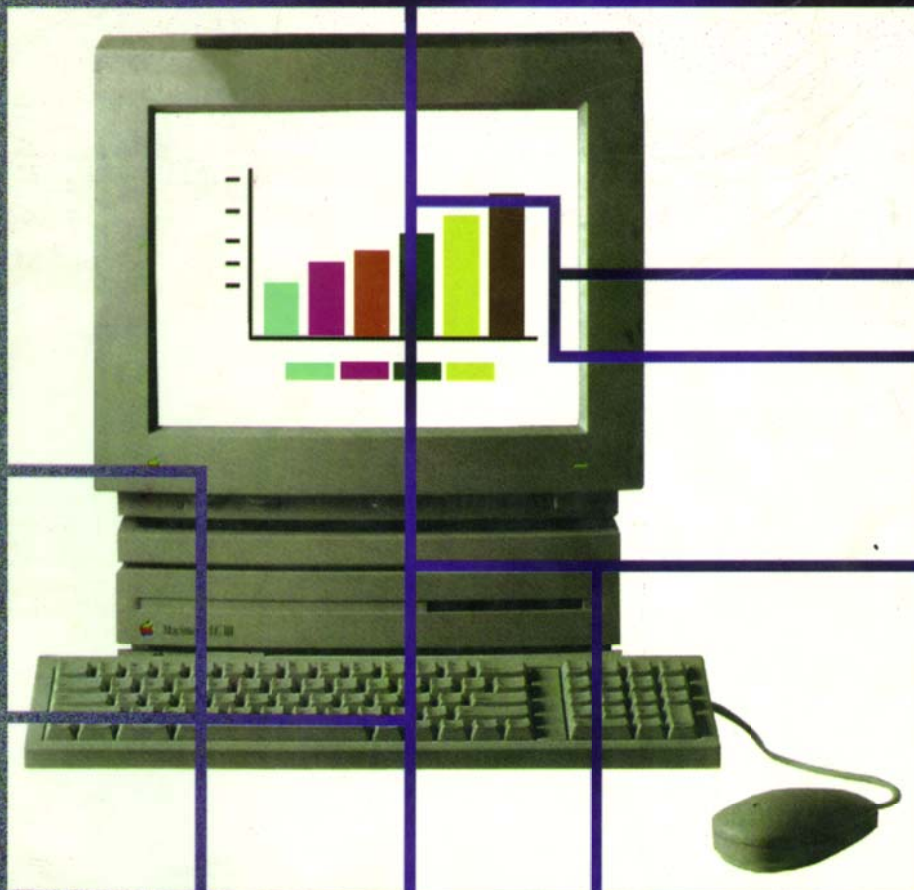


Auditoría en INFORMÁTICA



**UN ENFOQUE
METODOLÓGICO**

ENRIQUE HERNÁNDEZ HERNÁNDEZ

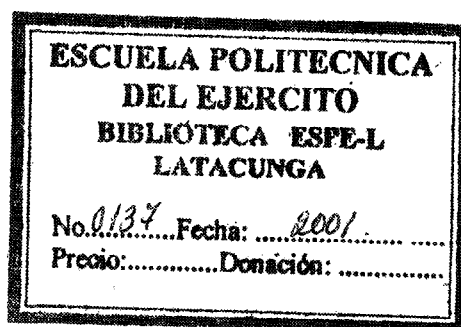
CECSA

Auditoría en informática

Un enfoque metodológico y práctico

PRIMERA EDICIÓN

Lic. Enrique Hernández Hernández



PRIMERA REIMPRESIÓN
MÉXICO, 1996

COMPAÑÍA EDITORIAL CONTINENTAL, S. A. DE C. V.
MÉXICO

Revisión técnica:

Lic. Moisés Cielak Eichenbaum

Director editorial ZIFF-DAVIS

Auditoría en informática

Derechos reservados para la primera edición

© 1995, COMPAÑÍA EDITORIAL CONTINENTAL, S.A. de C.V.

Renacimiento 180, Colonia San Juan Tlihuaca,

Delegación Azcapotzalco, Código Postal 02400, México, D.F.

Miembro de la Cámara Nacional de la Industria Editorial.

Registro núm. 43

ISBN 968-26-1283-7

Queda prohibida la reproducción o transmisión total o parcial del contenido de la presente obra en cualesquiera formas, sean electrónicas o mecánicas, sin el consentimiento previo y por escrito del editor.

Impreso en México

Printed in Mexico

Primera edición: 1995

Primera reimpresión: 1996



Dedicatorias

A mi esposa Vicky, por su apoyo y comprensión

*A mis hijos Enrique, Carlos Antonio, Erick Iván y Luis Alberto
por su brillante ejemplo*

A mis padres y hermanos por su ayuda incondicional

*A mis maestros y alumnos por la orientación y motivación que
me brindan*

*A mis amigos y compañeros de trabajo por darme parte de su
tiempo*

A Dios por darme una oportunidad

esto es, nada más se pondrán en el plan tareas orientadas a dar un valor agregado al negocio e incumban directamente a la función de auditoría en informática (seguridad, calidad y control).

A manera de ejemplo se mencionan algunas áreas de oportunidad propuestas por los mismos entrevistados en la etapa preliminar y que pueden ser apoyadas activa y formalmente por auditoría en informática:

- Elaboración, formalización y difusión de políticas y procedimientos de informática (funciones, servicios, metodologías, técnicas, herramientas de productividad, entre otras)
- Elaboración o adquisición de un plan de contingencias para informática
- Evaluación del hardware (por ejemplo: compatibilidad, tipo de uso y aprovechamiento)
- Evaluación de software (estandarización, legalización, capacitación, por citar algunas)
- Evaluación y selección de hardware y software de acuerdo con políticas del negocio
- Apoyo a informática con un enfoque de seguridad, calidad y control
- Apoyo a auditoría (financiera, operativa, etc., por ejemplo) en la implantación de los controles y procedimientos de un sistema de información que se liberará en un futuro cercano
- Apoyo a auditoría (financiera, operativa, etc.) con un enfoque de seguridad, calidad y control
- Otros

Algunos proyectos enfocados al aprovechamiento y logro de áreas de oportunidad recabadas en la etapa anterior (preliminar) requieren que los responsables directos de su planeación, desarrollo e implantación pertenezcan al personal de informática o de auditoría financiera u operativa, no al equipo del auditor en informática.

En el caso mencionado en el párrafo anterior, se debe tener cuidado de encauzar esas áreas de oportunidad a quienes correspondan y ofrecer el apoyo de auditoría en informática sólo en el caso que se necesite. Hay que cuidar muy bien las fronteras de la función de auditoría en informática y delegar las responsabilidades a quien corresponda.

Algunos proyectos que deben ser responsabilidad directa de informática son:

- Diseño, instalación y mantenimiento de una red de comunicaciones
- Investigación de tecnología (hardware, software, etcétera)
- Capacitación en el uso de metodologías de desarrollo de sistemas
- Capacitación en el uso de nueva tecnología de informática en el negocio
- Mantenimiento de hardware
- Actualización de software

- Desarrollo e implantación de sistemas
- Soporte a usuarios de informática en el negocio
- Otros

A continuación se mencionan también algunos que deben ser responsabilidad directa de auditoría (financiera, operativa, etcétera):

- Elaboración y difusión de políticas y procedimientos de control interno
- Evaluación del cumplimiento formal del control interno
- Auditoría a sistemas de información (contabilidad, inventarios, inversiones, etcétera)
- Establecimiento de controles y procedimientos operativos a sistemas de información antes de implantarse
- Otros

Una vez analizadas, evaluadas y determinadas las áreas de oportunidad (mediante el cuestionario de diagnóstico actual de la etapa preliminar) específicas de auditoría en informática, deben traducirse en el plan de auditoría en informática en tareas y productos terminados.

Las tareas o actividades que se reflejan en este momento se complementarán con la matriz de riesgos (que será contemplada a continuación) y forman los dos elementos más importantes para la formulación del plan general de auditoría en informática.

8.2 Matriz de riesgos/justificación por área de revisión

La siguiente tarea del auditor en informática en la presente etapa (justificación) es elaborar la matriz de riesgos, cuyo objetivo principal es detectar las áreas de mayor riesgo en relación con informática y que requieren una revisión formal y oportuna. Tareas, productos terminados, responsables e involucrados aparecen en la tabla 8.1; en la tabla 8.2 se muestra el contenido final que debe tener la matriz de riesgos.

Cabe aclarar que tanto la finalidad como el procedimiento de análisis y elaboración de la matriz de riesgos se detallaron en el capítulo 5 en el proceso de planeación de la auditoría en informática; sin embargo, se mencionarán los aspectos más relevantes a continuación:

- Es importante identificar el nivel de riesgo de cada uno de los elementos que integran la función de informática en el negocio a través del diagnóstico de la situación actual de informática.
- Las áreas que serán diagnosticadas pueden variar según el tamaño y estructura del negocio, originando en ocasiones que el auditor en informática tenga que evaluar productos y servicios de informática con un enfoque centralizado o descentralizado, según sea el caso.

Tabla 8.2 Matriz de riesgos

Empresa:		Gerencia:		Fecha de elaboración:	
Representante usuario:		Representante de informática:		Líder del proyecto:	
Áreas susceptibles de auditar	Aspectos o componentes por evaluar del área	Riesgo por componente	Clasificación del riesgo por área (Total)	Áreas por auditar según clasificación	
Administración de informática	1. Misión y objetivos	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Organización	%			
	3. Servicios	%			
	4. Parámetros de medición	%			
Dirección y niveles ejecutivos	1. Seguimiento a la función de informática por la dirección	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Comunicación e integración	%			
	3. Apoyo a toma de decisiones	%			
Usuarios de informática	1. Comunicación e integración	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Proyectos conjuntos	%			
	3. Administración de recursos de informática	%			
	4. Grado de satisfacción	%			
Control interno	1. Políticas y procedimientos	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
Ciclo de desarrollo e implantación de sistemas de información	1. Metodología	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Técnicas	%			
	3. Herramientas	%			
	4. Capacitación/actualización	%			
Sistemas de información	1. Planeación	%	%	Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Desarrollo	%			
	3. Operación	%			
	4. Soluciones de mercado	%			

(continúa)

Tabla 8.2 Matriz de riesgos (continuación)

Empresa:		Gerencia:		Fecha de elaboración:	
Representante usuario:		Representante de informática:		Líder del proyecto:	
Áreas susceptibles de auditar	Aspectos o componentes por evaluar del área	Riesgo por componente	Clasificación del riesgo por área (Total)	Áreas por auditar según clasificación	
Mantenimiento	1. Hardware	%		Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Software	%			
	3. Sistemas de información	%	%		
	4. Red de comunicaciones	%			
Redes locales	1. Administración	%		Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Instalación	%	%		
	3. Operación/seguridad	%			
Telecomunicaciones	1. Administración	%		Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Instalación	%	%		
	3. Operación/seguridad	%			
Hardware: Microcomputadoras minicomputadoras y mainframes	1. Administración	%		Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Instalación	%	%		
	3. Operación/seguridad	%			
Software: Paquetes de uso generalizado, lenguajes de programación, Sistemas operativos	1. Administración	%		Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado	
	2. Legalización	%	%		
	3. Operación/seguridad	%			
	4. Capacitación	%			

(continúa)

Tabla 8.2 Matriz de riesgos (continuación)

Fecha de elaboración:

Líder del proyecto:

Gerencia:

Representante de informática:

Áreas por auditar según clasificación

Empresa:

Representante usuario:

Riesgo por componente

Clasificación del riesgo por área (Total)

Aspectos o componentes por evaluar del área

Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado

1. Hardware
2. Software/aplicaciones
3. Plan de contingencias y de recuperación

Seguridad

Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado

1. Metodología
2. Técnicas
3. Herramientas
4. Capacitación/actualización

Planeación de informática

Secuencia sugerida para auditar cada componente y área según el nivel de riesgo estimado

1. Consideraciones generales

Investigación tecnológica: CASE, EDI, Multimedia, etcétera

%
%
%
%
%
%

Otros de interés específico para el auditor de informática

Nota: las áreas de revisión y los componentes de cada área mencionados en la tabla no son sugerencias que tratan de orientar a los auditores en informática; el orden y los aspectos mencionados no son estrictamente los que deben aplicarse, se pueden adecuar al criterio y características propias del negocio que afecten al proyecto.

- Algunos de los siguientes servicios de informática se mencionan de manera ilustrativa; no son limitativos o totalitarios para empresa alguna:
 - Administración de redes locales
 - Planeación de informática
 - Sistemas de información en operación
 - Administración de hardware y software
 - Desarrollo e implantación de sistemas de información
 - Soporte a usuarios (capacitación, asesoría, etcétera)
 - Administración de telecomunicaciones
 - Investigación y desarrollo tecnológico
 - Otros
- El auditor debe utilizar todos los parámetros de medición y evaluación posibles sin caer en un análisis detallado, ya que aquí sólo se trata de detectar la problemática principal de cada área (puede apoyarse en especialistas de informática, auditoría financiera, asesores o consultores externos).
- Si emanan anomalías de considerable importancia de algún elemento evaluado, se deben tomar acciones inmediatas orientadas a eliminarlas o al menos minimizarlas (se plantearán en el plan de auditoría en informática como acciones inmediatas).
- Determinar el nivel de riesgo que existe en cada área de la función de informática: cada área, producto o servicio de informática es susceptible de evaluación y control para asegurar que se desarrolle de acuerdo con los estándares, políticas y procedimientos específicos que le han sido asignados de acuerdo con su función.

Consideraciones que hay que tomar en cuenta al hacer el diagnóstico de la situación actual (etapa preliminar) que sirve para la obtención de la matriz de riesgos:

- El auditor en informática debe conocer de manera aceptable los aspectos de control relativos a cada una de las áreas de informática (tomando en consideración aspectos técnicos y administrativos)
- Se apoyará en la visión de los principales usuarios del negocio y del responsable de informática
- Asimismo, ha de entender que todas las debilidades o anomalías que encuentre serán analizadas y clasificadas por su nivel de riesgo e importancia de su impacto en el negocio

Consideraciones que se deben tomar en cuenta al elaborar la matriz de riesgos:

- Es una tarea relevante y necesaria para el auditor en informática
- Los parámetros para medir el nivel de riesgos pueden variar de acuerdo con factores como la experiencia y conocimiento en la auditoría y de las áreas que

conforman informática o el grado de profundidad y análisis que desee darle el auditor en informática

- Algunos hechos pueden indicar directamente al auditor en informática la existencia de riesgos relevantes (véase tabla 8.3)
- Revisar la matriz de riesgos con el responsable de auditoría en informática
- Asegurarse de tener el soporte que requieran las debilidades o anomalías detectadas (entrevistas, visitas y cuestionarios analizados, revisados y documentados)

Consideraciones para el momento de elaborar la matriz de riesgos:

- Las áreas susceptibles de auditar se mencionarán en el capítulo 13; cada una contempla la siguiente información:
 - Aspectos (componentes o elementos) por evaluar
 - Políticas y procedimientos recomendados
 - Técnicas y herramientas requeridas para su revisión
 - Cuestionarios por cada aspecto (subárea) por evaluar

Nota: Se mencionan las más importantes, pero el auditor en informática puede evaluar otras que considere relevantes para sus objetivos.

- Clasificar cada área y sus componentes por nivel de riesgo, lo que puede ser determinado por el líder de proyecto, los usuarios clave o el responsable de informática
- Dar prioridades a cada área de revisión de acuerdo con el nivel de riesgo o por factores específicos mencionados por la alta dirección o el responsable de informática
- Justificar cada una de las áreas seleccionadas para auditar. La justificación debe basarse en el nivel de riesgo que representa, de acuerdo con las prioridades establecidas por los involucrados de alto nivel o a solicitud expresa de la alta dirección o del responsable de informática (áreas de oportunidad). Esta puede hacerse en un formato parecido al que se presenta en la tabla 8.3.

8.3 Plan general del proyecto de auditoría en informática

Una vez elaboradas, revisadas y documentadas la matriz de riesgos (de acuerdo con los riesgos más relevantes) y las áreas de oportunidad, se procede a la formulación del plan general de informática, el cual consiste básicamente en plantear las tareas más importantes que se ejecutarán durante cierto periodo al efectuar la auditoría en informática.

