a cada área a evaluar o revisar en conjunto con los principales involucrados en el proyecto

* Definir fechas estimadas de Inicio y Terminación por Area de Revisión, no por componente.

* Otras de Interes para el Auditor de Informática de acuerdo a las características del Proyecto y el negocio

PLAN GENERAL DE AUDITORIA DE INFORMATICA (ETAPA DE JUSTIFICACION)

EMPRESA : **GERENCIA :** **FECHA DE APROBACION :**
REPRESENTANTE USUARIO : **REPRESENTANTE INFORMATICA:** **LIDER DEL PROYECTO :**

AREAS A AUDITAR SEGUN CLASIFICACION Y PRIORIDADES	APECTOS O COMPONENTES DEL AREA A AUDITAR	PRIORIDAD ASIGNADA	CLASIFICACION DEL RIESGO POR AREA(TOTAL)	FECHA DE INICIO / FECHA DE TERMINACION
AREA SELECCIONADA	**Componente (s) Seleccionado (s) del Area**	Número :	%	**dd / mm / aa** **dd / mm / aa**
AREA SELECCIONADA	**Componente (s) Seleccionado (s) del Area**	Número :	%	**dd / mm / aa** **dd / mm / aa**
AREA(S) SELECCIONADA(S)	**Componente (s) Seleccionado (s) del Area**	Número :	%	**dd / mm / aa** **dd / mm / aa**

Figura 7-3

Nota : **Algunos datos pueden ser omitidos o agregados según considere pertinente el Auditor de Informática, sin olvidar que en la Etapa de Formalización se dará todo el detalle requerido del Proyecto de Auditoría de Informática**

8. Etapa de Adecuación (Adaptación a características del Negocio) :

8.1. Plan detallado del Proyecto de Auditoría Informática

8.2. Aspectos a evaluar por Area de Revisión

8.3. Definición de Técnicas y Herramientas a utilizar por Area de revisión

8.4. Definición y/o Actualización de Estandares, Políticas y Procedimientos a verificar por Area de Revisión

8.5. Elaboración y/o Actualización de Cuestionarios por Area de Revisión

8. Etapa de Adecuación (Adaptación a características del Negocio) :

La Etapa que ahora nos ocupa es la que se enfoca al análisis, adecuación y actualización de todos los elementos que se involucran en un Proyecto de Auditoría de Informática pero a un nivel detallado.

Las tareas ejecutadas en la **Etapa de Adecuación** tienen como objetivo principal el adaptar todo el proyecto a las características del negocio, sin olvidar la referencia de los estandares, políticas y procedimientos de Auditoría de Informática comunmente aceptados y recomendados por las Asociaciones relacionadas con Auditoría de Informática, así como las formuladas y aprobadas de manera particular en los negocios para Informática.

Las tareas, Productos Terminados, Responsables e Involucrados de la **Etapa de Adecuación** se encuentran en la **Figura 8-1**

Etapa de Justificación
(Terminada)

Etapa de Adecuación
(En ejecusión)

Etapa de Formalización
(Posterior)

EL PROCESO METODOLOGICO DE LA AUDITORIA DE INFORMATICA : UN ENFOQUE PRACTICO				
Etapa	**Productos Terminados**	**Requerimientos**	**Responsables**	**Involucrados**
ADECUACION	1. DEFINIR ETAPAS DEL PROYECTO Y SU DETALLE	1.1. ETAPAS Y SUS TAREAS		
		1.2. PLAN ACTUALIZADO	A.I. / L.P.	R.A.I.
		1.3. RESPONSABLES E INVOLUCRADOS	A.I.	L.P.
		1.4. PRODUCTOS TERMINADOS	A.I.	L.P.
		1.5. REVISIONES (FORMAL E INFORMAL)	A.I.	L.P.
	2. ASPECTOS A EVALUAR POR AREA SELECCIONADA	2.1. ASPECTOS O ELEMENTOS A EVALUAR POR CADA AREA DE REVISION	A.I.	L.P.
	3. ESTABLECER TECNICAS Y HERRAMIENTAS A UTILIZAR POR AREA DE REVISION	3.1. TECNICAS A UTILIZAR	A.I.	L.P.
		3.2. SOFTWARE A UTILIZAR	A.I.	L.P.
		3.3. EQUIPO DE COMPUTO A UTILIZAR	A.I.	L.P.
		3.4. OTROS DE INTERES AL AUDITOR	A.I.	L.P.
	4. DEFINICION Y/O ACTUALIZACION DE POLITICAS POR AREA	4.1. POLITICAS Y PROCEDIMIENTOS A VERIFICAR DE ACUERDO A CADA AREA QUE SERA AUDITADA	A.I.	L.P.
		4.2. ESTANDARES POR AREA	A.I.	L.P
	5. ELABORACION Y/O ACTUALIZACION DE CUESTIONARIOS POR AREA	5.1. CUESTIONARIOS PARA APLICARSE DE ACUERDO A CADA AREA QUE SERA AUDITADA	A.I.	L.P.
		5.2. CUESTIONARIOS ADICIONALES	A.I	L.P.

NOMENCLATURA : A.D. = ALTA DIRECCION P.U. = PERSONAL USUARIO R.I. = RESPONSABLE DEL AREA DE INFORMATICA
P.I. = PERSONAL DE INFORMATICA R.A.I. = RESPONSABLE DEL AREA DE AUDITORIA DE INFORMATICA
L.P. = LIDER DEL PROYECTO DE AUDITORIA DE INFORMATICA A.I. = AUDITOR DE INFORMATICA

Figura 8-1

8.1. Plan detallado del Proyecto de Auditoría Informática

Esta es, sin duda una de las tareas más importantes de la **Etapa de Adecuación**, ya que en ella se define todo el detalle de los elementos involucrados en el proyecto, se especifican tareas, productos terminados, responsables, fechas, etc. que serán validadas y aprobadas en la **Etapa de Formalización** para arrancar el Proyecto definitiva y formalmente.

Plan Detallado de Auditoría de Informática : Es el que detalla la información relacionada con :

* El desarrollo de la Auditoría de Informática (Auditoría a las Areas seleccionadas en la fase de Justificación)

* La documentación, la revisión y aprobación del Informe de Auditoría de Informática

Los datos mencionados en el Plan Detallado de informática se enfocan a ser la guía del Proyecto de Auditoría de Informática desde el punto de vista del cliente ya que describe las tareas, productos terminados, responsables, involucrados, fechas de revisión, etc.

Aspectos relevantes del Plan Detallado de Auditoría de Informática :

+ Especifica Responsables e Involucrados en cada Area a Auditar
+ Es el detalle final del Plan
+ Ya fué adaptado y actualizado en base a caractrísticas especifícas del proyecto
+ Otros

8.2. Aspectos a evaluar por Area de Revisión

Los aspectos o componentes a evaluar ya fuerón mencionados en la Matriz de Riesgos, lo que procede en esta tarea es hacer una verificación de si son las requeridas y si los objetivos de las áreas mencionados son válidos y completos

Es recomendable que las Areas Susceptibles de Auditar y los componentes de cada Area que sean agregados por el Auditor de Informática en el momento de que un proyecto así lo requiera, se les elaboren los cuestionarios correspondientes y de ser posible que sean manejados en los formatos y secuencia de tareas aquí sugeridos para no perder continuidad.

8.3. Definición de Técnicas y Herramientas a utilizar por Area de revisión

Aquí se especifican las Técnicas y Herramientas recomendadas que debe conocer amplia y satisfactoriamente el Auditor de Informática para la revisión con conocimiento de causa de cada una de las Areas plasmadas en el Plan Detallado.**(Ver Figuras 5-2 y 5-3)**

La experiencia profesional que se haya obtenido en cada una de las áreas (Desarrollo, Telecomunicaciones, Mantenimiento, Administración de Informática, etc.) hacen más viable una auditoría y definición de soluciones eficiente y sin contratiempos.

No es un presagio negativo el no haber trabajado en las Areas que serán auditadas, simplemente el grado de investigación y actualización en los temas o aspectos que serán evaluados debe ser más profundo.

Es casi imposible asegurar que todos los Auditores de Informática dominan todas las Areas de Informática susceptibles a auditarse, sin embargo el Auditor de Informática debe especializarse y actualizarse en medida de lo posible en las Areas que el considere criticas para su negocio o especificamente de los requerimientos que van surgiendo a lo largo de su trabajo, no debemos olvidar por ultimo, que debemos ser proactivos, no reactivos.

8.4. Definición y/o Actualización de Estandares, Políticas y Procedimientos a verificar por Area de Revisión

Todas las acciones operativas y administrativas de las organizaciones deben ser direccionadas en base a lineamientos, políticas y procedimientos, con el objetivo principal de que los individuos que en ella laboran, lo hagan en forma metódica (sin entenderse como un trabajo mecánico y robotizado), con estandares de negocio o con normas de calidad y productividad comunmente aceptadas en negocios similares al mismo giro de empresa.

Además existen Asociaciones Profesionales, Instituciones Educativas, etc. que orientan a los individuos a trabajar de una manera productiva y especializada.

En lo que se refiere a Estandares, Políticas y Procedimientos se aclara que las actividades y elementos que se involucran con Informática se manejan con este criterio de operar bajo estandares comunmente aceptados en el medio ambiente de dicho campo.

Las funciones de Desarrollo e Implantación de Sistemas de Información, al igual que las de Planeación de Informática o las de Telecomunicaciones e Investigación se encuentran en un marco nacional e internacional donde existen estandares, metodologías, técnicas y herramientas de trabajo recomendadas para un desempeño eficiente de cada una de las actividades inherentes a sus tareas.

¿Como se definen los Estandares, Políticas, Procedimientos de Auditoría de Informática ?

Al igual que para las funciones de Planeación, Telecomunicaciones, etc. existen Asociaciones Nacionales e Internacionales que se integran por profesionistas de gran experiencia y conocimiento en el campo, que se enfocan a establecer, formalizar, difundir y recomendar la aplicacion de los estandares, políticas y procedimientos más convenientes a las necesidades actuales y futuras de la área de especialización a la que ellos se dediquen.

Se menciona a continuación las ventajas que tienen las Asociaciones Nacionales e Internacionales en lo referente al punto que se está tratando :

+ Los estandares 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 de Informática
+ Cursos y seminarios son impartidos continuamente
+ Se pueden cambiar experiencias con miembros de diferentes empresas y paises
+ Otras

8.5. Elaboración y/o Actualización de Cuestionarios por Area de Revisión :

Cada entrevista, visita o verificación que vaya a realizarse en la Etapa de Desarrollo de la Auditoría de Informática (Reflejada en el Plan Detallado de Auditoría de Informática como la Evaluación de las Areas Seleccionadas) debe ser soportada por preguntas específicas y definidas previamente.

La forma en que se aplicarán los cuestionarios, puede ser a traves de una entrevista personal con los involucrados en el proyecto (Usuarios o personal de Informática), por medio de visitas de verificación física (Evaluando los equipos y materiales de informática de interes para el proyecto) o la aplicación de checklists (Lista de preguntas breves y concretas) orientadas a personal que requiere 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 más importantes que deben cubrir los cuestionarios son al menos los siguientes : Actualizadas, orientadas a los aspectos evaluados, no redundantes, concretas, técnicas y basadas si es posible en estandares .

A CONTINUACION SE DESGLOSAN LOS CUESTIONARIOS SUGERIDOS PARA APLICAR LA AUDITORIA DE INFORMATICA, LA FORMA, LA SECUENCIA DE APLICACION, LAS PREGUNTAS COMPLEMENTARIAS U OTROS ASPECTOS QUE DESEEN SER EVALUADOS CON CUESTIONARIOS ADICIONALES SE RECOMIENDA SEAN ELABORADOS FORMALMENTE PARA EFECTUAR UNA EVALUACION COMPLETA Y VERAZ.

CUESTIONARIOS PARA EFECTUAR LA AUDITORIA DE INFORMATICA POR AREAS DE REVISION

ADMINISTRACION DE INFORMATICA

USUARIOS DE INFORMATICA

CONTROL INTERNO

METODOLOGIA DE DESARROLLO (CDISI)

SISTEMAS DE INFORMACION

MANTENIMIENTO

REDES LOCALES

SOFTWARE

SEGURIDAD

Nota : Al aplicar cada uno de los siguientes cuestionarios recomendados se debe tomar como referencia a las figuras 5-2 y 5-3 que muestran algunas de las Técnicas sugeridas para el desarrollo de la Auditoría de Informática.

Dichas figuras podrán ser complementadas con el uso de Técnicas y Herramientas especifícas recomendadas comunmente por los especialistas de cada una de las áreas que serán evaluadas.

OBJETIVOS DE ESTA REVISION :

- Verificar que se 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 Ambiente de Informática

- Asegurar que los recursos de Informática (Hardware, Software, Telecominunicaciones, Servicios, Personal, Etc.) sean orientados a los objetivos y las estrategías del negocio.

- **Verificar que exista una :**
  - Elaboración y Formalización de Planes de Informática
  - Organización y control formal sobre los recursos de Informática
  - Dirección, coordinación y control de los proyectos de Informática

- Verificar 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

ADMINISTRACION DE INFORMATICA

1. MISION Y OBJETIVOS DE INFORMATICA

ADMINISTRACION DE INFORMATICA

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla al responsable y/o encargados de Informática

ADMINISTRACION DE INFORMATICA

1. MISION Y OBJETIVOS DE INFORMATICA

Aspectos Claves a Evaluar

1. ¿ Existe un documento formal que describa claramente los siguientes aspectos :
   - Misión de Informática en el Negocio
   - Estructura Organizacional de la Función
   - Roles dentro de la organización
   - Funciones y actividades por cada puesto existente en el organigrama
   - Planes de Informática (Corto, Mediano y Largo Plazo)
   - Políticas y Procedimientos de Informática
   - Otros

1.1. ¿ Si el documento no existe, cuál ha sido la causa o motivos para no hacerlo formalmente (en documento) ?

2. ¿ En caso de que exista dicho documento, fué el mismo comentado con las áreas internas de Informática, Areas Usuarias y con la Alta Dirección respectivamente ?

3. ¿ Si es así cual fué el procedimiento que se utilizó :
   - Juntas
   - Vía memorandum´s, circulares, etc.
   - Platicado en un reunión informal
   - Inducción al momento de que el personal de Informática ingresa al negocio
   - Otros

4. ¿ Fué aprobado por la Alta Dirección ?

5. ¿ Está conciente el personal de Informática de la importancia que tiene el orientar los esfuerzos al cumplimiento formal y oportuno de : La misión, objetivos, estrategías y de las Políticas y Procedimientos de la Función de Informática ?

6. ¿ Se encuentran bien establecidos y entendidos los Roles de Informática en la organización ?

6.1. ¿ Cuales son dichos roles desde un punto de vista objetivo y práctico ?

6.2. ¿ Son los roles que se ejercen actualmente los requeridos por el negocio ?

6.3. En caso de que los roles deban ser actualizados o complementados ¿ que descripción les daría a los roles requeridos para un apoyo más significativo al negocio

7. ¿ Existe un Cómite de Informática ?

7.1. ¿ Quienes forman parte del Cómite de Informática?

7.2. ¿ Cuales son los objetivos y funciones principales del Cómite ?

1. MISION Y OBJETIVOS DE INFORMATICA

8. ¿ Existe una Estructura formal de Informática (Manual, Documento, etc.) que contemple al menos lo siguiente :

- Organigrama
- Descripcion 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

9. ¿Tiene el responsable de Informática o la Alta Dirección planeado algún cambio significativo en la estructura de Informática para los próximos doce meses ?

10. ¿ Cuáles de los siguientes fáctores negativos se presentan actualmente en la Función de Informática :

- Improductividad
- Falta de Motivación
- Imagen negativa en el negocio
- Otros

11. ¿ Existe un catalogo de servicios de informática ? ¿Está acorde a las necesidades actuales del negocio?

12. ¿ Cuando existen servicios de Informática proporcionados por terceros y que tienen un alcance periodico y estratégico en el negocio (Planeación de Informática, Desarrollo de Sistemas, Asesoría al personal usuario y/o Alta Dirección y/o Informática, etc.) se integran al catalogo de servicios ?

13. ¿ Existe un procedimiento formal de seguimiento al desempeño y rendimiento del personal de Informática ? ¿ En que consiste? ¿ Como se lleva a la práctica ? ¿ En que periodos?

14. ¿ Otros aspectos que considere relevantes para el mejoramiento de la Administración de la función de Informática?

USUARIOS DE INFORMATICA

1. COMUNICACION E INTEGRACION

OBJETIVOS DE ESTA REVISION :

- Detectar el grado de confianza, satisfacción y respaldo que perciben los usuarios de parte de la Función de Informática.

- 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 (detalle) por los usuarios y que este entendimiento sea congruente con la realidad.

La calidad, oportunidad, utilidad y confiabilidad real de cada uno de los Sistemas de Información debe ser definida por el auditor y validado por los responsables de Informática y de los Usuarios.

- Verificar el grado de involucración de los usuarios en

proyectos especifícos,como pueden ser el Desarrollo de Sistemas, Evaluacióny Adquisición de Paquetes que serán utilizadospor los mismos usuarios, Etc.

- Verificar Si existen procedimientos formales para el seguimiento de la comunicación entre los usuarios e Informática.

- Verificar si existe un cómite formal integrado por representantes de Informática y de los Departamentos Usuarios.

USUARIOS DE INFORMATICA

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla al responsable y/o encargados del (os) Departamento(s) Usuario(s)

USUARIOS DE INFORMATICA

1. COMUNICACION E INTEGRACION :

Aspectos Claves a evaluar

1.- ¿Conocen las áreas usuarias la misión de Informática en la empresa ?

2.- ¿Conocen Cuales son los roles de Informática en la empresa ?

2.1. ¿Conocen los Usuarios los Servicios y Productos proporcionados por Informática ?

3.- ¿Ha difundido el Area de Informática a las Areas Usuarias los conceptos anteriores de manera formal ?