Los principales aspectos al elaborar el plan general de auditoría en informática son:



Tabla 8.3 Detección de riesgos

Circunstancia	Riesgos
Software pirata	<ul style="list-style-type: none"> • Problemas legales • Mala imagen ante clientes y proveedores • Susceptibilidad de virus computacionales • Dificultad para actualizar los diversos usuarios • Falta de documentación • Pérdida de ofertas del proveedor del software
Inexistencia de metodologías o informalidad en su uso (planeación, desarrollo, etcétera)	<ul style="list-style-type: none"> • Trabajo desarrollado según el criterio de cada individuo • Proyectos individualistas y no de equipo de trabajo • Seguimiento nulo o informal a los proyectos de informática • Se trabaja con base en "inspiración" y no a partir de un método formal (resultado: a veces genialidades y en otras mala calidad) • Dependencia hacia el personal que maneja proyectos clave
Comunicación nula o informal entre informática y alta dirección o áreas usuarias	<ul style="list-style-type: none"> • Proyectos cancelados • Desconocimiento de los requerimientos de negocio • Prioridades mal entendidas • Recursos desperdiciados • Incertidumbre entre el personal ajeno a la toma de decisiones • Falta de compromiso ejecutivo • Estrategias y objetivos de negocio no soportadas por equipos de trabajo • "Amigos distantes"
Otros detectados en el diagnóstico	

- Tomar como referencia los datos recomendados en el proceso metodológico mencionado en el capítulo 6 para encontrar responsables e involucrados en esta tarea
- El plan general de auditoría en informática se deriva de los siguientes elementos:
 - Áreas de oportunidad
 - Matriz de riesgos
 - Prioridades de la alta dirección, de auditoría, de informática o de la misma función de auditoría en informática
- El plan elaborado en esta etapa es general, ya que sólo busca plantear los datos básicos para que la alta dirección los analice y apruebe

- El plan detallado se lleva a cabo posteriormente, en la etapa de adecuación
- Es muy importante la retroalimentación constante entre el líder del proyecto y los demás involucrados (considerando ser breves y concretos en las reuniones)
- Basarse en la tabla 8.4 para la elaboración del plan general

Las actividades principales del auditor en informática o del líder del proyecto para la elaboración del plan general son al menos las siguientes:

- Estimar el tiempo necesario para auditar cada área determinada en la matriz de riesgos y en las tareas de apoyo a fin de lograr las áreas de oportunidad planteadas
- Analizar y definir los aspectos o componentes más relevantes que se evaluarán, tomando como referencia las características propias del negocio y la tabla 8.2
- De ser necesario verificará la importancia y validez de los puntos anteriores con los involucrados sin consumir mucho tiempo ni aplicar tecnicismos en las entrevistas (puede ser vía telefónica, fax o personalmente)
- Asignar prioridades a cada área por evaluar o revisarlas con los principales involucrados en el proyecto
- Definir fechas estimadas de inicio y terminación por área de revisión, no por componente
- Establecer fechas de revisión formales (firmas, aprobaciones) e informales (avances)
- Definir responsables e involucrados directos por etapas del proyecto
- Otras de interés para el auditor en informática según las características del proyecto y el negocio

8.4 Compromiso ejecutivo

Es la última tarea de la etapa de justificación y su objetivo principal es obtener el visto bueno (aprobación) inicial de parte de la alta dirección, usuarios clave y del responsable de informática para continuar con el proyecto de auditoría en informática.

Los aspectos fundamentales para lograr el compromiso ejecutivo a fin de continuar con el proyecto de auditoría en informática son los siguientes:

- Presentación del plan con toda la información de soporte requerida bien documentada y validada con los principales involucrados:
 - Resumen del diagnóstico actual
 - Áreas de oportunidad
 - Matriz de riesgos
 - Prioridades
 - Otros comentarios de apoyo

Tabla 8.4 Plan general de auditoría en informática (etapa de justificación)

Empresa:		Gerencia:		Fecha de aprobación:	
Representante usuario:		Representante de informática:		Líder del proyecto:	
Áreas por auditar según clasificación y prioridades	Aspectos o componentes del área por auditar	Prioridad asignada	Clasificación del riesgo por área (total)	Fecha de inicio/fecha de terminación	
Área seleccionada	Componente(s) seleccionado(s) del área	Número	%	dd/mm/aa dd/mm/aa	
Área seleccionada	Componente(s) seleccionado(s) del área	Número	%	dd/mm/aa dd/mm/aa	
Área(s) seleccionada(s)	Componente(s) seleccionado(s) del área	Número	%	dd/mm/aa dd/mm/aa	

Nota: algunos datos pueden ser omitidos o agregados según considere pertinente el auditor en informática, sin olvidar que en la etapa de formalización se dará todo el detalle requerido del proyecto de auditoría en informática.

- Se debe ser objetivo y claro al exponer el plan general
- Justificar cada una de las áreas por auditar con datos concretos y bien documentados
- Lograr que la alta dirección tome conciencia del compromiso requerido de su parte para la culminación exitosa del proyecto
- Recibir una aprobación formal del plan general (firma)
- El líder de proyecto debe indicar fechas de inicio y terminación estimadas

Las principales actividades del auditor en informática o del líder del proyecto para la elaboración del plan general son al menos las siguientes:

- Revisar el plan general
- Considerar fecha posible de reunión con los involucrados en esta tarea
- Documentar y resumir el diagnóstico actual
- Verificar y documentar áreas de oportunidad y matriz de riesgos
- Justificar cada área de revisión con la información obtenida anteriormente
- Recomendar o negociar fecha de revisión y aprobación del plan con los involucrados
- Efectuar reunión
- Exponer y justificar el plan de auditoría en informática
- Obtener aprobación formal del plan general
- Establecer fechas de inicio del proyecto
- Obtener el compromiso ejecutivo en todo el transcurso del proyecto
- Otros que el auditor en informática considere pertinentes

Resumen

Finalizada satisfactoriamente la etapa preliminar, el auditor en informática se enfoca en la siguiente fase de la metodología, que corresponde a la etapa de justificación. En ésta se dedica a elaborar un documento fundamental para la aprobación del proyecto.

Tal documento contiene principalmente tres productos terminados que contemplan las áreas que se auditarán (matriz de riesgos), el tiempo sugerido para hacerlo (plan de auditoría en informática) y el visto bueno (compromiso ejecutivo) para revisar cada componente de informática seleccionado.

Nota: Es conveniente aclarar que el arranque de la auditoría en informática fue dado antes de que empezara la etapa preliminar.

En la fase de justificación el auditor ha de definir qué áreas y componentes de informática serán revisados y conseguir el compromiso del personal de informática, de los usuarios y demás involucrados para participar cuando les sea requerido.

El conjunto de áreas que se auditarán se documenta y programa en la etapa de justificación. Por otro lado, vale la pena mencionar que la etapa en estudio se deriva de los siguientes elementos:

- Información obtenida en la etapa preliminar
- Diagnóstico del negocio
- Diagnóstico de informática
- Muestreos específicos durante procesos importantes de algún componente que auditoría en informática considere necesario para fortalecer la justificación del proyecto
- Transacciones en los sistemas de información
- Transferencia de archivos paralelos en la red de comunicaciones o revisiones vía reprocesos
- Programas de revisiones rutinarias:
- Apoyo a revisiones de auditoría tradicional. Apoyo a revisiones de planes de seguridad de la empresa

Requerimientos específicos de la alta dirección de la empresa para auditar

La metodología de auditoría en informática establece como segundo paso la etapa de justificación; en ésta, el auditor en informática será lo más específico posible y la matriz de riesgos no generará motivo alguno de confusiones o desacuerdos.

Cada una de las áreas que serán revisadas — según el auditor en informática — tendrá al menos los siguientes elementos de apoyo:

Descripción de la debilidad encontrada y sus consecuencias actuales o futuras en el componente de informática sugerido para auditarse:

Según se detectó en la evaluación preliminar, ¿qué área hay que revisar?

¿Qué problemática se deriva de las debilidades encontradas?

¿Qué gastos o consideraciones económicas genera dicha problemática?

¿Qué aspectos de improductividad proceden de la anomalía detectada?

¿Qué grado de insatisfacción existe a causa de la problemática hallada durante el estudio efectuado en la etapa anterior?

¿Qué riesgos existen o se pueden presentar de persistir dicha anomalía?

Explicación objetiva de la solución recomendada

El auditor en informática debe detallar de manera por demás contundente todas las áreas y componentes de informática que presentan debilidades que ameritan su revisión en una matriz de riesgos.

Con el responsable de informática y un usuario de alto nivel, los clasificará por porcentaje de riesgo de acuerdo con la importancia e impacto en la organización;

asimismo, en un plan de auditoría en informática señalará el orden prioritario con que se han de auditar.

Por último se asegurará de que los responsables de las áreas usuarias y el mismo encargado de informática establezcan un compromiso ejecutivo y estén de acuerdo en cuáles áreas serán auditadas y con qué orden. Lo anterior es con el fin de que desde el momento en que se autorice el plan de auditoría en informática se vayan programando y estimando recursos para que el proyecto de auditoría sea exitoso.

Preguntas clave

1. ¿Qué factores deben existir antes de que el auditor inicie la justificación de su metodología para el desarrollo de sus proyectos?
2. ¿Cómo define la etapa de justificación?
3. Tres productos terminados resultantes de la etapa de justificación son fundamentales. ¿Cuáles son?
4. Mencione brevemente qué contiene cada uno de dichos productos.
5. ¿Quiénes se involucrarán — por parte de la empresa — en esta etapa del proyecto de auditoría y cuál será su función?
6. ¿Cuál es la función de los siguientes integrantes de la función de auditoría en informática en la etapa de justificación?:
 - Responsable de la función de auditoría en informática
 - Líder del proyecto de auditoría en informática
 - Auditor en informática
7. ¿Cuáles son las técnicas y herramientas mínimas que ha de emplear el personal del área de auditoría en informática en esta etapa?
 - Muestreo
 - Análisis
 - Observación/inspección
 - Control de proyectos (planeación de actividades y seguimiento de las mismas)
 - Documentación
 - Análisis costo/beneficio
 - Software de auditoría
 - Software para oficina (procesadores de palabra, hojas de cálculo, presentadores)
 - Microcomputadora
8. Mencione brevemente qué aplicación y beneficios brinda cada una de las técnicas y herramientas seleccionadas en la pregunta anterior durante la etapa de justificación.

9. ¿Qué restricciones se pueden presentar en la etapa de justificación y cómo las puede eliminar o reducir el personal de auditoría en informática a fin de asegurar el éxito del proyecto?
10. ¿Qué problemática se puede presentar a los auditores en informática si omiten la etapa de justificación?
11. ¿Qué se entiende por compromiso ejecutivo?
12. ¿Qué pasaría si faltara ese compromiso en un proyecto de auditoría en informática?

Etapa de adecuación

La etapa de adaptación o de adecuación a las características del negocio se enfoca en el análisis, adecuación y actualización detallados de todos los elementos que intervienen en un proyecto de auditoría en informática.

Las tareas ejecutadas en la etapa de adecuación tienen como objetivo principal adaptar todo el proyecto a las características del negocio, sin olvidar la referencia de los estándares, políticas y procedimientos de auditoría en informática comúnmente aceptados y recomendados por las asociaciones relacionadas con el proceso, así como las formuladas y aprobadas de manera particular en los negocios para informática.

Al terminar la presente etapa, el auditor en informática tendrá el proyecto bien especificado y clasificado; en las etapas restantes sólo se desarrolla e implanta lo definido en la etapa actual.

En la tabla 9.1 se exponen tareas, productos terminados, responsables e involucrados de la etapa de adecuación.

Nota: El orden de las tareas de la etapa de adecuación puede variar conforme la experiencia, recursos, tiempos y prioridades que tenga la función de auditoría en informática.

De acuerdo con el proceso metodológico (Cap. 6), esta etapa es más un trabajo interno que tareas que involucren a usuarios o personal de informática.

La ejecución formal y continua del proceso metodológico hará que muchas actividades se desarrollen con más agilidad y eficiencia con el transcurso del tiempo.

- Etapa de justificación (terminada)
- Etapa de adecuación (en ejecución)
- Etapa de formalización (posterior)

Tabla 9.1 Proceso metodológico de la auditoría en informática: un enfoque práctico

Etapas	Tareas		Productos		Responsable	Involucrados
	Adecuación					
	1.	Definir objetivos del proyecto	1.1	Objetivos y alcances del proyecto	LP	RAI
	2.	Definir etapas del proyecto y su detalle	2.1	Etapas y sus tareas		
			2.2	Plan actualizado	AI/RAI	RAI
			2.2	Responsables e involucrados	AI	LP
			2.3	Productos terminados	AI	LP
			2.4	Revisiones (formal e informal)	AI	LP
	3.	Definir los elementos por auditar por área de revisión	3.1	Aspectos o elementos por evaluar por cada área de revisión	AI	LP
	4.	Establecer técnicas y herramientas por área de revisión	4.1	Técnicas	AI	LP
			4.2	Software	AI	LP
			4.3	Equipo de cómputo	AI	LP
			4.4	Otros de interés para el auditor	AI	LP
	5.	Definición o actualización de políticas por área	5.1	Políticas y procedimientos por verificar de acuerdo con cada área que será auditada	AI	LP
			5.2	Políticas complementarias	AI	LP
	6.	Elaboración o actualización de cuestionarios por área	6.1	Cuestionarios para cada área que será auditada	AI	LP
			6.2	Cuestionarios adicionales	AI	LP

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

9.1 Definición y formulación de objetivos y requerimientos de éxito por área que se va a auditar

La primera tarea de la etapa de adecuación se lleva a la práctica tomando como referencia la información de la tabla 9.1, así como la matriz de riesgos y el plan general de auditoría en informática.

Se sugiere que los objetivos de cada etapa y tarea sean elaborados entre el líder de proyecto y los auditores en informática, que aquél coordinará a lo largo de la auditoría. Adicionalmente se recomienda que se validen con el responsable de la función de informática.

La tabla 9.2 contiene los datos más relevantes que se deben documentar en la presente tarea.

Cada área de revisión debe contemplar de manera clara, para el auditor en informática, sus objetivos (cuantitativos o cualitativos) para poder medir si se han logrado con el paso del tiempo o no.

De igual manera, cada área de revisión ha de especificar los requerimientos de éxito que guiarán al auditor en informática a la culminación exitosa del proyecto.

Nota: Los objetivos y requerimientos de cada área que será auditada se pueden determinar tomando como base la información detallada del capítulo 13; la tabla 9.2 se llenó a manera de ejemplo.

Es conveniente aclarar que la experiencia y criterio de los auditores en informática darán más riqueza y personalidad a la información solicitada a lo largo del proceso metodológico aquí sugerido.

9.2 Actualización del plan general

Conforme se avanza en el proyecto surgen cancelaciones, prioridades, requerimientos, expectativas, nuevos involucrados, etc., que obligan a actualizar el plan de auditoría en informática.

Dicha actualización debe justificarse, debido a que se hizo un compromiso inicial acerca de las áreas que serían auditadas, fechas, prioridades, etc., en la etapa anterior.

Hay que evitar caer en el ciclo de actualización-terminación-actualización-terminación; se recomienda poner en práctica todos los cambios pertinentes para proseguir con la elaboración del plan detallado de auditoría en informática.

Conviene llevar una bitácora de cambios al plan general que contemple:

- Cambio
- Motivo del cambio
- Responsable de solicitar el cambio



Tabla 9.2 Objetivos y requerimientos de auditoría en informática

Área que será auditada	Objetivos de auditoría	Requerimientos de éxito
Usuarios de informática	<ul style="list-style-type: none"> • Verificar la presencia de un comité de informática/usuarios • Asegurar que exista una comunicación formal al final del proyecto • Comprobar que haya un seguimiento formal de los proyectos de informática donde se involucre a los usuarios • Confirmar la presencia del análisis costo/beneficio en los proyectos de informática • Verificar el grado de satisfacción que tienen los usuarios de informática 	<ul style="list-style-type: none"> • Conocimiento satisfactorio de los usuarios de informática y sus funciones • Conocimiento de los servicios que presta Informática • Apoyo de la alta dirección en el desarrollo de la auditoría en informática • Seguimiento del proceso metodológico de la auditoría en informática • Aplicación de cuestionarios propios para esta área • Elaboración de conclusiones emanadas de la falta o cumplimiento formal de políticas y procedimientos definidos para esta área
Otras seleccionadas en la matriz de riesgos	<ul style="list-style-type: none"> • Las que apliquen a las áreas seleccionadas 	<ul style="list-style-type: none"> • Los que apliquen de acuerdo con las áreas seleccionadas

- Tareas o fechas que afecta
- Área(s) por evaluar afectadas por el cambio
- Responsable de aprobar el cambio
- Fecha del cambio
- Plan actualizado
- Otros que el auditor en informática considere necesarios para la culminación exitosa del proyecto

9.3 Plan detallado del proyecto de auditoría en informática

Es una de las tareas más importantes de la etapa de adecuación, ya que en ella se define todo el detalle de los elementos del proyecto; se especifican tareas, productos terminados, responsables, fechas, etc., que serán validados y aprobados en la etapa de formalización para arrancar el proyecto.