3.1. ¿Están por escrito ?

3.2. ¿Como lo han difundido (reuniones entre las áreas usuarias - Informática, etc.)

3.3. ¿Fuerón aprobados formalmente ?

4.- ¿Existe un compromiso formal de parte de las Areas Usuarias para cooperar en lo necesario con 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 cómite integrado por los Usuarios e Informática ? ¿ Que hace dicho cómite?

5.- ¿Si no hay cómite, quien se hace responsable de la función de informática por parte de las áreas usuarias ?

6.- ¿Como se difunde a las áreas usuarias los roles y responsabilidades de Informática a traves de la organización ?

7 .- ¿Existen sugerencias que considere los usuarios que puedan apoyar a los objetivos estrategías, roles y responsabilidades de la Organización por medio de los servicios de la Informática ? ¿ Cómo las han externado a Informática ?

8. ¿Como considera usted el nivel de comunicación que existe entre ustedes e Informática actualmente ? ¿Porque ?

9. ¿Como se aseguran que los compromisos de apoyo, seguimiento y aprobación a proyectos de Informática para las áreas usuarias se lleve a cabo oportuna y formalmente ?

1. COMUNICACION E INTEGRACION :

10..- ¿Conoce cuales son los proyectos a corto, mediano y largo plazo donde el usuario deba involucrarse ? ¿Como los difundio Informática? ¿ Se han dado los resultados esperados?

11 ¿ Si es así, que tipo de proyectos serán o están siendo desarrollados en conjunto con Informática : (mencionelos y clasifiquelos por orden de Importancia para usted) ?

12. ¿ El proceso utilizado para la elaboración y formalización de los proyectos se basa en alguna metodología formal utilizada por Informática o en las demás áreas del negocio ?

13. ¿ Que procedimiento o actividad se realiza para verificar avance y Calidad en los proyectos ? ¿quien lo lleva a cabo ?

14. ¿ En caso de existir inconsistencias entre los proyectos que acciones se llevan a la práctica ?

15.- ¿Ha difundido la Función de Informática los productos y Servicios que ofrece a los usuarios ? ¿ Si es así, como los difundieron? ¿ Son acordes a sus necesidades reales?

16.- ¿Que opina de los productos o servicios que usted está utilizando ? (especifique por servicio)

17.- ¿Existe(n) algun(os) Requerimiento(s) en su departamento que no esten apoyados por los productos y servicios de la Función de Informática ?

18.- ¿Según su opinión se da atención oportuna y formal a las solicitudes de servicios que usted hace ?

19. ¿ sugerencias para mejorar los Servicios y Productos de Informática?

20.- ¿Le brinda Informática cursos de capacitación ? ¿Son formales ? ¿Oportunos?

21. Respecto a los recursos de Informática (Aplicaciones, Equipos de Computo, Paquetes de Software) que existen en sus departamentos (áreas usuarias) ¿ Quien es el responsable de su administración? ¿Cómo se lleva a cabo? (especifique por tipo de recurso)

CONTROL INTERNO

1. POLITICAS Y PROCEDIMIENTOS

OBJETIVOS DE ESTA REVISION :

- Detectar el grado de estandarización y seguimiento formal que existe en el medio ambiente de Informática

- 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
  - Soporte a Usuarios (Capacitación, Aseoría en HW, SW, Aplicaciones, etc.)
  - Desarrollo e Implantación de Sistemas de Información
  - Mantenimiento de Sistemas de Información
  - Operación de Sistemas de Información
  - Automatización de Oficinas
  - Otras específicas en su negocio

- Verificar y asegurar el cumplimiento oportuno y formal de las Políticas y Procedimientos relacionados con la función de Informática

CONTROL INTERNO

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla al personal de Informática y a los usuarios

CONTROL INTERNO
POLITICAS Y PROCEDIMIENTOS

Aspectos Claves a Evaluar

1. ¿ Existen Políticas y Procedimientos formales (Aprobados por el Responsable de Informática y/o Alta Dirección y/o Auditoría de Informática relativos a la Administración de cada una de las funciones de Informática ?

1.1. Si es así, Mencionelas a continuación, explicando brevemente en que consiste cada una de ellas y las acciones que ejecuta para asegurar que se difundan, se entiendan, se cumplan y se les de seguimiento formal y oportunamente.

Area / Función	**Políticas / Procedimientos**	**Descripción y Objetivos**	**Acciones para Cumplimiento (Seguimiento)**
Soporte a los Usuarios (Capacitación, Asesoría, etc.) Desarrollo e Implementación de los Sistemas de Información *Mantenimiento / Actualización a los Sistemas de Información* Operación de Sistemas de Información Auditoría de Informática **Otras específicas en su negocio**			

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 Control Interno (o Funciones Similares) ?

2.1. Si es así, ¿ Cuales son las tareas y actividades que lleva a cabo ? ¿ En que periodos efectua dicha evaluación? ¿ Que tipo de informes presenta y a quienes lo entrega? ¿ Como se le da seguimiento a sus recomendaciones?

2.2. Dicha función verifica el grado de actualización que requieren dichas Políticas y Procedimientos para satisfacer los objetivos de control requeridos por el negocio ?

POLITICAS Y PROCEDIMIENTOS

3. ¿ Que acciones de Control se llevan a cabo cuando algunas de las siguientes funciones no cuentan con Políticas y Procedimientos que asegueren al negocio que la implantación, operación de tales servicios y productos no alteren la Integridad, veracidad y Confidenciabilidad requerida en el manejo de la Información del negocio :

CONCEPTO	ACCIONES DE CONTROL
- Soporte a Usuarios	
- Desarrollo e Implantación de Sistemas de Información	
- Mantenimiento de Sistemas de Información	
- Operación de Sistemas de Información	
- Otras específicas en su negocio ?	

4. ¿Existe una adecuada segregación de Funciones para el desarrollo de cada uno de los conceptos antes mecionados ?

METODOLOGIA DE DESARROLLO (CDISI)

1. METODOLOGIA

METODOLOGIA DE DESARROLLO (CDISI)

OBJETIVOS DE ESTA REVISION :

- Asegurar que exista un proceso metodológico para ejecutar el Ciclo de Vida de Desarrollo e Implantación de Sistemas de Información (CDISI) formal y estandarizado en la organización.

- Verificar y asegurar que se utilice la Metodología del CDISI en cada proyecto de Implantación de Sistemas de Información (Evaluar este aspecto durante el desarrollo e implantación de un Sistema de Información).

- Verificar 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 (Aplicable a personal de nuevo ingreso)

- Verificar que exista un curso de orientación basica enfocado al personal involucrado en los proyectos que no pertenece al área de desarrollo y que sin embargo juegan un rol importante en éste tipo de proyectos (Usuarios, Alta Dirección, Auditores, etc.).

METODOLOGIA DE DESARROLLO (CDISI)

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla al responsable y/o encargados del Desarrollo de Sistemas

METODOLOGIA DE DESARROLLO (CDISI)

1. METODOLOGIA

Aspectos Claves a evaluar

1. ¿Existe en su área una Metodología formal de Desarrollo e Implantación de Sistemas ?

2.- ¿Si es asi, contempla dicha metodología los pasos y lineamientos requeridos para la siguiente CLASIFICACION DE PROYECTOS :

a) Desarrollo de Sistemas
b) Compra de aplicaciones de mercado
c) Adaptación de Aplicaciones adquiridas a externos (aplicaciones de mercado)
d) Rediseño de Sistemas ya existentes
e) Otros

3.- ¿Esta documentada dicha metodología formalmente ?

3.1. ¿ Si es así, contempla la documentación al menos cada uno de los siguiente puntos :
- Un panorama general de la metodología
- Equipos de Trabajo sugeridos de acuerdo al tipo de proyecto
- Etapas del Proyecto
- Secuencia de las Etapas
- Responsables e involucrados en cada Etapa
- Productos Terminados a obtener por cada Etapa o Tarea
- Otros que el Auditor de Informática o el Responsable de Informática consideren importantes

4.- ¿En caso de contar con una metodología de Desarrollo e Implantación de Sistemas, la misma, fué desarrollada por Personal de Informática de la empresa, fue comprada o la rentan cuando es requerida ?

5.- ¿Se capacito al personal de desarrollo en el entendimiento y uso práctico de la misma ?

5.1. ¿ Si no se capacito al personal en el uso de la metodología como se asegura su entendimiento y uso eficiente durante los proyectos ?

6.- ¿Se actualiza la metodología cuando es requerido ? ¿Cómo ?

7.- ¿Se documentan formalmente estos cambios ?

8.-¿Capacitan formalmente al personal requerido en la actualización de la metodología ?

9.- ¿ Existe una congruencia de la metodología CDISI con las metodologías recomendadas como estandar en el mercado ?

10. ¿ Conoce el Personal de Informática cuales son las técnicas requeridas para el desarrollo, seguimiento y documentación formal de las Etapas del CDISI mencionadas anteriormente ? ¿ Cuáles son dichas Técnicas y Herramientas ? ¿ Las clasifican por etapa?

11.- ¿Que procedimiento se utiliza para la capacitación al personal de desarrollo en el uso de de dichas Técnicas y Herramientas ?

12 .- Documentar de acuerdo a la siguiente tabla las etapas, tareas, productos terminados y Responsables correspondientes a la Metodología de CDISI utilizadas por la Función de Informática para los Proyectos de Desarrollo e Implantación de Sistemas de Información :

Ciclo sugerido para la Administración de Proyectos de Implantación de Sistemas de Información (Soluciones de Negocio)						
FASES	TAREAS	PRODUCTOS	INVOLUCRADOS	RESPONSABLE	REVISIONES	DURACION
PLANEACION DEL PROYECTO						
ANALISIS DEL SISTEMA						
EVALUACION DE LA APLICACION						
INSTALACION DE LA APLICACION						
DISEÑO DEL SISTEMA						
PROGRAMACION / CONSTRUCCION						
PRUEBAS DEL SISTEMA						
IMPLANTACION DEL SISTEMA						
MEJORAS AL SISTEMA						

SISTEMAS DE INFORMACION :

1. OPERACION

SISTEMAS DE INFORMACION

OBJETIVOS DE ESTA REVISION :

- Verificar la existencia de políticas y procedimientos formales relativos a la operación de los Sistemas de Información

- Verificar que la liberación de los Sistemas que se encuentran en operación haya sido aprobada por los usuarios de manera formal

- Asegurar que existan al menos los controles y procedimientos requeridos para :

  - Entendimiento y uso eficiente de los Sistemas de Información en Operación

  - Documentación (Manuales de Operación)

  - Capacitación Previa a la Operación Inicial y Capacitación a personal de nuevo ingreso que estará involucrado con la operación de los Sistemas

  - Satisfacción de los requerimientos de Usuarios

  - Procedimientos que aseguren la Continuidad en la operación

  - Seguridad en la operación de los Sistemas

  - Totalidad, Mantenimiento, Actualización, Autorización, Exactitud y Registro de datos

- Asegurar que los Sistemas de Información en Operación hayan sido desarrollodos bajo el Proceso Metodológico CDISI establecido por Informática como el estandar en la empresa

SISTEMAS DE INFORMACION

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla al responsable de los Sistemas en Operación (Usuarios e Informática)

SISTEMAS DE INFORMACION

1. OPERACION

Aspectos Claves a evaluar

1.-¿Cuáles son los sistemas de información que usted requiere para el soporte de las funciones y actividades de su Gerencia/área/departamento ?

2.- ¿Cuales de ellos Están en operación/producción de manera formal actualmente ?

3.- ¿Estan los usuarios debidamente capacitados en el uso de los sistemas que operan actualmente ?

4.- Manejan de manera formal y satisfactoria el :

- 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

4.1. ¿ Existen sugerencias para el mejoramiento de cada uno de los aspectos mencionados a continuación para el mejoramiento de la Operación de los Sistemas actuales :

- 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

5.- ¿ Que procedimientos se siguen en la atención y solución de los nuevos requerimientos de su Area para el mejoramiento de los sistemas en Operación?

6.- ¿ Cómo se definierón, autorizarón y difundierón estos procedimientos ?

1. OPERACION

7.- ¿ Existe una función responsable, ya sea de su área o de Informática a darle seguimiento oportuno a dichos procedimientos ?

8. ¿Conocen todos los usuarios que operan los Sistemas dichos procedimientos? ¿Porque?

9. ¿ Considera que los procedimientos anteriormente mencionados son suficientes? ¿Porque?

10.- ¿Existen procedimientos para el manejo de errores o cambios en los sistemas actuales ?

11.- ¿Existe Documentación formal de los Sistemas que se encuentran actualmente en operación?

11.1.- Si la respuesta es afirmátiva verificar si existe al menos la siguiente documentación :

- Manuales de Usuarios
- Manuales de Operación
- Procedimientos de Contingencia y recuperación
- Procedimientos para el manejo del equipo donde se encuentran operando 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 ? ¿Porque ?

14.- Están distribuidos estos manuales donde les corresponde? (Verificarlo mediante observación directa en las áres de los usuarios, de operación y de Informática)

MANTENIMIENTO

1. HARDWARE

2. SISTEMAS DE INFORMACION

MANTENIMIENTO

OBJETIVOS DE ESTA REVISION :

- Verifificar la existencia de políticas y procedimientos formales relativos al Mantenimiento Preventivo y Correctivo del Hardware y los Sistemas de Información dentro de la organización.

- Verificar que el mantenimiento efectuado a los elementos antes mencionados, garantice la continuidad en las operaciones críticas del negocio.

- Verificar que el Area de Informática y las Areas usuarias sean oportunamente informadas de los calendarios de mantenimiento, y en su caso si son mantenimiento de tipo correctivo, debe proveerse a las areas afectadas de los elementos necesarios que les garanticen la continuidad en el manejo de equipo, sistemas y software.

MANTENIMIENTO

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla a los responsables de dar Mantenimiento al Hardware y los Sistemas de Información.

MANTENIMIENTO

1. HARDWARE

Aspectos Claves a Evaluar

1.- ¿Existe una lista del Hardware existente en su negocio (Departamento de Informática y Areas Usuarias) ?

2.- ¿Esta identificado el lugar físico del Hardware y los responsables de su uso y custodia ?

3.- ¿Se cuenta con manuales y/o procedimientos para el manejo del Equipo ?

4.-¿Existe un procedimiento formal, para darle mantenimiento al Hardware ?

4.1. ¿Contempla dicho procedimiento al menos lo siguiente :

- Formulación y Difusión del Plan de Mantenimiento Preventivo/Correctivo
- Difusión del Plan 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 tendrán mantenimiento
- Registro de las actividades realizadas, pendientes y problemas originados durante el Mantenimiento Preventivo/Correctivo

4.2.- ¿ Es este procedimiento valido para :

- Microcomputadoras / Redes Locales
- Minicomputadoras
- Mainframes
- Equipo periferico
- Otro equipo ? (especifique)

5.- ¿ES EL PROCESO DE MANTENIMIENTO HECHO POR EXTERNO/CONTRATO ?

6. ¿ Existen acciones complementarias que apoyen al proceso de Mantenimiento y que registren algunos datos relacionados con el mismo, dichas acciones pueden ser :

- 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
- Procedimientos de Seguridad (Egreso e ingreso del equipo)
- Etc.

MANTENIMIENTO

SISTEMAS DE INFORMACION

Aspectos Claves a evaluar

1.¿Existe una lista de los Sistemas de Información que están en operación actualmente ?

2.- ¿Dichos Sistemas fuerón aprobados formalmente por los usuarios ?

3.- ¿Se cuenta con manuales de usuario, técnicos y de operación para cada uno de los sistemas de información actualmente en producción ?

4.- ¿Están dichos manuales actualizados ? (verificarlo)

5.- ¿Existe un procedimiento formal de mantenimiento a los Sistemas de información ?

6.- ¿Estan Identificados los Sistemas de Información Comprados a externos ?

7.- Existe un mismo procedimiento formal para darle Mantenimiento (Actualización) a los Sistemas de Información instalados en :

- Micros - Minis - Mainframes

7.1.- ¿Se actualiza la Información de los manuales de usuarios, técnicos y de operación cuando así corresponda (verificar con los ultimos cambios) ?

8.- ¿Existen controles para que unicamente personal autorizado, le de mantenimiento a los sistemas de información que se encuentran en operación ?

8.1. ¿Si es así, cuáles son esos controles ?

9.- Existe 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
- Tareas, Fechas y Responsables del mantenimiento
- Etc.

REDES LOCALES

1. ADMINISTRACION

REDES LOCALES

OBJETIVOS DE ESTA REVISION :

- Asegurar que exista un función formal de Administración de la(s) Red(es) Local(es)

- 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 (Ver cuestionario de Seguridad para mayor detalle)

  - El Mantenimiento de las Redes Locales

  - Verificar que existan parametros de medición del desempeño de las Redes (Bitacoras, Gráficas, Estadísticas, Etc.)

- 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 inherentes a la(s) Red(es) de la empresa.

REDES LOCALES

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla a los responsables y usuarios de las Redes Locales

REDES LOCALES

1. ADMINISTRACION

1. ¿ Cuenta su empresa con Red(es) Local(es) ?

1.1. ¿ Si es así, ¿ Cuantas micros hay en dicha RED (incluyendo el servidor), mencione sus caracteristicas básicas? (mencione los perrifericos y cacterísticas básicas)

1.2. ¿ Que Software (Paquetes, Lenguajes, Sistemas de Información, Sistemas Operativos (S.O.), Bases de Datos, Etc. hay instalados ? ¡ Cuales son las versiones correspondientes?