Dos tipos de planes detallados con orientación diferente y objetivo común: la administración del proyecto

El momento presente es adecuado para realizar dos planes: en uno se da seguimiento interno a las tareas y responsabilidades de los auditores en informática y en el otro se

especifica el detalle emanado del plan general de auditoría en informática definido en la fase de justificación, mismo que involucra a la alta dirección, usuarios e informática. A continuación se explican brevemente.

- a) Plan interno. Le corresponde al líder del proyecto y su propósito principal es verificar el cumplimiento del proceso metodológico por parte de los auditores en informática a lo largo del proyecto (tabla 9.3). Cabe señalar algunas razones importantes de contar con un plan de este tipo:
 - Elaborar compromisos con base en tareas, productos terminados y los responsables que se recomiendan en el proceso metodológico del capítulo 6
 - Asignar funciones y responsabilidades a los auditores en informática involucrados en el proyecto
 - El líder de proyecto da seguimiento a los auditores en informática con base en dicho plan
 - Utilizar el grado de cumplimiento del plan en futuras evaluaciones del personal
- b) Plan detallado de auditoría en informática (tabla 9.4). Detalla la información relacionada con:
 - El desarrollo de la auditoría en informática, que corresponde a las áreas seleccionadas en la fase de justificación

Tabla 9.3 Plan interno para el seguimiento del proyecto de acuerdo con el proceso metodológico

Etapa	Tareas	Productos	Involucrados	Responsable	Revisiones	Duración
Preliminar						
Justificación						
Adecuación						
Formalización						
Desarrollo						
Implantación						

Nota: esta planeación es de uso exclusivo del líder de proyecto para darle seguimiento a los auditores en informática en el uso formal y adecuado del proceso metodológico. Esto se debe a que muchas tareas son transparentes para los demás involucrados.

Este plan interno se puede hacer antes de la etapa preliminar (o de diagnóstico), sólo que en ese momento se carece de mucho detalle. Esto no sucede en la etapa de adecuación, donde ya se cuenta con el plan detallado de las áreas por auditar (plan detallado de auditoría en informática)

Tabla 9.4 Plan detallado de la auditoría en informática

Tarea	Actividades	Productos terminados	Responsable	Involucrados	Fecha inicio/ fecha término	Fechas de revisión
Verificación de datos	1. Revisar datos del proyecto 2. Documentar	1. Prioridades y matriz de riesgos aprobados	Líder de proyecto/ auditores en informática	Alta dirección/usuarios/ informática		
Evaluación de las áreas por auditar	1. Concertar citas	• Compromiso formal	Auditores en informática	Usuarios/informática		
	2. Realizar entrevistas	• Datos • Documentos de soporte • Otros	Auditores en informática	Usuarios/informática		
	3. Efectuar visitas *	• Datos • Documentos de soporte	Auditores en informática	Responsables de las áreas por visitar		
	4. Aplicar cuestionarios	• Datos • Documentos de soporte	Auditores en informática	Usuarios/informática		
	5. Análisis de información	• Observaciones iniciales • Conclusiones iniciales • Acciones recomendadas	Auditores en informática	Usuarios/informática		
	6. Elaboración del informe preliminar	a) Antecedentes b) Situación actual: • Fortalezas • Debilidades (observaciones) • Áreas de oportunidad	Líder de proyecto/ Auditores en informática	Usuarios/informática		

* Las visitas se pueden llevar a cabo en centros de cómputo y áreas de los usuarios donde se encuentran aspectos de interés relacionados con el proyecto de auditoría en informática, como microcomputadoras, redes locales, equipos de seguridad (extinguidores, detectores de humo, cámaras, cintotecas, papelería, entre otros).

(continúa)

Tabla 9.4 Plan detallado de la auditoría en informática (continuación)

Tarea	Actividades	Productos terminados	Responsable	Involucrados	Fecha inicio/ fecha término	Fechas de revisión
		c) Situación propuesta: • Acciones de mejora • Plazos • Responsables				
	7. Clasificar y documentar el informe preliminar	• Datos • Documentos de soporte	Audidores en informática	Usuarios/informática		
	8. Revisión del informe preliminar	• Informe preliminar revisado	Audidores en informática	Usuarios/informática		
	9. Ejecutar pendientes	• Pendientes terminados	Audidores en informática	Usuarios/informática		
	10. Actualizar el informe preliminar	• Informe preliminar actualizado	Audidores en informática	Usuarios/informática		
	11. Revisar el informe preliminar actualizado	• Informe preliminar actualizado, revisado y aprobado	Líder de proyecto	Usuarios/informática		
Documentar el informe final del proyecto	1. Elaborar el informe de la alta dirección	• Informe de la alta dirección	Líder de proyecto	Usuarios/informática		
	2. Elaborar el informe detallado	• Informe detallado (para usuarios e informática)	Audidores en informática			

(continúa)

Tabla 9.4 Plan detallado de la auditoría en informática (continuación)

Tarea	Actividades	Productos terminados	Responsable	Involucrados	Fecha inicio/ fecha término	Fechas de revisión
Revisión del informe final de la auditoría en informática	1. Presentar los informes de la alta dirección actualizados, revisados y detallados	<ul style="list-style-type: none"> • Informes revisados • Informes aprobados formalmente 	Responsable de la función de auditoría en informática	Alta dirección Usuarios clave		
	2. Aprobación de los informes	<ul style="list-style-type: none"> • Compromiso ejecutivo para ejecutar las acciones sugeridas 	Líder de proyecto	Responsable de la función de informática		
	3. Compromiso ejecutivo					

- Documentación, revisión y aprobación del informe de auditoría en informática
- Implantación de las acciones recomendadas

Los datos mencionados en el plan detallado de informática se enfocan en ser la guía del proyecto de auditoría en informática desde el punto de vista del cliente, ya que describen tareas, productos terminados, responsables, involucrados, fechas de revisión, etcétera.

Aspectos relevantes del plan detallado de auditoría en informática:

- Especifica responsables e involucrados en cada área por auditar
- Es el detalle final del plan
- Ya fue adaptado y actualizado según características específicas del proyecto
- Con base en dicho plan se dará seguimiento por parte de la alta dirección, los responsables de los usuarios de informática, de informática y de auditoría en informática
- Con el plan detallado terminado y aprobado en la etapa de formalización, puede darse inicio a la auditoría en informática (evaluación de las áreas de informática seleccionadas)

9.4 Aspectos por evaluar en cada área de revisión

Estos aspectos o componentes fueron mencionados en la matriz de riesgos; lo que procede es confirmar si son las requeridas y si los objetivos de las áreas mencionados en la tabla 9.2 son válidos y completos (recuérdese que los datos de la tabla sólo son ilustrativos).

Los cuestionarios acerca de los componentes de cada área evaluable se mencionan en el capítulo 13; los mismos deben ser actualizados y validados conforme las características de las áreas de revisión sufran modificaciones relevantes por efecto del medio tecnológico o del mismo negocio.

Es recomendable que las áreas susceptibles de auditar y los componentes de cada área que sean agregados por el auditor en informática en el momento en que un proyecto lo requiera, cuenten con los cuestionarios correspondientes y, de ser posible, con el formato y secuencia de tareas sugeridas para no perder continuidad.

9.5 Definición de técnicas y herramientas por área de revisión

Aquí se especifican las técnicas y herramientas recomendadas que debe conocer amplia y satisfactoriamente el auditor en informática para la revisión de las áreas contempladas en el plan detallado.

La experiencia profesional que se haya obtenido en cada una de las áreas (desarrollo, telecomunicaciones, mantenimiento, administración de informática, etc.) hace más viable tanto la auditoría como la definición eficiente de soluciones.

No es un punto negativo no haber trabajado en las áreas que se auditarán; simplemente el grado de investigación y actualización en los temas o aspectos que se evaluarán debe ser más profundo.

Es casi imposible asegurar que todos los auditores en informática dominen todas las áreas de informática que se pueden auditar; sin embargo, el especialista en el campo ha de actualizarse en la medida de lo posible en las áreas que considere críticas para su negocio o, específicamente, en los requerimientos que van surgiendo a lo largo del trabajo. Por último, no hay que olvidar que se debe ser proactivo, no reactivo.

En el apéndice B se recomiendan algunas técnicas y herramientas para cada área definida en la tabla 8.1. Conviene aclarar que no son limitativas.

9.6 Definición o actualización de estándares, políticas y procedimientos por área de revisión

Todas las acciones operativas y administrativas de las organizaciones se deben orientar con base en lineamientos, políticas y procedimientos, con el objetivo principal de que los individuos que en ella laboran, lo hagan en forma metódica (sin entender esto como un trabajo mecánico y robotizado), con estándares de negocio o con normas de calidad y productividad comúnmente aceptadas en negocios similares al giro de empresa.

Además existen asociaciones profesionales, instituciones educativas, etc., que orientan a los individuos a trabajar de una manera productiva y especializada.

Las normas y habilidades personales no serán afectadas por políticas rígidas y obsoletas de algunos negocios; deberá haber compatibilidad y congruencia entre lo que determina el negocio como reglas de trabajo y las aspiraciones y habilidades del personal.

En lo que se refiere a estándares, políticas y procedimientos, se aclara que las actividades y elementos que se relacionan con informática suelen operar bajo estándares aceptados en el medio de dicho campo.

Las funciones de desarrollo e implantación de sistemas de información, al igual que las de planeación de informática o de telecomunicaciones e investigación, se encuentran en un marco nacional e internacional donde existen estándares, metodologías, técnicas y herramientas de trabajo recomendadas para un desempeño eficiente de cada una de las actividades inherentes a sus tareas.

¿Cómo se definen estándares, políticas y procedimientos de auditoría en informática?

Al igual que para las funciones de planeación, telecomunicaciones, etc., en este campo existen asociaciones integradas por profesionales de gran experiencia y conocimiento

en el campo que se enfocan en establecer, formalizar, difundir y recomendar la aplicación de los estándares, políticas y procedimientos más convenientes a las necesidades actuales y futuras del área de especialización a la que se dedican.

Los estándares, políticas y procedimientos de informática en tanto técnicas de análisis y diseño de sistemas de información, los diferentes tipos de base de datos, las topologías y protocolos en comunicaciones, y los lineamientos de control interno emanan de dichas asociaciones; sin embargo, las empresas pueden crear, formalizar y difundir sus propias políticas y procedimientos, aunque su alcance y cumplimiento será interno y, en ocasiones, con sus clientes o proveedores.

¿Es una obligación el uso de estándares?

Los estándares no son dogma de empresa alguna. Como diferentes asociaciones o profesionistas ofrecen variantes del mismo aspecto, lo importante es que den soluciones comunes al mismo problema o a la misma área de oportunidad. Es posible llevarlos a la práctica total o parcialmente u omitir su aplicación; depende de cada negocio.

En un futuro muy próximo se espera que cualquier tecnología (se trate de equipos de cómputo, lenguajes de programación, bases de datos, comunicaciones, metodologías y técnicas de desarrollo, planeación, etc.) ya no sea más elemento de alto desempeño y baja integración, desde el punto de vista de soluciones totales de informática.

Los estándares o normas se orientan a lo que su nombre se refiere: a uniformar métodos de trabajo, tecnologías, parámetros de desempeño, costos, cualidades, facilidades, etc. En esto reside la ventaja de seguir lo que dictan los estándares de mercado propuestos por las asociaciones profesionales e independientes, al menos mediante trabajos de investigación.

Ahora bien, el auditor en informática no dependerá de lo que dictan a nivel nacional o internacional los estándares; éstos sólo son puntos de referencia. Su criterio y experiencia profesional, aunados a las características del negocio donde ejerce, le dictarán la necesidad de actualizar estándares, políticas y procedimientos conforme den al negocio las soluciones requeridas.

Hay que estar atento a lo que los especialistas propongan como estándares, políticas y procedimientos (incluyendo la auditoría en informática) a través de suscripciones a revistas especializadas, bases de datos vía telecomunicaciones, inscripciones a asociaciones, asistencia a seminarios, actualización profesional con maestrías o cursos de posgrado, estudio constante del negocio, entre otros.

Por último, es conveniente atender los estándares propuestos por los especialistas independientes del campo, llámense consultores o asociaciones, reconocidos a nivel local, nacional o internacionalmente, los cuales se pueden enriquecer si intervienen proveedores líderes de mercado en el campo de la informática que se encuentre en estudio.

¿Únicamente las asociaciones pueden establecer estándares, políticas y procedimientos de auditoría en informática?

No; aunque agrupan el mayor número de personas expertas en la auditoría e informática dedicadas a estudiar y sugerir los elementos tecnológicos o administrativos relacionados con informática (incluyendo auditoría) que se encuentran en el mercado o que se pueden introducir al mismo y que brinden soluciones a los negocios de una manera más eficiente y segura.

En ocasiones (sucede continuamente con los equipos de cómputo o el software) las ventas que logra un proveedor a nivel mundial, establecen un nuevo estándar o, al contrario, la caída estrepitosa o los problemas legales afectan a tal grado la imagen de algún proveedor líder en el mercado, que — de manera casi automática — sus productos tecnológicos definidos como estándares salen del mercado para convertirse en obstáculos o sinónimos de obsolescencia en las empresas.

Cabe señalar que existen consultores independientes y bajo nómina tanto en empresas privadas como gubernamentales que pueden establecer estándares, políticas y procedimientos internos. Las características que han de cumplir para tomarse como tales en los negocios son las siguientes:

- Referir exigencias externas relativas al control y la seguridad
- Justificar la necesidad de su existencia ante el negocio
- Probados, difundidos y autorizados por el responsable directo donde se ejercerán o llevarán a la práctica
- Elaborados y descritos formalmente en documentos (hojas, archivos, etcétera)
- Aprobados por la alta dirección
- Difundidos amplia y formalmente por los involucrados en su cumplimiento
- Cumplirlos formalmente
- Actualizarlos con oportunidad (evitar su obsolescencia)

Hay que recalcar que las asociaciones profesionales tienen un reconocimiento oficial que no poseen los paradigmas establecidos por los consultores independientes o el personal interno de una empresa (a menos que el liderazgo o impacto de ellas trascienda a los demás negocios y se convierta en estándar de mercado).

Las ventajas de las asociaciones nacionales e internacionales al respecto son:

- Los estándares recomendados son reconocidos a nivel nacional e internacional
- Agrupan personal de gran experiencia en el campo
- Existen programas de actualización e iniciación en la auditoría en informática
- Conocen los requerimientos y habilidades que entraña la auditoría en informática para apoyar a los negocios con oportunidad y eficiencia en aspectos de seguridad y control
- Cursos y seminarios continuos

- Se pueden intercambiar experiencias con miembros de diferentes empresas y países

En el apéndice A se desglosan algunas políticas y procedimientos sugeridos que deben existir como mínimo en las áreas susceptibles de auditar mencionadas en capítulos anteriores.

9.7 Elaboración o actualización de cuestionarios por área de revisión

Cada entrevista, visita o verificación de la etapa de desarrollo de la auditoría en informática (reflejada en el plan detallado como la evaluación de las áreas seleccionadas) será apoyada con preguntas específicas y definidas con anterioridad.

Los cuestionarios que corresponden a cada área que será auditada tendrán carácter formal y estarán orientados a detectar las debilidades o inexistencias relativas al control y seguridad de informática que competen a cada área.

Los cuestionarios pueden aplicarse en una entrevista personal con los involucrados en el proyecto (usuarios o personal de informática), por medio de visitas de verificación física (evaluación de equipos y materiales de informática de interés para el proyecto) o mediante listas de verificación (listado de preguntas breves y concretas) orientadas al personal que requiere una atención breve por sus múltiples aplicaciones o simplemente porque lo que se busca de él es una participación mínima en el trabajo del proyecto.

Las características básicas de los cuestionarios son: actualización, orientados a los aspectos evaluados, sintéticos (no redundantes), técnicos si se requiere y basados — si es posible — en estándares nacionales o internacionales.

En el apéndice B se mencionarán los cuestionarios mínimos sugeridos para cada uno de los componentes de las áreas susceptibles de auditarse.

Resumen

En su estructura de trabajo, la metodología de la auditoría en informática define ciertas consideraciones y criterios que brindan flexibilidad y amplitud al auditor en informática con objeto de que sus proyectos puedan responder a las características de la empresa donde presta sus servicios profesionales.

La etapa de adecuación es un conjunto de tareas estructuradas básicamente para que el proyecto de auditoría en informática se adapte a las necesidades de la empresa estudiada. En este punto resulta, pues, de suma importancia recalcar que la metodología tratada en este libro no se limita a la auditoría en informática para grandes corporaciones o centros de cómputo de magnitudes considerables.



Las etapas, tareas y actividades recomendadas a lo largo del presente material se apoyan en la etapa de adecuación a fin de garantizar que todos los proyectos de auditoría en informática puedan ser exitosos.

La clave del auditor en informática es la adaptabilidad y flexibilidad que brinde a cada empresa y a la función de informática que ahí se encuentre.

A continuación se mencionan los elementos que se deben contemplar antes de iniciar formalmente la revisión de las áreas aprobadas en la etapa anterior (justificación).

1. Objetivos y requerimientos de éxito por cada área que será auditada

Luego de terminar las etapas preliminar y de justificación, el auditor en informática podrá definir con más certeza los objetivos y requerimientos particulares a fin de concluir positivamente la revisión de las áreas mencionadas en el plan de auditoría en informática.

2. Plan de auditoría actualizado

En esta fase — también llamada plan de auditoría en informática de la etapa de justificación — una vez especificados todos los requerimientos de éxito y conociendo los factores tecnológicos, humanos y organizacionales que intervienen, el auditor puede actualizar el plan de trabajo y detallar fechas, tiempos, resultados esperados, funciones y responsabilidades, así como estimar gastos y el número de personas de las áreas usuarias y de informática que participarán en el proyecto.

Ya es posible estimar, con alto grado de certidumbre, los aspectos o componentes que se deben evaluar por cada área de informática durante el desarrollo de la etapa de adecuación.

Debido a las características de la empresa o al criterio del personal clave involucrado en el proyecto, los componentes de las áreas contemplados en el plan se pueden subdividir o integrar a otros, si es que el escenario del negocio en cuestión lo justifica.

3. Definición de técnicas y herramientas

Una parte sobresaliente y estratégica para el buen desempeño de la auditoría en informática es que se definan las técnicas y herramientas idóneas y necesarias para revisar adecuada y eficientemente cada área seleccionada.

Se hace hincapié en que herramientas como las de auditoría de software que incluyen un conjunto de técnicas como análisis, documentación, muestreo, etc., son elementos indispensables para el aseguramiento de la calidad y confiabilidad de la auditoría.

4. Adecuación a la alta política de empresa

Ninguna de las tareas realizadas por la auditoría en informática debe ser ajena al cumplimiento de los estándares, políticas y procedimientos establecidos por las

asociaciones profesionales relativas a la misma; tampoco se omitirán los procedimientos y políticas formalmente establecidos en la empresa donde se preste el servicio durante el desarrollo de la auditoría. Definido y detallado el plan, el auditor procederá con suma objetividad y disciplina a establecer referencias cruzadas entre los estándares, políticas y procedimientos comúnmente aceptados y cada uno de los componentes de informática que serán auditados.

Por mencionar algunos ejemplos, microcomputadoras, sistemas de información y metodología de desarrollo tienen definida una serie de características. El auditor habrá de referirse a éstas en primera instancia cuando inicie la revisión en la etapa de desarrollo (explicada en un capítulo posterior).

5. Cuestionarios

Un conjunto de cuestionarios particulares complementan el trabajo del auditor durante el desarrollo de su evaluación; de los mismos se derivan entrevistas, visitas a los centros de cómputo o departamentos usuarios.

Los cuestionarios son una herramienta de gran valor para el auditor en informática; están estructurados de manera que sirven de guía a fin de verificar la confiabilidad de la información del personal entrevistado; además, permiten percibir el grado de cumplimiento de estándares, políticas y procedimientos comúnmente aceptados.

Preguntas clave

1. ¿Qué factores deben existir antes de que el auditor inicie la etapa de adecuación de la metodología de auditoría en informática para el desarrollo de sus proyectos?
2. ¿Cómo define la etapa de adecuación?
3. ¿Qué importancia tiene para el auditor definir los objetivos y requerimientos de éxito de cada área que será auditada?
4. ¿Qué componentes debe enriquecer el auditor en informática para terminar su plan detallado?
5. ¿Hay que subdividir en componentes cada área por auditar? Cite algunos componentes básicos de cada una de las áreas mencionadas a continuación:
 - Sistemas de información
 - Redes locales
 - Seguridad
6. ¿Por qué es importante para el auditor en informática definir con claridad las técnicas y herramientas que utilizará en cada componente de las áreas auditadas?
7. Mencione las técnicas y herramientas básicas para cada uno de los componentes que mencionó en el punto 5.

8. ¿A qué se debe la importancia de respetar y tomar como referencia los estándares, políticas y procedimientos comúnmente aceptados y establecidos por asociaciones profesionales?
9. ¿Considera importante tomar en cuenta las políticas y procedimientos de informática establecidos previamente en la empresa? ¿Por qué?
10. ¿Qué importancia tiene para usted el uso de cuestionarios de auditoría en informática?
11. ¿Es conveniente adecuar los cuestionarios de acuerdo con las características de la empresa o pueden ser los mismos para todas las áreas de informática?
12. ¿Quiénes han de involucrarse en esta etapa del proyecto y cuál será su función?
13. ¿Cuál será la función de cada uno de los siguientes integrantes de la función de auditoría en informática en la etapa de adecuación:
 - Responsable de la función de auditoría en informática
 - Líder del proyecto de la auditoría en informática
 - Auditor en informática
14. ¿Cuáles de las siguientes técnicas y herramientas debe utilizar como mínimo el personal del área de auditoría en informática cuando lleven a cabo dicha etapa?:
 - Muestreo
 - Análisis
 - Observación/inspección
 - Control de proyectos (planeación de actividades y seguimiento de las mismas)
 - Documentación
 - Análisis costo/beneficio
 - Software de auditoría
 - Software para oficina (procesadores de palabra, hojas de cálculo, presentadores)
 - Microcomputadora
15. Mencione brevemente qué aplicación y beneficios le brindarían en la etapa de adecuación cada una de las técnicas y herramientas que seleccionó en la pregunta anterior
16. ¿Qué restricciones se pueden presentar en la etapa de adecuación y qué acciones debe implantar el personal de auditoría en informática a fin de eliminarlas o al menos minimizarlas para asegurar el éxito del proyecto?
17. ¿Qué problemática se puede presentar a los auditores en informática si se omite el desarrollo de la etapa de adecuación?

Etapas de formalización

Las fases anteriores fueron de introducción e investigación del negocio y sus diversas funciones; en ellas se detectaron las debilidades y fortalezas más relevantes; se definió la planeación y proyección de las áreas que requieren ser auditadas, y se documentaron las adecuaciones o agregados requeridos. En la presente etapa (formalización) corresponde a la alta dirección dar su aprobación y apoyo formal para el desarrollo del proyecto de auditoría presentado por el líder de proyectos y el responsable de la función de auditoría en informática.

- Etapa de adecuación (terminada)
- Etapa de formalización (en ejecución)
- Etapa de desarrollo (posterior)

La participación real de la alta dirección es básica, lo mismo que la del responsable de la función de informática en el negocio. Los usuarios clave también deben estar presentes durante el proceso de formalización del proyecto.

El objetivo primario de esta etapa es claro: justificar el desarrollo del proyecto con base en todos los argumentos y detalles encontrados, analizados y clasificados en las fases anteriores.

La duración de la etapa no debe ser muy prolongada, ya que se obtuvo el visto bueno de los usuarios clave y del personal de informática en la etapa de adecuación, específicamente en el plan detallado de informática.

Ahora bien, conviene tener presente que la etapa de formalización se puede desarrollar al mismo tiempo que la fase de adecuación si existen los recursos y los involucrados se encuentran disponibles.

Tareas, productos terminados, responsables e involucrados se especifican en la tabla 10.1.

Tabla 10.1 Proceso metodológico de la auditoría en informática: un enfoque práctico

Etapa	Tareas		Productos	Responsable	Involucrados
Formalización	1. Verificar prioridades y cursos de acción	1.1	Prioridades clasificadas	LP	RAI
		1.2	Áreas por auditar verificadas	AI/LP	RAI
	2. Verificar plan y actividades	2.1	Etapas y sus tareas	AI	LP
		2.2	Plan detallado final		
	3. Presentación formal del proyecto	3.1	Proyecto revisado de la auditoría	RAI	AD/PU/RI
		3.2			
	4. Aprobación formal del proyecto de auditoría en informática	4.1	Aprobación del proyecto	AD/PU/RI AD LP	RAI/LP RAI/RI/PU AD/PU/PI
		4.2	Compromiso ejecutivo		
		4.3	Inicio formal del proyecto		
	5. Presentación del proyecto a los usuarios de informática	5.1	Entendimiento del proyecto	RI PI/PU PI/PU	LP/AI LP/AI LP/AI
		5.2	Aceptación del proyecto		
		5.3	Compromiso de cada una de las áreas involucradas		
	6. Definir las áreas por visitar y concertar citas con el personal que se va a entrevistar	6.1	Fechas de entrevistas	LP LP LP	PI/PU PI/PU PI/PU
		6.2	Fechas de visitas		
		6.3	Fechas para aplicación de cuestionarios		

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor de informática

10.1 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 en informática, ya que mediante su realización se clarifica el rumbo, límites y cobertura que tendrá el proyecto.

Las actividades requeridas en la presente tarea son una serie de pequeñas entrevistas personales o reuniones de varios involucrados con un enfoque muy objetivo y práctico.

Se recomienda que el auditor en informática (o el líder de proyecto) documenten lo expuesto en las reuniones o entrevistas que se efectúen mediante una minuta o resumen (tablas, gráficas, narrativa, etc.), donde se mencionen los puntos tratados y las conclusiones. Lo anterior tiene más validez si aparecen las firmas de conformidad de cada participante.

Prioridades. Son las acciones que deben llevarse a cabo antes que las demás sugeridas para el proyecto. Esto se justifica al menos por las siguientes circunstancias:

- Urgencia de mejorar algún hecho que perjudica en alto grado al negocio
- Un requerimiento específico de la alta dirección
- Implantación de algún proceso previamente justificado
- Otros

Restricciones. Son los hechos o circunstancias identificables que están ocurriendo o que pueden ocurrir en el transcurso de la auditoría y que van afectar directa o indirectamente al proyecto. Por lo general son limitaciones o carencias que no se podrán resolver de inmediato o a lo largo del proyecto; por ejemplo:

- Falta de experiencia de los auditores en informática
- Bajo presupuesto para asignar recursos al proyecto
- Escepticismo de la alta dirección o de los usuarios respecto de este tipo de proyectos
- Otros

Alcance. Aquí se define la cobertura específica que tendrá el proyecto; se aclara qué se hará en éste (tareas, etapas) y los resultados (productos terminados).

Lo que no se mencione aquí (excepto que se justifique la omisión) no se obtendrá durante el proyecto. Es muy importante valorar estos aspectos al menos una vez antes de que arranque el proyecto; después sería ir en contra del proceso metodológico y de los recursos y tiempos dedicados hasta este punto.

10.2 Actualización del plan de auditoría en informática

Se ha hablado de cómo actualizar un plan; lo importante en este momento es asegurarse de que los pocos (pero significativos) cambios que se hayan suscitado después de realizar la tarea anterior, se reflejen en el plan detallado de auditoría en informática que se presentará a la alta dirección para su aprobación final y formal.

10.3 Presentación formal del plan de auditoría en informática

La presente tarea es la más importante para el líder del proyecto y el responsable de la auditoría en informática, ya que en ésta se justificará la continuación del proyecto.

Las actividades primordiales del responsable de esta tarea son:

- Asegurarse de contar con toda la información en un formato de presentación resumida e inteligible, ya que su principal audiencia será la alta dirección, los usuarios clave y el responsable de informática
- Revisarla y verificarla con este último
- Concertar la cita en una fecha y lugar apropiados
- Ser fluido, claro y contundente en la presentación de la información
- Asegurar el entendimiento de la audiencia de los datos presentados

Las consideraciones clave son:

- Contar con todo el soporte documentado de lo que será presentado
- No asistir a la junta sin aclarar las dudas o pendientes de tareas anteriores
- Lograr que la alta dirección tome conciencia de la importancia de su apoyo al proyecto
- Hacer que todos los presentes comprendan que forman un equipo de trabajo
- Apoyarse en los usuarios clave o en el responsable de informática, de ser necesario

10.4 Aprobación formal del proyecto de auditoría en informática

Se puede decir que es la tarea más breve y una de las más importantes, ya que de ella surge la aprobación formal del proyecto.

Una vez logrado el visto bueno de todos los involucrados, la responsabilidad de la función de auditoría en informática es más clara y evidente: terminar con éxito el proyecto, pues uno de los dilemas a que se enfrentan muchos proyectos ha sido superado, el obstáculo de continuar con la etapa siguiente (en gran número de empresas muchos proyectos viven entre lo que llaman comúnmente proyectos en proceso de

justificación, en cartera [o espera] o cancelados). Aquí ha pasado a la autorización para su desarrollo y terminación, según el plan de auditoría en informática.

Consideraciones clave que aseguran la terminación satisfactoria de esta tarea:

- Presentar un resumen de la matriz de riesgos, áreas de oportunidad, plan detallado de auditoría en informática, prioridades, restricciones, etc. (en términos claros)
- Entendimiento del proyecto (la información tiene el mismo significado para todos)
- No surgen adecuaciones al proyecto (nuevas prioridades, áreas por revisar, etcétera)
- Se aprueba formalmente el proyecto (firma de conformidad de los involucrados)
- Se autorizan las fechas de inicio del proyecto
- Otras que el auditor en informática considere pertinentes en su negocio

Nota: La alta dirección no siempre autoriza todo lo planeado; en ocasiones, la falta de una buena venta del proyecto en la presentación o la falta de compromiso por alguno de los involucrados puede retrasar su aprobación formal; sin embargo, el líder del proyecto o el responsable de auditoría en informática tienen que continuar justificando y documentando el proyecto hasta lograr la aprobación de todos.

10.5 Compromiso ejecutivo

Sólo se comentará que una vez terminada la tarea anterior, el siguiente paso es lograr que la alta dirección, los usuarios clave, el responsable de informática y el responsable de la auditoría en informática se comprometan a lo largo del proyecto, desde ese momento hasta lo que es el desarrollo e implantación de las acciones recomendadas por auditoría en informática en su informe final.

El apoyo requerido por los involucrados se traduce en los siguientes aspectos:

- Difusión de los objetivos y alcance del proyecto con los usuarios y personal de informática que serán entrevistados y visitados por los auditores en informática
- Proporcionar la información requerida por auditoría en informática
- Asignación de recursos como:
 - Equipo de cómputo
 - Espacio físico para trabajar si se requiere estar por tiempo prolongado en las áreas de informática o usuarias
 - Tiempo
- Cumplimiento de su función dentro del proyecto de manera oportuna
- Revisión y aprobación del informe (el cual debe ser justificado)

- Implantación de las acciones recomendadas al final del proyecto
- Otros

La función de auditoría se compromete a:

- Utilizar un proceso metodológico y adecuado al negocio
- Trabajar con ética y profesionalismo
- Dar soluciones factibles y de valor agregado
- Apoyar a informática y áreas usuarias en la implantación de soluciones recomendadas en el proyecto
- Guardar de manera confidencial la información manejada en el proyecto

Resumen

En conjunto, las etapas anteriores brindan al auditor un panorama de la situación de la empresa y de la función de informática (evaluación preliminar), un diagnóstico de debilidades y problemática de las áreas relacionadas con informática, así como un plan preliminar para la auditoría en informática (justificación).