FUNCION	TAREAS	ACCIONES DE SEGUIMIENTO
1.3. Mencione que aspectos mencionados a continuación son cubiertos en su empresa : - La evaluación de HW, SW, Etc. de la RED - Adquisición/Instalación de: HW/SW de RED - Asignación y Baja de Usuarios a l a RED - Nivel de Servicios para usuarios de la RED : - Desempeño - Capacitación - Soporte - Mantenimiento - Operación de : - Equipo - Software - Aplicaciones - Seguridad : - Datos - Procesos - Equipos - Software - Otros		

1. ADMINISTRACION

2. ¿Existe alguna participación de personal externo para el desempeño de las funciones de Administración de la RED antes mencionada ?

2.1 ¿Si es así, mencione cuales son y el porque de que lo efectue dicho personal ?

3. ¿ Existen procedimientos que aseguren la oportuna y adecuada instalacion de los diferentes componentes de la RED, conforme se hayan realizado los contratos y compras formales de los mismos ?

4.-¿Se cuenta con manuales de operación de la red ? ¿Contemplan aspectos de Seguridad?

5.- ¿Se tiene identificada formalmente la siguiente Informacion :

- Usuarios de la Red
- Logins y niveles de Acceso
- Terminales conectadas a la Red
- Responsables de la Red
- Capacidad de Discos/Espacio Libre x Servidor y micros
- Etc. ?

5.1. ¿Estos registros son generados por algún software de RED o los generan de manera independiente los responsables de la administración de misma ?

6.- ¿Existe un procedimiento formal para dar un servicio oportuno y eficiente a los requerimientos de los usuarios de la Red ?

6.1.- ¿Lo conocen los usuarios de la Red ?

7. ¿Se tienen procedimientos de Respaldo (Equipo / Datos Software Etc.) ?

7.1. ¿ Se conocen por todos los usuarios y responsables de la Red?

8.- ¿Se tiene un seguro que proteja el software y equipo de la Red ?

SOFTWARE

1. ADMINISTRACION

2. LEGALIZACION

SOFTWARE

OBJETIVOS DE ESTA REVISION :

- Asegurar que exista un función formal de Administración del SOFTWARE

- Asegurar la existencia de Procedimientos y Controles que orienten a la satisfacción de :
  - La Administración del SOFTWARE
  - La Instalación del SOFTWARE
  - La Operación y Seguridad del SOFTWARE (Ver cuestionario de Seguridad para mayor detalle)
  - El Actualización del SOFTWARE

- Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio el SOFTWARE existente.

- Determinar si existen los suficientes controles y procedimientos de Seguridad inherentes al SOFTWARE de la empresa.

- Asegurar que solo Software Legalizado se encuentre instalado en todas las microcomputadoras y/o Redes Locales de la organización

SOFTWARE

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla al responsable y/o usuarios del Software

SOFTWARE

1. ADMINISTRACION

1. ¿ Cuenta su empresa con microcomputadoras, minicomputadoras o mainframes ?

1.1. ¿ Existe un documento que muestre la distribución del equipo y sus usuarios?

1.2. ¿ Que Software (Paquetes, Lenguajes, Sistemas de Información, Sistemas Operativos (S.O.), Bases de Datos, Etc. hay instalados ? ¿ Cuales son las versiones correspondientes?.

2. ¿Se llevó a cabo en su empresa un Estudio de Justificación de Instalación / Actualización/Reemplazo de Software que contemplará al menos lo siguiente :

- SW Requerido :
  - Aspectos Legales - Paquetes de Computo
  - Lenguajes de Programación -S.O. -Etc.
  - HW Requerido :
    - Micros - Perifericos, Etc.
  - Evaluación Costo/Beneficio
  - Procedimientos de :
  - Capacitación - Seguridad - Operación
  - Actualización - Monitoreo - Etc.

3. ¿ Que procedimientos de Seguridad existen para el manejo adecuado del software instalado en la empresa '

3. ¿ Cuales son dichos procedimientos ?

3.2. ¿ Quienes son los responsables de ejecutar dichos procedimientos ?

3.3. ¿ Cómo se da seguimiento formal al cumplimiento de dichos procedimientos ?

3.4. ¿ Cómo se ejecuta dicho procedimiento?

4. ¿Existe alguna participación de personal externo para el desempeño de las funciones de Administración del Software antes mencionada ?

4.1 ¿Si es así, mencione cuales son y el porque de que lo efectue dicho personal ?

5. ¿Existe la documentación formal que especifique el que hacer y como llevar a cabo cada una de las funciones de Administración del Software ?

SOFTWARE
2. LEGALIZACION

Aspectos Claves a Evaluar :

1. ¿ Existen procedimientos que aseguren la oportuna y adecuada evaluación / legalización / instalación y actualización del Software , conforme se hayan realizado los contratos y compras formales del mismo ?

PROCEDIMIENTOS	**RESPONSABLES DE EJECUTARLOS**	**RESPONSABLES DE SEGUIMIENTO**

2. ¿ Las compras del Software , así como su instalación se derivan de un proceso de planeación y evaluación formal ? ¿ Como se aseguran de que esto sea cumplido siempre?

3. ¿ En caso de que las compras e instalación del Software no hayan sido planeadas formalmente como se justifican ante los responsables de Informática y de las Areas usuarias involucradas en el uso del mismo ?

4. ¿Se tiene un plan de evaluación y compra de Software por semestre / año?

5. Respecto a la Instalación de Software ¿ Como se aseguran que éste haya sido comprado legalmente ? ¿ Como se aseguran que dicho Software no sea instalado en otros equipos de la empresa que no tienen licencia de uso ? ¿ Que hacen cuando detectan algunas anomalias al respecto?

6. ¿ Se conoce cual es el inventario actual de Software instalado en su empresa ?

7. ¿ Se conoce cual de ese Software instalado es legal ?

8. ¿ Que se piensa hacer respecto al Software que no es legal ?

9. ¿ Existen Políticas que aseguren que se compre solo Software estandar y que no se violen los acuerdos de legalización de la empresa ?

10. ¿ Cuales son ?

10.1 ¿ Quien les da seguimiento ?

10.2. ¿ Cómo se les da seguimiento ?

SEGURIDAD

HARDWARE

SOFTWARE / APLICACIONES

PLAN DE CONTINGENCIAS Y DE RECUPERACION

OBJETIVOS DE ESTA REVISION :

- Verificar que existan los planes, políticas y procedimientos relativos a la seguridad dentro de la Organización.

-Verificar que exista un Analisis Costo / Beneficio de los controles y procedimientos de Seguridad antes de ser implantados.

-Verificar que los planes y políticas de Seguridad y de Recuperación sean difundidos y conocidos por la Alta Dirección.

- Evaluar el grado de compromiso que existe por parte de la Alta Dirección, de los Departamentos Usuarios y del personal de Informática hacia el cumplimiento satisfactorio de los planes, políticas y procedimientos relativos a la Seguridad

- Asegurar la disponibilidad y continuidad del equipo de computo, por el tiempo que requiera los usuarios para el procesamiento oportuno de sus aplicaciones.

- Asegurar que las políticas y procedimientos brinden confidenciabilidad a la información que es manejada en el medio ambiente de desarrollo, implantación, operación y mantenimiento.

- Verificar que exista la Seguridad requerida para el aseguramineto de la Integridad de la Información que es procesada, en los aspectos de totalidad y exactitud.

- Asegurar que se brinde la seguridad necesaria a los diferentes equipos de computo que existen en la organización.

- Verificar que exista una función responsable de la Administración de la Seguridad para :

- Recursos Humanos relacionados con la Tecnología de Informática

- Recursos Materiales relacionados con la Tecnología de Informática

- Recursos Financieros relacionados con la Tecnología de Informática

- Recursos Tecnológicos de Informática

SEGURIDAD

Actividades Principales para Auditar esta Area :

1.- Verificar proyectos contra la Planeación de Auditoría.
2.- Concertar Citas con Personal a entrevistar.
3.- Revisar formulario correspondiente y ver conveniencia de actualizarlo a necesidades especifícas del negocio.
4.- Ratificar y formalizar fechas de entrevistas y de visitas.
5.- Efectuar las entrevistas y visitas que sean necesarias para cubrir los puntos correspondientes a este módulo.
6.- Elaborar borrador con 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 borrador con el responsable del proyecto por parte de las Areas evaluadas.
10.- Elaborar y documentar formalmente conclusiones y recomendaciones finales de esta revisión.
11.- Anexar esta información al documento que definirá el Informe Final.

Requerimientos para el exito de la revisón :

1.- Formalizar el apoyo de la Alta Dirección al Auditor de Informática con el fin de brindarle las facilidades necesarias, para la ejecución satisfactoria de sus actividades; Algunas acciones de apoyo serian :

2. Conocimiento por parte del Auditor de Informática del Area a evaluar

3. Uso de Técnicas y Herramientas de Productividad apropiadas para la revisión

4. Aplicarla a los Responsables de Seguridad, así como a los usuarios de Informática

SEGURIDAD
1. HARDWARE

Aspectos a Evaluar

1.- ¿Existen políticas y procedimientos relativos al uso y protección del Hardware existente en la Organización ?

2.- ¿Si existen, Están formalmente identificados los siguientes aspectos de seguridad :

- Administración del Hardware :

Micros, Minis y Macrocomputadoras (Mainframes)
Tecnología de Comunicaciones, Redes, Etc.