Además, antes de iniciar la etapa de formalización cuenta con todo el detalle de componentes metodológicos, técnicos y de logística necesarios (adecuación) para resolver con éxito el proyecto de auditoría en informática.

El objetivo actual es cerrar positivamente las tareas y actividades de las etapas anteriores con el visto bueno de la dirección para revisar a profundidad las áreas de informática justificadas con anterioridad.

Se puede afirmar que la etapa de formalización compete de manera exclusiva al director de la empresa o a los ejecutivos interesados en que la auditoría en informática se realice.

La autorización y difusión del inicio del proyecto marca la pauta para que todos los involucrados en la revisión participen y proporcionen información de la manera siguiente:

- Mencionen debilidades que entorpecen la operación o generan improductividad
- Revisen resultados emanados de la auditoría
- Brinden líneas estratégicas para que el auditor las considere en las recomendaciones que generen acciones en el mediano y largo plazo
- Faciliten espacio y herramientas a los auditores del proyecto
- Los apoyen para que sean recibidos por el personal a su cargo y, por último, se comprometan a implantar oportunamente las acciones recomendadas en el informe final (producto generado en la etapa de desarrollo)

Por su parte, la dirección general de la empresa o la alta dirección de la misma se compromete a brindar apoyos financieros y de autoridad para que los tiempos y resultados se den conforme a lo recomendado por el auditor en informática.

A continuación se mencionan algunos puntos para asegurar el éxito del proyecto o equipo de trabajo:

- Funciones
- Tiempo de participación
- Deseado
- Actitud
- Lugar físico de trabajo
- Tareas rutinarias
- Revisiones informales
- Revisiones formales
- Capacitación
- Recursos
- Asesoría
- Analistas

Preguntas clave

1. ¿Qué factores debe haber antes de iniciar la etapa de formalización de la metodología de la auditoría en informática para el desarrollo de los proyectos de revisión?
2. ¿Cómo se define la etapa de formalización?
3. ¿Qué actividades relevantes se llevan a cabo en la etapa de formalización?
4. ¿Qué beneficios brinda dicha aceptación?
5. ¿Qué problemas generaría el rechazo de la presente etapa?
6. ¿Qué características debe tener el reporte de auditoría en informática para la aprobación formal?
7. ¿Qué productos terminados de las etapas anteriores hay que documentar y presentar para la justificación o aprobación del proyecto?
8. ¿Por qué es importante que el auditor en informática defina con claridad las reglas del proyecto de auditoría durante la fase de desarrollo e implantación?
9. Mencione algunas reglas básicas y necesarias para el éxito del proyecto.
10. ¿Qué deben hacer los responsables de las áreas usuarias y de informática que participarán en la auditoría para que el personal involucrado la asimile y acepte?
11. ¿Es importante tomar en cuenta las políticas y procedimientos de informática establecidos en la empresa con anterioridad? ¿Por qué?
12. ¿Qué importancia tiene la aprobación formal del proyecto de auditoría en informática?
13. ¿Quiénes intervendrán en esta etapa del proyecto y cuál será su función?
14. ¿Cuál es la función de cada uno de los siguientes integrantes de la función de auditoría en informática en la etapa de adecuación?



- Responsable de la función de auditoría en informática
 - Líder del proyecto de auditoría en informática
 - Auditor en informática
15. ¿Cuáles de las siguientes técnicas y herramientas debe utilizar el personal del área de auditoría en informática en dicha etapa?
- Muestreo
 - Análisis organizacional/análisis de sistemas/análisis de procesos
 - Observación/inspección
 - Control de proyectos (planeación de tareas y seguimiento)
 - Documentación
 - Análisis costo/beneficio
 - Software de auditoría o software para oficina (procesadores de palabras, hojas de cálculo, presentadores) microcomputadora
16. Explique brevemente qué aplicación y beneficios le brindarían en la etapa de desarrollo cada una de las técnicas y herramientas que seleccionó en la pregunta anterior.
17. ¿Qué restricciones se pueden presentar en la etapa de formalización y qué acciones ha de realizar el personal de auditoría en informática para eliminarlas o al menos reducirlas a fin de garantizar el éxito del proyecto?
18. ¿Qué problemática se puede presentar a los auditores en informática si se omite el desarrollo de la etapa de formalización?

Etapa de desarrollo

Es la etapa más importante para el auditor en informática porque aquí ejerce su función de manera práctica; empieza a ejecutar las tareas de su trabajo de acuerdo con el plan aprobado en la etapa de formalización.

Esta fase comprende:

- a) Concertación de fechas de entrevistas, visitas y aplicación de cuestionarios
- b) Verificación de tareas, de involucrados y productos terminados
- c) Clasificación de técnicas, herramientas, cuestionarios y entrevistas
- d) Aplicación de entrevistas y cuestionarios
- e) Visitas de verificación
- f) Elaboración del informe preliminar correspondiente a los componentes por área auditada
- g) Revisión del informe preliminar
- h) Clasificación y documentación del informe preliminar
- i) Finalización de tareas o productos terminados pendientes
- j) Elaboración del informe final de la auditoría en informática
- k) Presentación a la alta dirección y participantes clave
- l) Aprobación del proyecto y compromiso ejecutivo

En la tabla 11.1 se especifican tareas, productos terminados, responsables e involucrados de la etapa de desarrollo.

- Etapa de formalización (terminada)
- Etapa de desarrollo (en ejecución)
- Etapa de implantación (posterior)

Tabla 11.1 Proceso metodológico de la auditoría en informática: un enfoque práctico

Etapas	Tareas	Productos	Responsable	Involucrados
Desarrollo	1. Concertar citas	1.1 Fechas aprobadas o actualizadas	AI	PI/PU
	2. Verificar tareas, involucrados, etc.	2.1 Tareas, involucrados, etc. revisados	AI	PI/PU
	3. Clasificar técnicas, cuestionarios y herramientas por usar	3.1 Técnicas clasificadas	AI	LP
		3.2 Cuestionarios clasificados	AI	LP
		3.3 Herramientas clasificadas	AI	LP
	4. Efectuar entrevistas	4.1 Entrevistas realizadas	AI	PI/PU
		4.2 Entrevistas documentadas	AI	AI
		4.3 Análisis de entrevistas	LP/AI	RAI
	5. Aplicar cuestionarios	5.1 Cuestionarios aplicados	AI	PI/PU
		5.2 Cuestionarios documentados	AI	AI
		5.3 Análisis de cuestionarios	LP/AI	RAI
	6. Efectuar visitas de verificación	6.1 Visitas realizadas	AI	RI/PI/PU
		6.2 Comentarios documentados	AI	AI
		6.3 Análisis de comentarios	LP/AI	RAI
	7. Elaborar informe preliminar acerca de las áreas auditadas	7.1 Observaciones (acerca de debilidades o carencia de controles)	AI	LP
		7.2 Áreas de oportunidad	AI	LP
		7.3 Alternativas por cada área de oportunidad detectada	AI	LP
		7.4 Recomendaciones (acciones específicas) por alternativa	AI	LP
		7.5 Responsables de ejecutar cada acción	AI	LP
		7.6 Plazos de ejecución por acción	AI	LP
		7.7 Áreas auditadas clasificadas	AI	LP
		7.8 Informe documentado, almacenado y clasificado	AI	AI

(continúa)

Tabla 11.1 Proceso metodológico de la auditoría en informática: un enfoque práctico (continuación)

Tabla 11.1 Proceso metodológico de la auditoría en informática: un enfoque por etapas						
Etapa	Tareas	Productos	Responsable		Involucrados	
			LP	RAI/AI		
Desarrollo	8. Revisar el informe preliminar por área	8.1 Borrador de auditoría en informática revisado	LP		RAI/AI	
	9. Autorizar el borrador del informe preliminar	9.1 Informe preliminar revisado	LP		PI/PU/AI	
		9.2 Informe preliminar corregido	AI		LP	
		9.3 Informe preliminar entregado	LP		LP	
		9.4 Informe preliminar autorizado	AD/PI/PU		AD/PI/PU	
	10. Efectuar entrevistas, cuestionarios y visitas complementarias	10.1 Entrevistas, cuestionarios y visitas pendientes realizados	LP/AI		PI/PU	
		10.2 Informe actualizado con observaciones, acciones, etc.	AI		LP	
	11. Elaborar informe final	11.1 Informe final revisado con información de todas las áreas auditadas	AI		LP	
		11.2 Informe con visto bueno del responsable de la función de auditoría en informática	RAI		LP/AI	
		11.3 Informe final almacenado en medios magnéticos (respaldo)	AI		AI	
		11.4 Documentación del informe para la alta dirección	LP/AI		RAI	
		11.5 Documentación del informe para responsables de los usuarios de informática e informática	AI		LP	
	12. Elaborar un plan de implantación general de acciones sugeridas	12.1 Acciones clasificadas por plazos sugeridos	LP/AI		RAI	
		12.2 Costo/beneficio del plan	LP/AI		RAI	

(continúa)

(continúa)

Tabla 11.1 Proceso metodológico de la auditoría en informática: un enfoque práctico (continuación)

Etapa	Tareas		Productos		Responsable	Involucrados
13.	Aprobar informe y plan de implantación	13.1	Informe de auditoría en informática y plan aprobados		AD/RI/PU	RAI/LP
		14.1	Informe final y plan presentados a la dirección		RAI	AD/RI/LP
14.	Presentación del informe de auditoría en informática y del plan de implantación	14.2	Informe final y plan presentados a personal usuario y de informática		LP/AI	PI/PU
		15.1	Revisión del informe de auditoría en informática		AD/RI/PU	RAI/LP/PI
15.	Aprobar informe final	15.2	Aprobación del informe de auditoría en informática		AD/RI	RAI/LP/PU
		15.3	Compromiso ejecutivo		AD/RI	RAI/PU

Nomenclatura: AD = alta dirección, PU = personal usuario, RI = responsable del área de informática, PI = personal de informática, RAI = responsable del área de auditoría en informática, LP = líder del proyecto de auditoría en informática, AI = auditor de informática.

Es importante señalar que a partir de la primer tarea que corresponde a la presente etapa, el auditor en informática debe conjuntar todo lo recomendado en los capítulos anteriores:

- Profesionalismo
- Ética personal
- Virtudes y habilidades personales
- Metodología de trabajo
- Técnicas
- Herramientas de productividad:
 - Microcomputadoras portátiles, procesadores de palabras, graficadores, bases de datos, software de auditoría, entre otros
- Experiencia profesional
- Otras propias de cualquier auditor en informática

La asimilación y puesta en práctica de los aspectos anteriores tiene los siguientes objetivos en los proyectos:

- Proyectar seguridad y confianza en todos los involucrados del proyecto
- Verificar y dar seguimiento a las funciones de cada involucrado
- Detectar las áreas de oportunidad no visualizadas con anterioridad
- Verificar debilidades e inexistencias relativas al control y seguridad
- Impulsar la motivación y cumplimiento de políticas y procedimientos relativos al control y seguridad en informática de manera permanente
- Otros originados por el desarrollo profesional de la auditoría en informática

Las actividades más importantes del auditor en informática en la etapa de desarrollo son las siguientes:

- Ejecutar las tareas de acuerdo con la secuencia establecida en el plan detallado de auditoría en informática (tabla 9.4)
- Respetar el proceso metodológico (Cap. 6)
- Coordinar los recursos humanos con eficiencia para el cumplimiento oportuno del proyecto
- Impulsar el apoyo permanente de la alta dirección
- Motivar a todos los involucrados en el proyecto
- Orientar los recursos humanos, tecnológicos y financieros hacia resultados que brinden soluciones factibles y de valor agregado
- Otros considerados por el líder del proyecto conforme las características del negocio y la función de informática
- Documentar los datos relevantes de cada entrevista, visita o cuestionario relativos a debilidades o falta de políticas y procedimientos de control y seguridad inherentes a cada área de revisión y sus componentes (Fig. 11.1)

Empresa/departamento:	Observación	Recomendación	Solución				Función responsable de la solución
			AI	CP	MP	LP	
Área de revisión:							
Componentes del área de revisión:							
•							
•							
•							
•							
Técnicas de auditoría utilizadas en esta área:							
•							
•							
•							
•							
•							
•							
•							
Persona entrevistada:							
Puesto:							
Fecha de la auditoría:							
Auditor:							
Comentarios:							
			AI = acción inmediata MP = mediano plazo CP = corto plazo LP = largo plazo				

Figura 11.1 Resumen de observaciones y recomendaciones de la auditoría en informática

- Elaborar informes de alta calidad con la documentación requerida
- Otros que crea pertinentes la función de auditoría en informática de acuerdo con el negocio y las características propias de informática

Nota: Cada una de las tareas de la etapa de desarrollo se explica de manera uniforme para hacerla más práctica e inteligible; se mencionan las actividades más importantes del auditor en informática y los productos terminados mínimos que se deben obtener al finalizar cada una de ellas (tabla 11.2).

Resumen

Una vez hecho el diagnóstico de donde se desprenden los riesgos y debilidades más importantes de los diferentes componentes relacionados con informática y elaborados y aprobados la matriz de riesgos y el plan de auditoría en informática, se realiza la auditoría en informática de cada área.

Es importante recordar que las etapas previas fueron de recopilación, análisis y diagnóstico de todas las áreas de informática de la empresa. En la etapa de desarrollo el auditor en informática revisa las áreas mencionadas en la matriz de riesgos y aprobadas en el plan de auditoría en informática.

Después de superar la parte metódica y conceptual del proyecto, hay que poner en práctica la auditoría en informática de acuerdo con estándares, normas y procedimientos recomendados por asociaciones profesionales (por ejemplo, el Instituto Mexicano de Contadores Públicos, la Asociación Mexicana de Auditoría en Informática, A.C. [AMAI], etcétera).

Asimismo, al llevar a cabo la auditoría en informática los responsables de la misma deberán considerar y respetar los principios y estándares de informática comúnmente aceptados para especialidades como desarrollo de sistemas, planeación de informática, comunicaciones, entre otras.

En esta fase, la aplicación de los conocimientos y experiencia de los auditores da resultados que salvaguardan la integridad y rentabilidad de la información y de otros recursos de informática de la empresa.

También se espera que al revisar la función de informática el auditor se vuelva un asesor de negocios y cambie la resistencia hacia el proceso de revisión en trabajo de equipo; es el momento de ser visto como un asesor que conoce el negocio y la tecnología, no como un verdugo o policía de la organización.

Se debe demostrar que la revisión de los componentes de informática es una necesidad permanente para preservar la congruencia y confiabilidad de la información que fluye a lo largo y ancho del negocio.

El auditor ha de ejecutar su trabajo con profesionalismo, sensibilidad y entusiasmo durante la revisión de las áreas seleccionadas. En esta etapa se ejecuta la práctica de la auditoría en informática.