- Cuantificación del Hardware
- Descripción del Hardware (Características básicas)
- Distribución del Hardware (Ubicación Física)
- Registro de: Hardware instalado, dado de baja, en proceso de adquisición, etc.)
- Uso del Hardware :
- Funciones responsables del control del Hardware
- Etc.

- Procedimientos y Controles de seguridad para :

- La Evaluación, Selección y Adquisición de Hardware :

A) Existen políticas que verifiquen que el software que sea adquirido cubra los siguientes puntos :

- Módulos de seguridad para :
  - Acceso al Hardware (Llaves de seguridad, por ejemplo)
  - Uso del Hardware (Facilidades de monitorear la operación)
  - Bitacoras de uso del Hardware :
    - Quien ? , Cuándo ?, Para que ?, etc.
  - Etc. ?

C) Existen políticas que verifiquen que el Hardware que sea reemplazado y/o actualizado cubra los siguientes puntos :

- Autorización del Hardware por medio de :

- Justificación del reemplazo del Hardware
- Impacto de la implantación del Hardware en el medio ambiente de Informática
- Implicaciones de control en la Implantación y uso del Hardware nuevo.
- Etc. ?

2.- ¿En cuanto al equipo de Soporte se tienen al menos los siguientes datos :

. Localización Física, Control y Mantenimiento de :

- Aire Acondicionado
- Equipo No-Break
- Equipos contra Incendios
- Otros

4.- ¿La ubicación fisica del Equipo de Computo dentro del edificio es la más adecuada contra los diversos desastres o contingencias que se pueden presentar :

- Manifestaciones (Huelgas, por ejemplo) - Inundaciones - Incendios
- Robos - Temblores - Etc.

Nota : Verificar si el edificio presenta facilidades de escape en casos de emergencia

5.- ¿Existen procedimientos que garantizen la continuidad y disponibilidad del equipo de computo en caso de desastres o contingencias ?

6.- Si es así, ¿estan documentadas y difundidas formalmente ? (Verificar la existencia de esos documentos y la difusión de los mismos en la Organización)

7.- ¿Se cuenta con controles y procedimientos para :

- Clasificación y justificación del personal que tiene acceso a los centros de computo del negocio y a las oficinas donde se encuentra papeleria y/o accesorios relacionados a Informática
- Restringir el acceso a los centros de computo solo a personal autorizado
- Definición y difusión de las horas de acceso que son permitidas al centro de computo
- Uso y control de bitacoras de acceso a centros de computo
- Definir la aceptación de entrada a visitantes
- Manejo de bitacoras especiales para visitantes a los centros de computo ?

Nota : Verificar el cumplimiento de estos controles y procedimientos.

8.- ¿Existe personal de Seguridad encargado de manera específica a la salvaguarda de los equipos de computo del negocio?

9.- ¿Existen políticas relacionadas al ingreso y salida de Hardware dentro de la organización, que aseguren al menos lo siguiente :

SEGURIDAD
2. SOFTWARE / APLICACIONES

Aspectos Claves a Evaluar

1.- ¿Existen políticas y procedimientos relativos al uso y protección del Software existente en la Organización ?

2.- ¿Si existen, Están formalmente identificados los siguientes aspectos de seguridad :

- Administración del Software :

Sistemas Operativos, Utilerias, Paquetes, etc.

- Cuantificación del Software (Original y copias)
- Descripción del software (Por original)
- Distribución del Software (En que equipos y/o dispositivos de almacenamiento secundarios se encuentra, mencionar un lugar físico donde se localizan: Areas del negocio, Bancos, etc.)
- Registro de: Software instalado, dado de baja, en proceso de adquisición, etc.)
- Uso del Software (Tipo de uso, responsables de su uso, Etc.)
- Etc. ?

- Procedimientos y Controles de seguridad para :

- La Evaluación, Selección y Adquisición de Software :

A) ¿Existen políticas que verifiquen que el software que sea adquirido cubra los siguientes puntos :

- Acceso al Software
- Uso del Software
- Bitacoras de uso del Software :
- Quien ? , Cuándo ?, Qué ?, etc.
- Etc. ?

B) ¿Existen políticas que verifiquen que el software que sea reemplazado cubra los siguientes puntos :

- Autorización del Software por medio de :
- Justificación del reemplazo del Software
- Impacto de la implantación del Software en el medio ambiente de Informática :
- Implicaciones de control en la Implantación y uso del software nuevo.
- Etc. ?

3.- ¿Existen políticas relacionadas al ingreso y salida de software dentro de la organización? ¿ Cuáles son ?

- Que el software que ingrese a la empresa sea :

- Revisado (Contenido, cantidad, destino)
- Aprobado por el responsable de Informática
- Registrado
- Devuelto (Verificar contra fecha estimada de devolución)
- El personal este comprometido formalmente a no hacer un mal uso del mismo (Copia, Daños, etc.)
- Etc. ?

4. En cuanto a las aplicaciones (Sistemas de Información) que se desarrollan en la empresa los controles y procedimientos necesarios para garantizar la seguridad mínima que requieren los sistemas a ser desarrollados ?

4.1. - En caso de que existan, contemplan dichos controles al menos lo siguiente :

- Procedimientos de llenado de documentos fuente
- Procedimientos de uso del computador :
  - Encedido y arranque del equipo
  - Restauración del equipo en caso de fallas
  - Manejo de bitacoras de uso del computador
  - Monitoreo de uso del computador
  - Etc.
- Niveles de acceso (perfil de Usuarios) a los módulos de :
  - Captura
  - Actualización
  - Consulta
  - Generación de Reportes
  - Respaldos
  - Etc.
- Procedimientos de uso de los módulos de :
  - Captura
  - Actualización
  - Consulta
  - Generación de Reportes
  - Respaldos
  - Etc.

- Etc.

SEGURIDAD
3. PLAN DE CONTINGENCIAS Y DE RECUPERACION

Aspectos Claves a Evaluar

1. ¿ Considera usted que tanto la Alta Dirección, Usuarios y Personal de Informática están concientes que todos los recursos involucrados con la informática son activos del negocio y deben protegerse de una manera formal y permanente ? ¿ Porque?

1.1. ¿ Cuales de los siguientes Recursos relacionados con Informática considera usted que son más críticos para la organización y cuales crea que contemplan más y mejores métodos de protección para que puedan seguir operando/trabajando/apoyando a los objetivos del negocio en condiciones optimas :

RECURSOS	**Grado de Importancia(A) (C / I / N / M / NS)**	**Métodos Formales para su Protección (-)**
HUMANOS		
MATERIALES		
FINANCIEROS		
TECNOLOGICOS		
DE INFORMACION		

(A) C = CRITICO I = IMPORTANTE N = NECESARIO
M = MINIMO NS = NO SABE

(-) Verificar que los recursos que ellos consideran criticos, importantes o necesarios tengan los métodos de seguridad necesarios para prevenir y enfrentar contingencias, en caso de que no existan se podrá observar que dichas consideraciones son más teoricas que prácticas.

Para aquellos recursos que ellos consideren de importancia mínima o que la desconozcan tendremos que preguntar el porque de tales afirmaciones.

1.2.- ¿Existen planes de contingencias y de recuperación de operaciones para casos de contingencias o desastres ?

1.3. ¿ Contemplan dichos Planes de Contingencia y de Recuperación al menos los siguientes aspectos :

- Red de Comunicaciones (RC)
- Hardware
- Software / Aplicaciones / Datos
- Recursos Humanos
- Lugares Físicos donde se localizan los recursos anteriores
- Otros

SEGURIDAD
3. PLAN DE CONTINGENCIAS Y DE RECUPERACION

2.- Si es así, fuerón difundidos formalmente en toda la organización ?

2.1. ¿ Fuerón elaborados por terceros, personal de Informática, por los usuarios o fué un proyecto donde se involucrarón varias áreas del negocio ?

2.2. ¿ En el proceso de Planeación de Contingencias y Recuperación y de su Implementación de su empresa, cuales fuerón las Tareas realizadas, cuales están pendientes, cuales en desarrollo y quienes son sus responsables :

TAREA	STATUS (D / T / NI) (-)	PRODUCTOS TERMINADOS
1.DEFINICION DE METAS Y OBJETIVOS DEL PLAN		
2. EVALUACION E IDENTIFICACION DE RIESGOS		
3. ELABORACION DE ACCIONES. POLITICAS Y PROCEDIMIENTOS POR TIPO DE RIESGO		
4. DOCUMENTACION DEL PLAN		
5. APROBACION DEL PLAN DIFUSION DEL PLAN		
6. SIMULACION DEL PLAN		
7. ACTUALIZACION DEL PLAN		

(-) D = TAREA EN DESARROLLO
T = TAREA TERMMINADA
N/I = TAREA NO INICIADA

2.3. ¿ Se han presentado contingencias que hayan sido enfrentadas con el Plan de Contingencias y de recuperación diseñado para su empresa ? ¿ Cuales fuerón los resultados ?

2.4. ¿ Si no existe un Plan de Contingencias y de Recuperación que acciones han tomado para enfrentar dichas eventualidades y quienes han sido los responsable de ejecutar estas acciones ?