Tabla 11.2 Productos terminados mínimos

Tarea	Actividades principales	Productos terminados
<p>Concertar fechas tanto de entrevistas y visitas como de aplicación de cuestionarios</p> <p>Nota: las visitas se hacen con el objetivo de validar el uso de políticas y procedimientos de seguridad y control como el registro de acceso a centros de cómputo y áreas donde existe documentación o tecnología importante para el negocio; existencia de extinguidores, detectores de humo, etc.; respaldos de información en cintotecas, equipos en buen estado, avisos de seguridad, etcétera</p>	<ul style="list-style-type: none"> • Solicitar al responsable de informática una lista con todos los nombres, puestos y departamentos del personal de informática y de las áreas usuarias involucradas en el proyecto • Hablar personal o telefónicamente con los involucrados para concertar citas 	<ul style="list-style-type: none"> • Lista del personal de informática y de usuarios • Fecha y hora formal de cada entrevista
Verificar tareas, involucrados y productos terminados	<ul style="list-style-type: none"> • Verificar si la tarea anterior alteró el orden de las tareas mencionadas en el plan detallado • Asegurar que los cambios sean mínimos y de bajo impacto en el plan • Documentar los cambios necesarios y justificados 	<ul style="list-style-type: none"> • Cambios justificados • Cambios documentados
Clasificar técnicas, herramientas, cuestionarios, entrevistas y otros	<ul style="list-style-type: none"> • Verificar la lista de métodos, técnicas y herramientas sugeridas por área que será auditada (véase Cap. 13) • Verificar cuestionarios sugeridos (Cap. 13) a fin de asegurar que sean los requeridos para cada área que se auditará • Actualizar cuestionarios, de ser necesario • Documentar los cambios • Elaborar entrevistas con base en la experiencia, cuestionarios y necesidades del proyecto • Clasificar y documentar según el proyecto 	<ul style="list-style-type: none"> • Lista de métodos, técnicas y herramientas clasificadas por área de revisión • Cuestionarios actualizados y documentados de cada área • Entrevistas documentadas al personal de informática y usuarios

(continúa)

Tabla 11.2 Productos terminados mínimos (continuación)

Tarea	Actividades principales	Productos terminados
Aplicación de entrevistas y cuestionarios	<ul style="list-style-type: none"> • Efectuar cada una de las entrevistas en las fechas y horas planeadas • Aplicar cada uno de los cuestionarios en las fechas planeadas • Documentar las entrevistas y cuestionarios • Obtener el apoyo requerido (reportes, copias, documentos fuente, entre otros) • Registrar entrevistas y cuestionarios pendientes 	<ul style="list-style-type: none"> • Entrevistas aplicadas y documentadas • Cuestionarios aplicados y documentados • Cancelaciones y causas documentadas • Documentación de comentarios de apoyo relevantes para el proyecto
Efectuar visitas de verificación	<ul style="list-style-type: none"> • Validar objetivos e información buscada en cada visita (véase Cap. 13) • Efectuar las visitas a centros de cómputo o a los departamentos usuarios o de informática • Notificar la visita a los responsables de dichos departamentos • Registrar la información más relevante y obtener el soporte requerido (bitácoras por ejemplo) • Registrar pendientes 	<ul style="list-style-type: none"> • Visitas de revisión y verificación efectuadas • Documentación de los datos relevantes relacionados con debilidades o falta de control y seguridad • Registro de causas de visitas canceladas • Fechas de visitas pendientes aprobadas por los usuarios y personal de informática responsables de los lugares por visitar
Elaborar informe preliminar	<ul style="list-style-type: none"> • Analizar la información documentada que se originó de las entrevistas, visitas y aplicación de cuestionarios • Elaborar observaciones y conclusiones de cada uno de los componentes y áreas auditadas • Llenar la hoja de resumen de observaciones y recomendaciones de la auditoría en informática (Fig. 11.1) 	<ul style="list-style-type: none"> • Hojas de resumen de observaciones y recomendaciones de la auditoría (Fig. 11.1) • Observaciones, conclusiones y recomendaciones por: <ul style="list-style-type: none"> – Componente – Área

(continúa)



Tabla 11.2 Productos terminados mínimos (continuación)

Tarea	Actividades principales	Productos terminados
Revisión del informe preliminar	<ul style="list-style-type: none"> • Verificar cada una de las observaciones y recomendaciones por componente y área con el líder del proyecto • Registrar sugerencias para el mejor planteamiento de observaciones y recomendaciones • Asegurarse de tener por escrito todo el soporte requerido para hacer válida cada una de las observaciones (copias de reportes, bitácoras, documentos fuente, minutas, memorandos...) • Concertar citas con el responsable de informática y de los usuarios para dar un avance del proyecto y sus principales conclusiones y recomendaciones 	<ul style="list-style-type: none"> • Observaciones, conclusiones y recomendaciones verificadas y depuradas • Reunión informal de notificación de avance del proyecto con el responsable de informática y el responsable de los usuarios • Compromiso de terminación de pendientes por medio de entrevistas, visitas o aplicación de cuestionarios
Clasificación y documentación del informe preliminar	<ul style="list-style-type: none"> • Registrar de manera formal cada observación, conclusión y recomendación sugerida, revisada y aprobada • Clasificar la información por componente y área auditada 	<ul style="list-style-type: none"> • Observaciones, conclusiones y recomendaciones clasificadas y documentadas por: <ul style="list-style-type: none"> - Componente - Área
Finalizar tareas o productos pendientes	<ul style="list-style-type: none"> • Verificar lista de entrevistas, visitas y cuestionarios pendientes • Finalizar cada pendiente • Analizar la información emanada de cada entrevista, visita y cuestionario terminados • Elaborar observaciones y recomendaciones correspondientes • Actualizar, documentar y clasificar el informe de la auditoría en informática 	<ul style="list-style-type: none"> • Entrevistas, visitas y cuestionarios terminados • Observaciones y recomendaciones clasificadas y documentadas en el informe de auditoría en informática por: <ul style="list-style-type: none"> - Componente - Área

(continúa)

Tabla 11.2 Productos terminados mínimos (continuación)

Tarea	Actividades principales	Productos terminados
Elaborar el informe final de la auditoría en informática	<ul style="list-style-type: none"> • Elaborar un informe orientado a la alta dirección • Redactar un informe detallado para el responsable de informática y los usuarios clave • Verificar que el informe contenga al menos: antecedentes, observaciones, conclusiones, recomendaciones, responsables y tiempos por área auditada 	<ul style="list-style-type: none"> • Informe para la alta dirección • Informe detallado para: <ul style="list-style-type: none"> – Responsable de informática y usuarios clave
Presentación a la alta dirección e involucrados clave	<ul style="list-style-type: none"> • Verificar que los informes sean claros, completos y congruentes entre sí • Comprobar que se tenga el soporte de lo mencionado en los informes • Formalizar fecha de la presentación de informes • Presentar los informes de la alta dirección • Elaborar una minuta 	<ul style="list-style-type: none"> • Informes verificados • Informes finales • Informes presentados a la alta dirección e involucrados clave del proyecto (responsable de informática y responsable de los usuarios) • Minuta de la reunión
Aprobación del proyecto y compromiso ejecutivo	<ul style="list-style-type: none"> • Obtener la aprobación formal (documento) de la terminación del proyecto de la auditoría en informática • Obtener el compromiso formal (documento) de la alta dirección para la implantación de los cursos de acción recomendados por la auditoría en informática en los dos informes • Delegar en informática y las áreas usuarias la implantación de las acciones recomendadas 	<ul style="list-style-type: none"> • Aprobación formal de la alta dirección de la terminación del proyecto de la auditoría en informática • Compromiso ejecutivo para brindar el apoyo requerido en la etapa de implantación de todas las recomendaciones contempladas en los informes • Compromiso del responsable de informática y de las áreas usuarias para ejecutar la etapa de implantación

A fin de tener un producto final de calidad y beneficios tangibles para el negocio al final de la etapa de desarrollo, al momento de revisar las áreas requeridas el auditor en informática deberá realizar las siguientes acciones:

- Basarse en el plan de auditoría en informática elaborado y aprobado en las etapas anteriores para la secuencia y duración de su trabajo en la presente etapa
- No interrumpir la continuidad de las operaciones de la empresa
- Utilizar técnicas y herramientas según lo demande cada tarea de la etapa actual
- Apoyar su trabajo con políticas y estándares comúnmente aceptados
- Involucrar a los usuarios y personal de informática según lo amerite cada tarea
- Usar los cuestionarios para cada área auditada (consúltase apéndice B)
- Hacer entrevistas de manera profesional y adecuarlas al perfil de cada entrevistado
- Cuando se visiten los centros de cómputo y áreas de trabajo de los usuarios, se debe ser respetuoso de las políticas que imperan en ese medio
- Analizar con objetividad los escenarios emanados de la aplicación de cuestionarios, entrevistas y visitas realizados

Elaborar informes preliminares con la siguiente información:

- Áreas de oportunidad para mejorar de inmediato procesos de negocio apoyados en informática
- Observaciones (debilidades, carencias) de los aspectos de informática auditados
- Recomendaciones preliminares para cada una de las observaciones encontradas
- Responsables
- Actualización del plan de auditoría en informática
- Revisión detallada de los aspectos que tengan un impacto considerable en la operación del negocio o que soporten alguna estrategia del negocio
- Comunicación abierta con los usuarios y el personal de informática involucrados
- Presentar un plan de implantación de auditoría en informática factible y realista que contemple los siguientes elementos:
 - Debilidades o carencias de control, su problemática y causas que la originan
 - Acciones inmediatas de corto y mediano plazo
 - Responsables e involucrados en la implantación de estándares, políticas y procedimientos en cada componente de informática que así lo requiera
 - Costo/beneficio del proyecto de implantación
 - Aprobación formal de los directivos usuarios y del responsable de informática

Durante la etapa de desarrollo el auditor revisará áreas típicas de informática en algunos casos y en otros tendrá que enfrentarse a componentes más complejos y nuevos en el negocio; sin embargo, el seguimiento de la metodología, el uso de buenas

5.1 Proceso de planeación del negocio

Este proceso consiste en determinar las estrategias y cursos de acción del negocio; se establece mediante entrevistas y análisis detallados de cada proceso básico de la organización como:

- a) Producción, ventas, recursos humanos o administración en una empresa de manufactura
- b) Recursos humanos, administración, ventas y compras en una empresa dedicada a la comercialización de productos ya manufacturados
- c) Inversiones, ahorros y recursos humanos en una empresa bancaria
- d) Secretaría académica, posgrado, control escolar y recursos humanos en una institución educativa
- e) Auditoría, finanzas, administración, informática y recursos humanos en una empresa de auditoría y consultoría de negocios
- f) Otras áreas de empresas con giros bien definidos

Cualquier entidad privada o de gobierno de diferentes tamaños y estructuras organizacionales debe formalizar el plan del negocio, ya que aquí se define el rumbo del mismo.

Los proyectos que se deriven de este proceso contemplan, a manera general, las siguientes características:

- Es un proceso que involucra todas las áreas del negocio
- Se evalúa el medio externo en sus diferentes entornos
- Se apoya en asesores externos o especialistas del negocio
- Detecta fortalezas, debilidades y áreas de oportunidad del negocio (financieras, recursos humanos, tecnología, mercadotecnia, etc.)
- Establece las amenazas que representa la competencia
- Determina estrategias y metas del negocio
- Los proyectos se contemplan a corto, mediano y largo plazo
- Es aprobado por los accionistas o dueños del negocio
- Etcétera

El periodo de elaboración o actualización del plan del negocio depende de las estrategias y formalidad que tenga este proceso en cada organización. Se recomienda que al ser aprobado de manera formal por los accionistas, se ejecute con eficiencia y se actualice al menos cada año (esta actualización debe ser acorde a las estrategias y metas del negocio y autorizada por la alta dirección). Para un entendimiento de las tareas primordiales del proceso de planeación del negocio y quiénes son los responsables de su ejecución y seguimiento, consúltase la tabla 5.1.

Tabla 5.1 Tareas básicas del proceso de planeación del negocio y responsabilidades

Actividad	Responsable de ejecución	Responsable del seguimiento	Comentarios
Determinación de las áreas de oportunidad para el negocio	Gerente o coordinador de planeación	Alta dirección o director de planeación	Se determinan tendencias y amenazas del medio externo, fortalezas y debilidades del negocio, etc. Se seleccionan las áreas de oportunidad estratégicas y los proyectos de cada proceso básico del negocio
Elaboración del plan del negocio	Gerente o coordinador de planeación	Alta dirección o director de planeación	Cada proyecto debe justificar su inversión, garantizando que brinda al negocio rentabilidad y ventaja competitiva
Presentación del plan a los accionistas o director general o ambos	Director o gerente de planeación	Accionistas o alta dirección del negocio	Se recomienda que se haga de manera oportuna (al iniciar el periodo fiscal, por ejemplo) y que se autorice formalmente
Ejecución del plan de negocio	Gerente o coordinadores de cada área o proceso básico del negocio	Alta dirección o gerente de planeación	Cada área o proceso básico del negocio ha de ejecutar los proyectos, con ayuda de asesores externos si se justifica. Planeación verificará su cumplimiento

5.2 Proceso de planeación en informática

Consiste en definir el conjunto de proyectos relacionados con la función de informática en tiempos a corto, mediano y largo plazo. Cada proyecto debe estar orientado a objetivos y estrategias específicos del negocio (los cuales fueron definidos en el plan del negocio).

El periodo de elaboración o actualización del plan de informática depende de las estrategias y formalidad que tenga dicho proceso en cada organización. Ahora bien, se recomienda que al ser aprobado por la alta dirección se ejecute oportuna y formalmente, con una actualización anual como mínimo (ésta será acorde a las estrategias y metas del negocio y será autorizada también por la alta dirección). Para un entendimiento de las tareas básicas de un proceso de planeación en informática, consúltese la tabla 5.2.

5.3 Proceso de planeación de la auditoría

En esencia consiste en definir un conjunto de proyectos de evaluación y verificación de políticas, controles y procedimientos inherentes a las áreas administrativas,

Tabla 5.2 Tareas básicas del proceso de planeación en informática y responsabilidades

Actividad	Responsable de ejecución	Responsable del seguimiento	Comentarios
Determinación de áreas apoyadas por informática (plan del negocio)	Coordinador o supervisor de planeación de informática	Director o gerente de informática	Las áreas de oportunidad relativas al negocio, al igual que proyectos específicos solicitados por la alta dirección o recomendados por asesores externos de alto nivel, emanan del plan del negocio
Elaboración del plan de informática	Coordinador o supervisor de planeación de informática	Director o gerente de informática	Es importante que la función responsable de ejecutar cada proyecto se involucre en esta tarea; por ejemplo, el área de desarrollo o el área de telecomunicaciones
Presentación del plan a la alta dirección	Director o gerente de informática	Alta dirección del negocio	Antes de presentar el documento se verifica que existe un análisis costo/beneficio de cada proyecto, así como fechas de terminación
Ejecución del plan de auditoría	Funciones de informática: <i>Desarrollo, investigación, comunicaciones, soporte a usuarios, entre otros</i>	Gerente o supervisores	En algunas empresas las funciones de desarrollo de sistemas, soporte a usuarios, planeación, etc., han sido delegadas a personal externo y en ciertas ocasiones han pasado a ser responsabilidad del mismo usuario

financieras, operativas, etc., del negocio, con objeto de asegurar el buen manejo y administración de los recursos de la organización (véase sección de Conceptos).

En los negocios, diferentes responsables suelen implantar los proyectos emanados del plan de auditoría y en diferentes plazos, de acuerdo con los requerimientos y características del negocio (tabla 5.3).

Es importante considerar que los negocios deben tener un conjunto de políticas emanadas de la alta dirección que manifiesten la necesidad de contar con una función externa o interna del negocio que asegure la congruencia de todos los estados financieros y contables con las operaciones y transacciones que se realizan en la empresa; por ejemplo, las transacciones relacionadas con las ventas, compras y la contabilización de las mismas.

Esta función ha de ser un área de control y aseguramiento, es decir, una entidad en el negocio independiente y profesional, capacitada para ejercer las tareas de evaluación y seguimiento sobre todas las actividades u operaciones que afecten de manera directa o indirecta los estados financieros, contables y administrativos.



Tabla 5.3 Tareas básicas del proceso de planeación de auditoría y responsabilidades

Actividad	Responsable de la ejecución	Responsable del seguimiento	Comentarios
Determinación de las áreas por auditar en el negocio	Coordinador o supervisor de auditoría	Director o gerente de auditoría	Aquí se da prioridad a la evaluación de los sistemas de información financieros y contables. El auditor debe verificar si requiere el apoyo del personal de auditoría informática. (externo o interno)
Elaboración del plan de auditoría	Coordinador o supervisor de auditoría	Director o gerente de auditoría	Las fechas y periodos en que se auditarán las áreas pueden obedecer a estrategias propias de la alta dirección o a necesidades de la función de auditoría
Presentación del plan a la alta dirección	Director o gerente de auditoría	Alta dirección del negocio	Se recomienda que se haga de manera oportuna (al iniciar el periodo fiscal por ejemplo) y que se autorice formalmente
Ejecución del plan de auditoría	Supervisor o auditores (externos o internos)	Gerente o supervisores	Algunas empresas consideran que es recomendable utilizar personal de auditoría externo para dar independencia al informe o aligerar las cargas de trabajo

La función de auditoría se responsabiliza tanto de la planeación y ejecución de cada proyecto al cumplimiento formal y oportuno de las políticas, controles y procedimientos establecidos por la alta dirección, así como del seguimiento permanente de los mismos.

El periodo de elaboración o actualización del plan de auditoría depende de las prioridades o necesidades externas (por ejemplo gubernamentales) que tenga dicho proceso en cada organización.

Como se ha expresado antes, se recomienda la ejecución oportuna y formal del plan, luego de que la dirección lo ha aprobado. Asimismo, resulta conveniente actualizarlo al menos dos veces al año, según las estrategias y metas del negocio.