9. Etapa de Formalización :

9.1. Verificación de Prioridades, Restricciones y Alcances del Proyecto

9.2 Actualización del Plan de Auditoría de Informática

9.3. Presentación Formal del Plan de Auditoría de Informática

9.4. Aprobación Formal del Proyecto de Auditoría de Informática

9. Etapa de Formalización :

Las Etapas anteriores fuerón de introdución e investigación a la empresa y sus diversas funciones de negocio, sus debilidades y fortalezas más relevantes fuerón detectadas, la planeación y proyección de las áreas que requieren ser auditadas ya se han definido, así como las adecuaciones y/o agregados requeridos ya fuerón documentados, **ahora en la presente Etapa de Formalización (Figura 9-1) corresponde a la Alta Dirección, dar su aprobación y apoyo formal para el desarrollo del Proyecto de Auditoría de Informática presentado por el Lider de Proyecto y del Responsable de la Función de Auditoría de Informática.**

Etapa de Adecuación
(Terminada)

Etapa de Formalización
(En ejecusión)

Etapa de Desarrollo
(Posterior)

La participación real de la Alta Dirección es crítica, lo mismo que la del Responsable de la Función de Informática en el negocio. Los usuarios claves deben tambien estar presentas durante el proceso de Formalización del Proyecto.

9.1. 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 de Informática, ya que mediante su realización se clarifica el rumbo, límites y cobertura que tendrá el proyecto.

Aquí las actividades requeridas para efectuar 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 de las reuniones o entrevistas que se efectuen, el Auditor de Informática (o el Lider de Proyecto) documenten lo ahí expuesto mediante una minuta o resumén (Tablas, gráficas, narrativa, etc) donde se mencionen los puntos tratados y las conclusiones a que se llegó, lo anterior se soporta más formalmente si aparecen las firmas de conformidad de cada uno de los involucrados.

EL PROCESO METODOLOGICO DE LA AUDITORIA DE INFORMATICA : UN ENFOQUE PRACTICO				
Etapa	**Productos Terminados**	**Requerimientos**	**Responsables**	**Involucrados**
FORMALIZACION	**1. VERIFICAR PRIORIDADES, RESTRICCIONES, ETC.**	1.1.PRIORIDADES CLASIFICADAS	L.P.	R.A.I.
		1.2. AREAS A AUDITAR VERIFICADAS	A.I. / L.P.	R.A.I.
	2. ACTUALIZACION DEL PLAN DE AUDITORIA DE INFORMATICA	2.1. PLAN ACTUALIZADO		
		2.2. PLAN DOCUMENTADO	R.A.I.	A.D. / P.U. / R.I. / L.P.
	3. PRESENTACION DEL PROYECTO DE AUDITORIA DE INFORMATICA	3.1. ENTENDIMIENTO DEL PROYECTO	R.I.	L.P. / A.I.
		3.2. ACEPTACION DEL PROYECTO	P.I. / P.U.	L.P. / A.I.
		3.3. COMPROMISO DE CADA UNA DE LAS AREAS INVOLUCRADAS	P.I. / P.U.	L.P. / A.I.
	4. APROBACION FORMAL DEL PROYECTO	4.1. INFORME APROBADO	L.P.	P.I. / P.U.
		DE MANERA FORMAL	L.P.	P.I. / P.U.
		4.2. COMPROMISO EJECUTIVO	L.P.	P.I. / P.U.

NOMENCLATURA : A.D. = ALTA DIRECCION P.U. = PERSONAL USUARIO R.I. = RESPONSABLE DEL AREA DE INFORMATICA
P.I. = PERSONAL DE INFORMATICA R.A.I. = RESPONSABLE DEL AREA DE AUDITORIA DE INFORMATICA
L.P. = LIDER DEL PROYECTO DE AUDITORIA DE INFORMATICA A.I. = AUDITOR DE INFORMATICA

Figura 9-1

9.2 Actualización del Plan de Auditoría de Informática

Se ha hablado ya de como efectuar la tarea de actualización de un Plan, **lo importante en este momento es asegurarnos de que los pocos (pero significativos) cambios que se hayan efectuado despues de realizar la Tarea anterior, sean reflejados en el Plan Detallado de Auditoría de Informática** que será presentado a la Alta Dirección para su aprobación final y formal.

9.3. Presentación Formal del Plan de Auditoría de Informática

La presente tarea es la más crítica para el Lider del Proyecto y para el Responsable de Auditoría de Informática, ya que justificará en ésta, la continuación del proyecto.

Las actividades más relevantes y necesarias del responsable de esta tarea son :

+ Asegurarse de contar con toda la información en un formato de presentación sumarizada y entendible, ya que su principal audiencia será la Alta Dirección, los Usuarios Claves y el Responsable de Informática.
+ Revisarla y verificarla con el Responsable de Auditoría de Informática
+ Concertar la cita en una fecha y lugar apropiados
+ Otras que se consideren oportunas para el éxito de la tarea

9.4. Aprobación Formal del Proyecto de Auditoría de Informática

Se puede decir que es la Tarea que lleva menos tiempo y que sin embargo es una de las **más importantes, ya que de ella surge la aprobación formal del proyecto.** Aqui el proyecto pasa a ser un proyecto autorizado para su desarrollo y terminación según el Plan de Auditoría de Informática.

Consideraciones claves que aseguran la terminación satisfactoria de esta tarea :

+ Presentar un resumen de la Matriz de Riesgos, Areas de Oportunidad, Plan detallado de Auditoría de 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 a revisión, etc.)
+ Se aprueba formalmente el proyecto (Firma de conformidad de los involucrados)
+ Se autoriza las fechas de incio del proyecto
+ Otras que el Auditor de Informática considere pertinentes en su negocio

Nota : No todo lo planeado y justificado es siempre autorizado por la Alta Dirección, 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 la aprobación formal del proyecto, sin embargo el Lider de Proyecto debe lograr el visto bueno de todos a traves de buen soporte.

10. ETAPA DE DESARROLLO :

10.1. Concertar fechas de entrevistas, visitas y aplicación de cuestionarios

10.2. Clasificar técnicas, herramientas, cuestionarios, entrevistas, etc.

10.3 Aplicación de Entrevistas y Cuestionarios

10.5 Efectuar visitas de verificación

10.6 Elaborar informe preliminar por :

+ Area auditada

10.7 Revisión del Informe Preliminar

10.8 Elaborar el Informe Final de Auditoría de Informática :

10.9 Presentación a la Alta Dirección e involucrados claves

10. ETAPA DE DESARROLLO :

La Etapa de Desarrollo (Figura 10-1) es la más importante para el Auditor de Informática, ya que es aquí donde se ejerce su función de manera práctica, empieza a ejecutar las tareas de su trabajo de acuerdo al Plan aprobado en la Etapa de Formalización.

Etapa de Formalización
(Terminada)

Etapa de Desarrollo
(En ejecusión)

Las actividades más importantes del Auditor en Informática en la Etapa de Desarrollo son al menos las siguientes :

+ Ejecutar las tareas de acuerdo a la secuencia establecida en el Plan detallado de Auditoría de Informática

+ Respetar el Proceso Metodológico (Capitulo Cinco)

+ Coordinar los Recursos Humanos ficientemente para el cumplimiento oportuno del proyecto

+ Impulsar el apoyo permanente de la Alta Dirección

+ Motivar a todos los involucrados del Proyecto

+ Orientar a los recursos humanos, tecnológicos y financieros a resultados que brinden soluciones fáctibles y de valor agregado

+ Otros considerados por el Lider del Proyecto de acuerdo a las caractrísticas de su negocio y de la Función de Informática

Nota : Cada una de las tareas de la Etapa de Desarrollo será explicada de una manera uniforme para hacerla más práctica y entendible, se mencionarán las actividades más importantes que llevará a cabo el Auditor de Informática y los Productos Terminados mínimos que debe obtener al finalizar cada una de ellas. (VER FIGURAS 10.2, 10.3, 10.4)