Para entender las tareas fundamentales del proceso de planeación de auditoría, véase la tabla 5.3.

5.4 Proceso de planeación de la auditoría en informática

Consta de la definición y formalización de proyectos. Abarca 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 en informática

a la alta dirección, y que estarán orientados primordialmente al aseguramiento de la calidad y control de los diferentes elementos que se encuentran relacionados de manera directa o indirecta con los recursos de informática.

Para un entendimiento de las importantes tareas de un proceso de planeación de auditoría en informática, consúltese la tabla 5.4.

Proceso detallado de la planeación de auditoría en informática

Es importante aclarar que este proceso de planeación depende en gran medida del diagnóstico previo que haga el auditor en informática de la situación que prevalece en cada una de las áreas o servicios de la función de informática. También se deben considerar las necesidades o prioridades que tenga la alta dirección de auditar o evaluar un área específica de informática.

Tabla 5.4 Tareas básicas del proceso de planeación de auditoría en informática y responsabilidades

Actividad	Responsable de Ejecución	Responsable del seguimiento	Comentarios
Determinación de las áreas por auditar en el negocio	Coordinador o supervisor de auditoría en informática	Director o gerente de auditoría en informática	Se efectúa 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 (véase matriz de riesgos)
Elaboración del plan de auditoría en informática	Coordinador o supervisor de auditoría en informática	Director o gerente de auditoría en informática	Las fechas y periodos en que se auditarán las áreas puede obedecer a la solicitud expresa de la alta dirección o a requerimientos de la función de auditoría en informática
Presentación del plan a la alta dirección	Director o gerente de auditoría en informática	Alta dirección del negocio	Se recomienda que se haga de manera oportuna (al iniciar el periodo fiscal por ejemplo) y que se autorice formalmente
Ejecución del plan de auditoría en informática	Supervisor o auditores de informática (externos o internos)	Gerente o supervisores de la función de auditoría en informática	Algunas empresas consideran que es recomendable utilizar personal de auditoría externo para dar independencia al informe o aligerar las cargas de trabajo

Nota: En los capítulos 6 a 12 se explicará en forma detallada la metodología de auditoría en informática.

El diagnóstico de la situación de informática previo a la planeación de ésta deberá ser breve y muy objetivo; de ninguna manera debe descuidarse el objetivo principal de esta tarea, que es determinar las áreas de mayor riesgo de la función de informática con base en criterios económicos, grado de satisfacción de la alta dirección, seguridad, calidad, productividad, vanguardia tecnológica, etcétera.

Actividades sugeridas para el proceso: elaboración, documentación, autorización y difusión formal del plan de auditoría en informática

Es importante identificar el nivel de riesgo de cada uno de los elementos que integran la función de informática en el negocio a través del diagnóstico de la situación actual en informática (los cuestionarios y formatos sugeridos para su desarrollo se analizan en un capítulo posterior).

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

Algunos de los siguientes servicios se mencionan de manera ilustrativa, esto es, no son limitativos o totalitarios para empresa alguna, ya que será el propio perfil y sus características los que definan 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, asesoría, entre otros)
- Administración de telecomunicaciones
- Investigación y desarrollo tecnológico
- Otros

El auditor deberá utilizar todos los parámetros de medición y evaluación posibles, sin caer en un análisis detallado, para detectar la problemática principal de cada área.

Si este proceso mostrara anomalías de considerable importancia en alguno de los elementos evaluados, se tomarán acciones inmediatas orientadas a minimizarlas o eliminarlas.

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 asegurar que se desarrolle de acuerdo con los estándares, políticas y procedimientos específicos que le han sido asignados según su función.

Consideraciones que se deben tomar en cuenta al diagnosticar la situación actual para la obtención de la matriz de riesgos: el auditor en informática ha de conocer de manera aceptable los aspectos relativos a auditoría e informática que deben tener cada

una de las áreas de informática. Lo anterior es un requisito indispensable, ya que tendrá que basarse en su experiencia y dominio de la auditoría en informática para efectuar un diagnóstico objetivo y contundente; además, se apoyará en la visión de los principales usuarios del negocio y del responsable de informática.

Diagnóstico de la situación actual de los sistemas de información en operación

Dado que los sistemas de información en operación son un elemento primordial dentro del funcionamiento formal de cualquier negocio (aquí se manejan los datos de las áreas financieras, productivas y administrativas para la toma de decisiones), conviene recalcar las consideraciones y criterios más importantes que ha de tomar en cuenta el auditor en informática (se hace referencia más detallada de las demás áreas en los siguientes capítulos).

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

- a) Se obtiene una lista de los principales sistemas de información y de los usuarios principales de cada uno (se establece cuáles fueron desarrollados por la empresa y cuáles comprados a terceros, para saber cuál será la fuente principal de estudio si alguno requiriese mayor evaluación).
- b) Se toman como base los comentarios positivos o negativos de los principales usuarios de cada sistema de información que se encuentre en operación a fin de establecer los volúmenes de transacciones promedio.
- c) Se registran las fallas o regularidades más comunes del sistema o equipo de cómputo, así como las prioridades de operación.
- d) Se recaban los informes de desempeño hechos con anterioridad a los usuarios principales, a los analistas de sistemas y al personal de producción (oportunidad, calidad, confiabilidad).
- e) Se anota la fecha de liberación de los sistemas y la última vez que se auditaron. Esto permite valorar la posibilidad y grado de riesgo.
- f) Se revisa la configuración del equipo donde se encuentre instalado (en una microcomputadora aislada, en una red local, en una minicomputadora, etcétera).
- g) Se estudia su integración a otros sistemas de información.
- h) Se valoran otros de interés propio del auditor en informática para la empresa que evalúe en ese momento.

Debilidades que pueden motivar la auditoría de 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 mismo.

Segundo: que el sistema nunca haya sido auditado. Esto sugiere la alternativa de auditarlo de inmediato, sobre todo si es un sistema básico para la 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 fundamental, se programa su revisión en los proyectos intermedios o finales de la auditoría.

Clasificación del nivel de riesgo que representa el uso de hardware y software en la organización

Lo que se desea determinar en este punto es que los sistemas de información computarizados y los datos sean procesados en un ambiente tecnológico confiable, seguro y eficiente. Aquí se pueden auditar los equipos o paquetes de software que dan soporte a los sistemas primordiales del negocio; o bien se audita de manera periódica el mantenimiento y uso que se hace de la tecnología dentro del equipo y software (herramientas de productividad) en la organización.

La capacidad de los equipos, cantidad de unidades (discos, cintas, terminales, etc.), los tipos (microcomputadoras, redes, minicomputadoras, *mainframes*), distribución física y 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 del mismo, así como la estandarización de paquetes, apoyan al auditor en la programación de los proyectos de auditoría.

Evaluación del nivel de riesgo que representa el uso inadecuado de los productos y servicios por el personal de informática y usuarios dentro de la organización

Esto se refiere básicamente al grado de conocimientos que se tiene sobre el uso de los servicios, software y equipos.

La información que puede ser de apoyo en este punto para el auditor son los organigramas, la descripción de puestos, procedimientos y políticas que se relacionen con los productos y servicios de informática (si no existen, es probable que se estén utilizando de manera limitada las bondades de la informática; asimismo, el conocimiento de los sistemas y equipos puede no ser el más adecuado, lo que motiva al auditor a profundizar posteriormente en este punto. La presencia de catálogos de productos y servicios (hardware, software, proveedores, precios, tipos de asesorías y sus costos por hora), manuales para usuarios, manuales de sistemas, manuales de operación y la distribución y uso de los mismos, así como bitácoras de cursos de capacitación, es de gran relevancia para establecer el grado de confianza que existe por parte del personal involucrado en el manejo de los sistemas, paquetes de software y equipo.

Otros aspectos: telecomunicaciones, EDI (intercambio electrónico de datos), automatización de procesos, CASE

Estos se deben evaluar con base en estándares comúnmente aceptados a nivel internacional y según la proyección de uso que piensa darle el negocio a corto, mediano y largo plazo. Además, hay que considerar los comentarios o asesorías de personal especializado en esta área, ya sea gente externa o de la función de informática de la empresa en evaluación.

Clasificación de los riesgos según criterios establecidos por la función de auditoría en informática

- Cumplimiento de estándares comúnmente aceptados a nivel nacional e internacional
- Cumplimiento formal de políticas y procedimientos
- Grado de satisfacción de la alta dirección y del personal usuario
- Prioridades de la alta dirección
- Prioridades de la función de informática
- Prioridades de la función de auditoría en informática
- Otros de interés específico del auditor en informática en el momento de llevar a cabo la evaluación

Elaboración de una matriz de riesgos que muestre las áreas de la función de informática susceptibles de una revisión por parte de auditoría en el siguiente periodo

Dicha matriz muestra resultados en orden descendente. Esto implica que el área con el valor más alto es la entidad con mayor riesgo; por lo tanto, será la primera auditada y así sucesivamente, hasta conocer las áreas de menor riesgo.

Elaboración de un plan consolidado de proyectos

Este plan ha de contar al menos con 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, entre otros)

Revisión de la matriz de riesgos y el pronóstico de proyectos de auditoría en informática con la gerencia o dirección a la que reporta directamente la función de auditoría en informática

Se ejecutará de manera oportuna y formal con el fin de que se dé 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.*

El plan se elabora cubriendo al menos los siguientes aspectos:

- Área por auditar
- Prioridad
- Fechas de inicio y término
- Involucrados
- Responsables
- Fechas de revisión formales e informales
- Otros de interés particular del auditor en informática en el momento de efectuar esta tarea

Presentación del plan de proyectos de la función de auditoría en informática a la alta dirección

Lo anterior tiene como finalidad los siguientes propósitos:

- Conocer los proyectos de auditoría en informática antes de que inicie el año fiscal
- Verificar que las áreas que considere fundamentales para el buen funcionamiento del negocio hayan sido contempladas en el plan de auditoría en informática y en la matriz de riesgos para su debida reorganización antes de que sea autorizado
- Que la alta dirección se comprometa de manera permanente a apoyar a los auditores en el desarrollo de cada uno de los proyectos
- Obtener la aprobación formal de la planeación de auditoría en informática por parte de la alta dirección

Realización de cada uno de los proyectos de acuerdo con el plan de auditoría en informática

Este punto entraña la ejecución de actividades de seguimiento y revisión formal de cada proyecto.

Integración y formalización de equipos de trabajo

Los equipos estarán integrados por:

- a) Gerente(s) de las áreas usuarias que se evaluarán

- b) Gerente de la función de informática
- c) Líder del proyecto de la función de auditoría en informática

Aprobación formal de la alta dirección del informe final de la auditoría en informática realizada

Por último, se dará seguimiento oportuno y formal a cada una de las recomendaciones contempladas en dicho informe; se aplicarán políticas y controles estandarizados a nivel internacional, y la implantación de este proceso de planeación de auditoría en informática será permanente.

Para terminar, lo mencionado a lo largo de este capítulo muestra la importancia de la participación de la función de auditoría en informática en los diversos procesos de planeación contemplados con anterioridad. La tabla 5.5 ilustra algunos proyectos que emanan de cada uno de esos planes.

Resumen

Hay que considerar el proceso de planeación en cualquier organización como el pilar de todas las actividades que se ejecuten en ella. La desestimación o informalidad en los planes ha provocado importantes decepciones en todos los que pregonan que planear es una pérdida de tiempo y un recipiente de buenos deseos.

En todas las organizaciones los proyectos al vapor causan retrasos en la entrega de resultados, costos superiores a los estimados al inicio y calidad cuestionable en los entregables.

Un problema común en proyectos de mediano o largo plazo es la alta rotación de los encargados. Al no tener definidos su función, responsabilidad, tiempos ni resultados, este personal es el candidato perfecto para convertirse en culpable cuando aumentan los costos del proyecto, los tiempos de soluciones se alargan o simplemente cuando los usuarios olvidan los requerimientos originales.

La planeación se entiende como un proceso formal donde al menos se encuentran los siguientes elementos:

- Etapas
- Tareas
- Actividades
- Costos/beneficios
- Resultados esperados por actividad, tarea y etapa
- Responsables de cada actividad o tarea
- Involucrados o participantes
- Revisiones formales e informales

Tabla 5.5 Tipo de proyectos con responsables e involucrados sugeridos

Tipo de proyectos	Responsables	Involucrados
Negocio		
Adquirir empresas	Accionistas	Gobierno, asesores
Reducción de costos	Directores	Gerencias, asesores
Internacionalización	Accionistas, directores	Clientes, proveedores, gobierno
Reingeniería	Accionistas, directores	Asesores, gerencias, clientes y proveedores
Informática		
Automatización de oficinas	Informática	Proveedores, áreas usuarias
Red local	Informática	Proveedores, usuarios de la red
Implantar filosofía CASE	Asesores, informática	Proveedores
Desarrollo de sistemas	Informática	Áreas usuarias, asesores
Auditoría		
Financiera	Audidores internos o externos	Áreas de la empresa
Fiscal	Audidores internos o externos	Áreas de la empresa
Operativa	Audidores internos o externos	Áreas de la empresa
Auditoría en informática		
Auditoría a sistemas de información	Audidores en informática internos o auditores externos	Informática, usuarios de los sistemas de información
Auditoría a seguridad	Audidores en informática internos o auditores externos	Informática, áreas usuarias de los recursos de informática
Auditoría al mantenimiento de hardware y software	Audidores en informática internos o auditores externos	Áreas de operación de informática y áreas usuarias

- Técnicas para ejecutar actividades
- Herramientas para realizar cada una de las actividades del proyecto

Se puede sobrevivir trabajando en base a las crisis de la empresa y no de acuerdo con estrategias y objetivos de la dirección; es factible seguir dando resultados temporales de “útese y tírese” en vez de brindar al negocio resultados duraderos y congruentes con sus necesidades; asimismo, es posible trabajar al día. Sin embargo, también es importante planear, estimar y esperar antes de actuar. Hay muchos beneficios de planeación, pero el más importante es poder asegurar — con alto grado de credibilidad — a ejecutivos y empresarios cuánto invertirán y cuánto obtendrán de beneficio por cada proyecto.

No hay que subestimar lo que tantos hombres de negocio prominentes pregonan con el ejemplo: el que planea sabe a dónde va y cuándo llegará; dejemos de depender de la buena suerte.

Se puede dejar el proceso de la auditoría en informática como un proceso informal, pero en cada uno de los proyectos es pronosticable la presencia de problemas o irregularidades imprevistas. Si no se planea el trabajo es lógico pensar que tampoco se planean las anomalías y decepciones que el desarrollo de dicho trabajo acarreará.

No se vive de buenos deseos sino de metas claras, medibles y factibles. El auditor de informática y la función o área que la administre deben considerar la importancia y relevancia que tiene, para su éxito como parte del negocio, contar con un plan formal que contemple los proyectos de auditoría así como los diferentes planes relacionados con la informática.

No hay que perder de vista la relación directa entre el grupo responsable de la función de auditoría en informática y los procesos de planeación del negocio, la auditoría tradicional y la función o área de informática.

Se entiende por planeación del negocio la actividad que contempla el planteamiento, elaboración y formalización de los proyectos de cada área o dirección de una organización encaminados a satisfacer las estrategias y objetivos de los accionistas, dueños o responsables directos del negocio a corto, mediano y largo plazo.

Para fines prácticos, se entiende por planeación de auditoría tradicional todas las actividades de los auditores tradicionales orientadas al planteamiento, elaboración y formalización de proyectos relativos a la revisión y dictamen de los aspectos administrativos, operativos, financieros, etc., de una organización de acuerdo con prioridades y necesidades propias de cada negocio.

Se entiende por planeación de informática el proceso que llevan a cabo los responsables de esa área con el fin de plantear, elaborar y formalizar el conjunto de proyectos de corto, mediano y largo plazo que darán soporte estratégico, táctico y operativo al negocio.



Por último, se define como planeación de auditoría en informática el proceso que consiste en plantear, elaborar y formalizar una serie de proyectos de corto, mediano y largo plazo orientados a la evaluación y revisión oportuna de todos los componentes inherentes a la informática, según prioridades propias de la empresa y con una orientación de apoyo directa a los planes mencionados.