EL PROCESO METODOLOGICO DE LA AUDITORIA DE INFORMATICA : UN ENFOQUE PRACTICO				
Etapa	**Productos Terminados**	**Requerimientos**	**Responsables**	**Involucrados**
DESARROLLO	**1. CONCERTAR CITAS DE VISITAS Y ENTREVISTAS**	1.1. FECHAS APROBADAS Y/O ACTUALIZADAS	A.I.	P.I. / P.U.
	2. CLASIFICAR TECNICAS, CUESTIONARIOS Y LAS HERRAMIENTAS A USAR	2.1. TECNICAS CLASIFICADAS	A.I.	L.P.
		2.2. CUESTIONARIOS CLASIFICADOS	A.I.	L.P.
		2.3. HERRAMIENTAS CLASIFICADAS	A.I.	L.P.
	3. EFECTUAR ENTREVISTAS, VISITAS Y APLICAR LOS CUESTIONARIOS	3,1. ENTREVISTAS REALIZADAS	A.I.	P.I. / P.U.
		3.2. VISITAS REALIZADAS	A.I.	A.I.
		3.3. CUESTIONARIOS APLICADOS	L.P. / A.I.	R.A.I.
	4. ELABORAR Y REVISAR INFORME PRELIMINAR	4.1 OBSERVACIONES DETECTADAS	A.I.	L.P.
		4.2. RECOMENDACIONES / ACCIONES	A.I.	L.P.
		4.3. INFORME REVISADO	A.I.	A.I.
	5. ELABORAR EL INFORME FINAL DEL PROYECTO	5,1 OBSERVACIONES DETECTADAS	A.I.	L.P.
		5,2. RECOMENDACIONES / ACCIONES	A.I.	L.P.
		5,3. DETALLAR SOLUCIONES	A.I.	A.I.
		5.4. CLASIFICAR SOLUCIONES	A.I.	L.P.
	6.PRESENTAR EL INFORME FINAL	6.1. PRESENTAR Y APROBAR INFORME DE AUDITORIA DE INFORMATICA	A.D. / R.I. /P.U.	R.A.I. / L.P.
		6.3. ESTABLECER FECHAS PARA EJECUTAR ACCIONES / SEGUIMIENTO		

NOMENCLATURA : A.D. = ALTA DIRECCION P.U. = PERSONAL USUARIO R.I. = RESPONSABLE DEL AREA DE INFORMATICA
P.I. = PERSONAL DE INFORMATICA R.A.I. = RESPONSABLE DEL AREA DE AUDITORIA DE INFORMATICA
L.P. = LIDER DEL PROYECTO DE AUDITORIA DE INFORMATICA A.I. = AUDITOR DE INFORMATICA

Figura 10-1

TAREA	ACTIVIDADES PRINCIPALES	PRODUCTOS TERMINADOS
Concertar fechas de entrevistas, visitas y de Aplicación de Cuestionarios	+ Solicitar una lista con todos los nombres, puestos y departamentos del Personal de Informática y de las áreas usuarias involucrados en el proyecto + concertar citas	+ Lista del Personal de Informática y de usuarios + Fecha y hora formal de cada entrevista
Clasificar Técnicas, Herramientas, cuestionarios, entrevistas, etc.	+ Verificar la lista de Métodos, Técnicas y Herramientas requeridas + Verificar cuestionarios requeridos + Clasificar y documentar de acuerdo al Proyecto.	+ Lista de Métodos, Técnicas y Herramientas clasificadas por área de Revisión + Cuestionarios de cada área, actualizados y documentados
Aplicación de Entrevistas y cuestionarios	+ Efectuar Entrevistas y Cuestionarios + Elaborar Observaciones y Recomendaciones	+ Entrevistas y cuestionarios aplicados y documentados + Observaciones y Recomendaciones iniciales
Efectuar visitas de verificación	+ Realizar cada entrevista programada + Documentar debilidades de control y seguridad detectadas en cada visita	+ Visitas de revisión y verificación efectuadas + Observaciones y Recomendaciones iniciales

(Figura 10-2)

TAREA	ACTIVIDADES PRINCIPALES	PRODUCTOS TERMINADOS
Elaborar Informe Preliminar	+ Analizar la Información documentada en tareas anteriores + Elaborar observaciones y conclusiones de cada área auditada. + Documentar Observaciones y Recomendaciones de Auditoría de Informática **(Ver Figura 10-5)**	+ Hojas de Resumen de Observaciones y Recomendaciones de Auditoría **(Ver Figura 10-5)** + Observaciones, conclusiones y Recomendaciones por : *** Area**
Revisión del Informe Preliminar	+ Verificar cada una de las observaciones y recomendaciones por Area con el Lider del Proyecto + Asegurarse que se tenga en documento todo el soporte requerido para cada observacion + 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 recomendacioes verificadas y depurada + Reunión informal de notificación de avance del proyecto con el responsable de Informática y con el Responsable de los usuarios + Compromiso de terminación de pendientes por medio de entrevistas y/o visitas y/o aplicación de cuestionarios
Elaborar el Informe Final de Auditoría de Informática	+ Elaborar el Informe Final + Verificar que el Informe contenga al menos : * Antecedentes * Observaciones, Conclusiones, Recomendaciones, Responsables y Tiempos por Area Auditada	**+ Informe para la Alta Dirección** **+ Informe detallado para:** *** Responsable de Informática** *** Usuarios Claves**

(Figura 10-3)

TAREA	ACTIVIDADES PRINCIPALES	PRODUCTOS TERMINADOS
Presentación a la Alta Dirección e Involucrados Claves	+ Verificar que los Informes sean claros, completos y congruente entre sí + Verificar que se tenga el soporte de lo mencionado en los informes + Formalizar fecha de la presentación de informes + Presentar los Informes de Alta Dirección y detallado + Elaborar una minuta + Obtener la aprobación formal (documento) de la Terminación del Proyecto de Auditoría de Informática. + Delegar en Informática y las áreas usuarias la implantación de las acciones recomendadas	+ Informes verificados + Informes finales + Informes presentados a la Alta Dirección y a los Involucrados claves del Proyecto (Responsable de Informática y el Responsable de los Usuarios al menos) + Minuta de la Reunión + Aprobación formal de la Alta Dirección de la terminación del proyecto de Auditoría de Informática + Compromiso del Respónsable de Informática y de las Areas usuarias para ejecutar la Etapa de Implantación.

(Figura 10-4)

FIGURA 10-5

RESUMEN DE OBSERVACIONES Y RECOMENDACIONES DE AUDITORIA DE INFORMATICA

EMPRESA / DEPARTAMENTO:

AREA DE REVISION :

COMPONENTES DEL AREA DE REVISION ;

TECNICAS DE AUDITORIA UTILIZADAS EN ESTE PROCESO:

PERSONA ENTREVISTADA:

PUESTO :

FECHA DE LA AUDITORIA :

AUDITOR :

COMENTARIOS :

OBSERVACION	RECOMENDACION	SOLUCION				FUNCION RESPONSABLE LA SOLUCION
		AI	CP	MP	LP	

AI = ACCION INMEDIATA
CP = CORTO PLAZO
MP = MEDIANO PLAZO
LP = LARGO PLAZO

FUENTES DE INFORMACION PARA UNA ACTUALIZACION PERMANENTE DE LA FUNCION DE AUDITORIA DE INFORMATICA.

11. FUENTES DE INFORMACION PARA UNA ACTUALIZACION PERMANENTE DE LA FUNCION DE AUDITORIA DE INFORMATICA

Algunas acciones que nos garantizan la eficiencia en el desarrollo permanente de la Auditoría de Informática son entre otras :

- Apoyo de la Alta Dirección
- Planeación formal de la Auditoría de Informática
- Involucración de los Usuarios y del Personal de Informática
- Apoyo en los proyectos por Asesores externos cuando así se requiera
- Actualización del Proceso Metodológico de Auditoría de Informática
- Actualización del Auditor de Informática en los campos de Auditoría e Informática
- Otros

La actualización del Auditor en los aspectos metodologicos, técnicos y de manejo de herramientas de productividad se puede lograr llevando al menos las siguientes acciones :

- Capacitación por medio de :

- Seminarios o Cursos de :

- Auditoría de Informática
- Auditoría
- Informática
- Areas especializadas de Negocio (Finanzas, manufactura, etc.)

- Suscripciones a revistas especializadas de Auditoría de Informática

- Suscripciones a revistas especializadas de Informática y/o Auditoría

- Participación permanente y formal en :

- Asociaciones Profesionales Nacionales o Internacionales de :

- Auditoría de Informática
- Auditoría
- Informática

- Otros medios que se consideren convenientes

Dicha actualización tiene como objetivo primordial el garantizar que el proceso formal de Auditoría de Informática cumpla con los requerimientos de Seguridad y Control apropiados para el negocio, así como con los estandares sugeridos por las Asociaciones Profesionales a nivel nacional e internacional.

LIBRO / FUENTE	AUTOR	EDITORIAL	AÑO	PAIS
Auditoria I	Expositores de la Asociacion Mexicana de Auditores de Informática	Asociacion Mexicana de Auditores de Informática	1990 1993	México
Auditoria I I	Expositores de la Asociación Mexicana de Auditores de Informática	Asociacion Mexicana de Auditores de Informática	1990 1991 1992	México
Auditoría en Informática	José Antonio Echenique	Mc Graw Hill	1991	México
Control Objetives	The EDP Auditors Foundation, Inc.	The EDP Auditors Foundation, Inc.	1991	Estados Unidos
EDP Auditing and Controls	MIS Training Institute	MIS Training Institute	1993	Estados Unidos
INFOAMAI (BOLETINES) / The EDP Auditors Journal	Asociación Mexicana de Auditores en Informática / The EDP Auditors Foundation, INC.	Asociación Mexicana de Auditores en Informática / The EDP Auditors Foundation, INC.	1988-1993	México / Estados Unidos
INTEREX HP Computer Users Conference	INTEREX The International Association of Hewlett Packard Computers Users	INTEREX	1992	Estados Unidos
Normas y procedimientos	Instituto Mexicano de Contadores Públicos	IMCP	1992 1993	México