Los requisitos mínimos para que la planeación de auditoría en informática sea formal, permanente y exitosa son:

- a) Involucramiento directo del auditor en informática en el proceso de planeación estratégica del negocio para:
 - Entender requerimientos, tiempos y prioridades de cada proyecto del negocio a fin de poder evaluar, revisar o asesorar a las áreas involucradas
 - b) Compromiso del responsable de auditoría en informática con cada proyecto del plan de informática para implementar un esquema de control y seguridad preventivo y completo.
 - c) Participación del auditor en informática en el proceso de planeación de auditoría tradicional para hacer en controles y medidas correctivas.
- Los beneficios surgidos de la participación entrañan la supresión de:
- Riesgos de no planear la auditoría
 - Responsables de tareas inadecuados
 - Falta de compromiso de los involucrados en el proyecto
 - Aparición de costos imprevistos
 - Retrasos en la obtención de beneficios
 - Mala calidad en los resultados
 - Rotación del personal clave
 - Inadecuada segregación de tareas y actividades
 - No alineación con planes de negocio, auditoría o informática
 - Errores en la disposición de las cargas de trabajo
 - Tensión y falta de motivación en los participantes
 - Uso impropio o no utilización de técnicas y herramientas apropiadas
 - Falta de una estructura sólida para los proyectos (etapas, secuencias, tiempos)

Preguntas clave

1. ¿Qué entiende por planeación?
2. ¿Qué es un plan de negocios?
3. ¿Cuál es la relevancia de que los auditores de informática conozcan dicho plan?
4. ¿Qué es un plan de auditoría tradicional (financiera, administrativa, etcétera)?

5. ¿Cuál es la importancia de que los auditores de informática lo conozcan?
6. ¿Qué es un plan de informática?
7. ¿Qué interés tiene que los auditores de informática lo conozcan?
8. ¿Qué entiende por planeación de auditoría en informática?
9. Si el auditor de informática carece de un plan formal de su función, ¿qué efectos negativos se le podrían presentar?
10. ¿Qué beneficios directos brinda al negocio el hecho de contar con planes formales?
11. ¿Cuáles elementos mínimos componen un proceso formal de planeación?
12. ¿Cuál es la función del auditor de informática en los siguientes tipos de proyectos?
 - a) negocio
 - b) informática
 - c) auditoría tradicional
 - d) auditoría en informática

Metodología para el desarrollo e implantación de la auditoría en informática

La auditoría en 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 en informática efectúa sus tareas y actividades mediante una metodología (véase Fig. 6.1).

No es recomendable fomentar la dependencia en el desempeño de esta importante función sólo con base en la experiencia, habilidades, criterios y conocimientos sin una referencia metodológica. Contar con un método garantiza que las cualidades de cada auditor sean orientadas a trabajar en equipo para la obtención de productos de calidad estandarizados.

La función de auditoría en informática ha de contar también con un desarrollo de actividades basado en un método de trabajo formal, que sea entendido por todos los auditores en informática y complementado con técnicas y herramientas propias de la función.

Lo anterior se facilita si los auditores en 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 áreas 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, funciones y responsabilidades, etc., definidas previamente en un documento formal que contiene la metodología necesaria. Esto tiene el fin de brindar 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 sí sola el éxito de los proyectos de auditoría en informática; además se requiere un buen dominio y uso constante de los siguientes aspectos complementarios:

METODOLOGÍA DE AUDITORÍA EN INFORMÁTICA

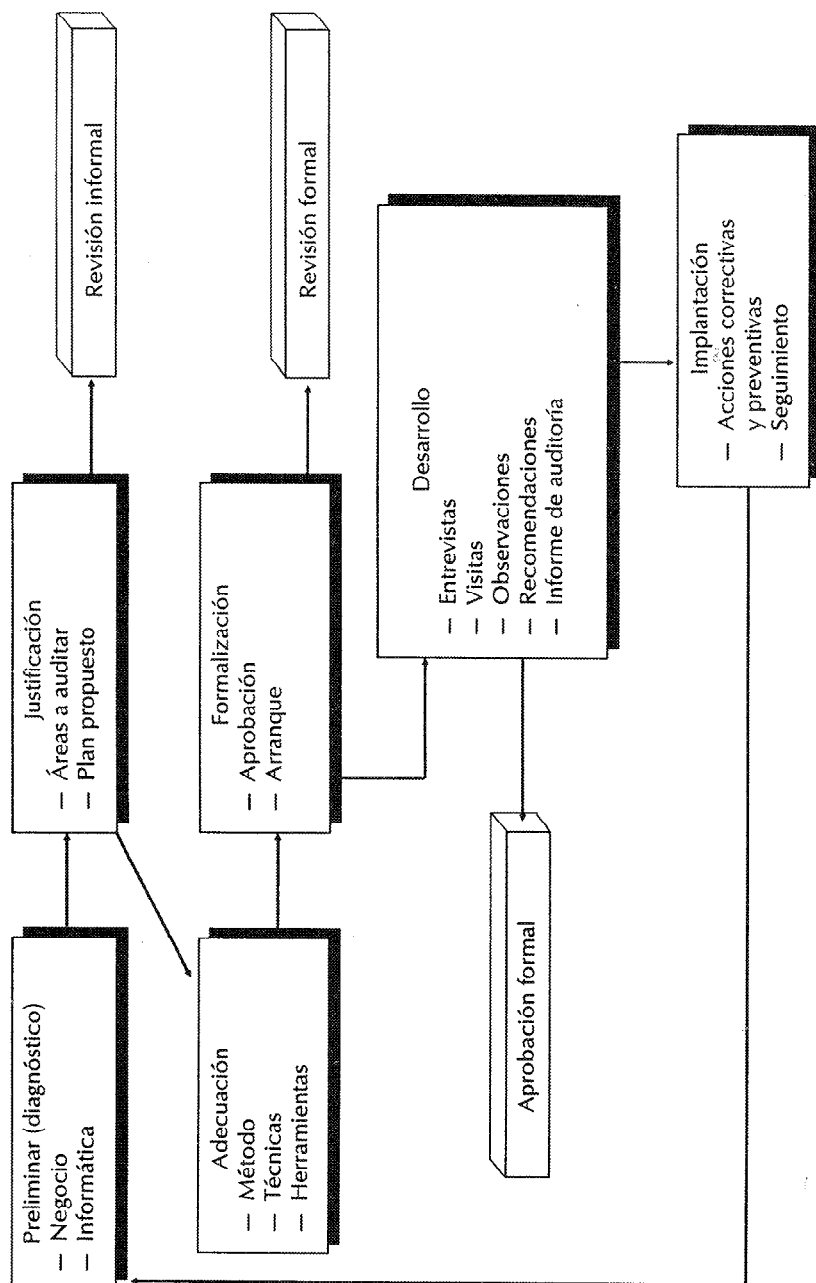


Figura 6.1 Estrategia para implantar un proceso metodológico de auditoría en informática (enfoque práctico)

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

6.1 Proceso metodológico de la auditoría en informática

El uso de un proceso de trabajo metodológico y estándar en la función de auditoría en informática genera 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 en informática
- Se facilita en alto grado la administración y seguimiento de los proyectos, pues la metodología obliga a la planeación detallada de cada proyecto bajo criterios estándares
- Facilita la superación profesional y humana de los individuos, ya que orienta los esfuerzos hacia la especialización, responsabilidad, estructuración y depuración en las funciones del auditor en informática
- Es un complemento clave en el desarrollo de cada individuo, ya que su formal seguimiento, aunado a las habilidades, normas y criterios personales coadyuva al cumplimiento exitoso de los proyectos de auditoría en informática
- El proceso de capacitación o actualización en el uso de un proceso metodológico es más ágil y eficiente, dado que se trabaja sobre tareas y productos terminados perfectamente definidos

Requisitos para el éxito del proceso metodológico

Contar con una metodología formalmente documentada no es garantía de que los proyectos de auditoría en informática tendrán éxito; empero, **no** cumplir con las siguientes condiciones llevará a la función de auditoría en informática a que sus proyectos no cumplan con los tiempos, costos o resultados esperados:

- Aprobación de la metodología por la alta dirección
- Adecuación de la metodología a los requerimientos específicos del negocio (cuidado con reducir tareas y eliminar productos importantes con el fin de ahorrar tiempo o por criterios personales; es útil apoyarse en un asesor experto)
- Documentación o actualización de la metodología
- Capacitación formal en el uso de la metodología (de acuerdo con el perfil y nivel de participación de cada individuo por capacitar)
- Elaboración de los planes de auditoría en informática según la metodología
- Verificación del uso formal de la metodología en cada proyecto
- Capacitación formal para el personal de nuevo ingreso o cuando se hagan actualizaciones relevantes a la metodología
- Otros observados por las mismas empresas en sus proyectos

La tabla 6.1 describe las etapas de la metodología de auditoría en informática, así como los datos generales relacionados con cada una.

Esta visión será de gran utilidad tanto para el auditor en informática como para los demás involucrados en el proyecto.

El responsable de la función de auditoría en informática puede valerse de la información consolidada de la tabla de descripción general de la metodología de auditoría en informática, para dar un seguimiento oportuno y estructurado a cada proyecto, debido a que tareas y productos están terminados (salvo algunas tareas y resultados).

En capítulos posteriores se detalla cada etapa con el fin de que su entendimiento sea más claro y fácil de aplicar en cada proyecto de auditoría en informática.

El proceso metodológico no debe tomarse como un dogma, pues en ningún momento se manifiesta tal intención; al contrario, ha de considerarse como una referencia que trata de orientar al líder de proyecto e involucrados para un mejor desarrollo de cada tarea requerida en la auditoría en informática. Una obligación de toda área dentro de la organización es actualizarse, adecuando procesos y métodos a las características propias del negocio, sin perder las recomendaciones comúnmente aceptadas por los negocios, asociaciones profesionales y demás especialistas.

6.2 Métodos, técnicas y herramientas por área de revisión

Como se ha comentado en capítulos anteriores, el desarrollo exitoso de la auditoría en informática depende de un conjunto de factores interrelacionados. Conjuntar y coordinar de manera eficiente los siguientes factores brindará el aseguramiento de resultados satisfactorios por parte del desempeño de la función de los auditores en informática:

- Dominio de los conceptos técnicos y administrativos relacionados con la auditoría en informática
- Habilidades inherentes a la auditoría en informática

Tabla 6.1 Proceso metodológico general de la auditoría en informática: un enfoque práctico

Etapa	Productos terminados	Requerimientos	Responsable	Involucrados
Preliminar (diagnóstico)	1. Diagnóstico de negocio	<ul style="list-style-type: none"> • Involucramiento de la dirección • Información veraz 	LP	AD/AI RI/RAI
	2. Diagnóstico de informática		LP	
Justificación	1. Matriz de riesgos	<ul style="list-style-type: none"> • Análisis de riesgos y áreas de oportunidad • Definir responsables y tiempos 	LP	RAI/RI
	2. Plan de auditoría en informática		LP	RAI
Adecuación	1. Plan y metodología de acuerdo con el cliente	<ul style="list-style-type: none"> • Entendimiento del negocio y de la función de informática • Detallar tareas y tiempos 	LP	RI/RAI/PU
	2. Plan detallado		AI	RI/RAI/PU
Formalización	1. Plan aprobado	<ul style="list-style-type: none"> • Aprobación formal (firmas) • Respaldo y apoyo al proyecto 	AD	RI/RAI/PU
	2. Compromiso ejecutivo		AD	RI/RAI/PU
Desarrollo	1. Auditar áreas seleccionadas	<ul style="list-style-type: none"> • Aprobación de la dirección • Asignar responsables y tiempos para cada acción recomendada 	LP	RI/PU/AI
	2. Informe de auditoría en informática		AD/PI/PU	RAI/LP/AI
Implantación	1. Recomendaciones y acciones terminadas	<ul style="list-style-type: none"> • Compromiso ejecutivo • Basarse en plan de implantación • Verificar cumplimiento del plan 	RI/PU	LP/AI
	2. Aprobación final		LP/AI	RI/PU/RAI

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor en informática.

- Normas personales
- Entendimiento de la auditoría en informática y sus tendencias
- Adaptación o actualización según el medio dominante
- Organización y administración formal de la auditoría en informática en el negocio
- Involucramiento formal en el proceso de planeación del negocio, informática y de la auditoría tradicional
- Desarrollo de un proceso formal de planeación de auditoría en informática
- Entendimiento y aplicación de un proceso metodológico formal de la auditoría en informática
- Gusto y amor profesional por la carrera de auditoría en informática (es un requisito moral, no una política organizacional)
- Participación formal — en la medida de lo posible — en las asociaciones, institutos educativos, etc., con fines de actualización o de compartir las experiencias profesionales adquiridas en el campo de la auditoría en informática
- Entendimiento satisfactorio de los métodos, técnicas y herramientas necesarios para auditar las áreas seleccionadas en el proceso de planeación de la auditoría en informática
- Otros que dependen de las características de la organización en que se desarrolle la función de auditoría en informática

Uno de los factores primordiales para el auditor en informática en el desempeño eficiente de su trabajo es el conocimiento y aplicación de los métodos, técnicas y herramientas comúnmente aceptados para la informática en los negocios o asociaciones.

En la medida en que el auditor en informática posea experiencia y conocimientos actualizados sobre los diferentes aspectos que evaluará, tendrá resultados pobres o exitosos en la organización donde trabaja.

En la tabla 6.2 se muestra un conjunto de elementos metodológicos, técnicos y operativos recomendados para apoyar la función de auditoría en informática en la revisión y evaluación de áreas específicas de informática y los demás componentes relacionados con ella.

Resumen

El éxito de cualquier proyecto no se basa únicamente en que lo apruebe la alta dirección o en la disponibilidad de recursos destinados para ello. La estructura que plasma el camino que se ha de seguir, las funciones y compromisos de los involucrados, la secuencia y productos obtenidos a lo largo de la trayectoria del proyecto son — en gran medida — otros elementos que garantizan un resultado final satisfactorio.

La aprobación de los proyectos de auditoría en informática sólo garantiza el inicio y compromiso temporal de las personas que se verán involucradas voluntaria o

Tabla 6.2 Grado de importancia de los métodos, técnicas y herramientas en las etapas del proceso metodológico de la auditoría en informática

Concepto	Etapas de preliminar	Etapas de justificación	Etapas de adecuación	Etapas de formalización	Etapas de desarrollo	Etapas de implantación	Etapas de seguimiento
Metodología							
• Planeación de negocios	Básico	Básico	Básico	Básico	Conveniente	Básico	Básico
• Planeación de informática	Básico	Básico	Básico	Básico	Básico	Básico	Básico
• Implantación de sistemas	No requerido	No requerido	Conveniente	No requerido	Básico	Básico	Básico
Técnicas							
• Análisis							
- Organizacional	Básico	Básico	Básico	Básico	Básico	Básico	Básico
- Sistemas	No requerido	Conveniente	Conveniente	Conveniente	Básico	Básico	Básico
- Computacional	No requerido	No requerido	No requerido	No requerido	Básico	Básico	Básico
• Diseño							
- Conceptual	No requerido	Conveniente	Básico	Conveniente	Básico	Básico	Básico
- Computacional	No requerido	No requerido	No requerido	No requerido	Básico	Básico	Básico
• Costo/beneficio	Conveniente	Básico	Básico	Básico	Básico	Básico	Básico
• Modelo de datos y procesos	Conveniente	Básico	Básico	Conveniente	Básico	Básico	Conveniente
• Documentación							
- Ejecutiva	Conveniente	Conveniente	Básico	Básico	Básico	Básico	Básico
- Detallada	No requerido	Conveniente	Conveniente	No requerido	Básico	Básico	Básico
• Entrevistas	Básico	Básico	Básico	Básico	Básico	Conveniente	Básico
• Cuestionarios	Conveniente	Básico	Básico	No requerido	Básico	Conveniente	Conveniente
• Otras técnicas *	*	*	*	*	*	*	*
• Controles, políticas y estándares nacionales e internacionales	No requerido	Conveniente	Conveniente	No requerido	Básico	Conveniente	Básico
• Áreas de especialización	*	*	*	*	*	*	*
- Comunicaciones *	*	*	*	*	*	*	*
- Otros *	*	*	*	*	*	*	*
• Habilidades o virtudes							
- Creatividad	No requerido	Conveniente	Conveniente	Conveniente	Básico	Conveniente	Conveniente
- Abstracción	Básico	Básico	Básico	Básico	Básico	Conveniente	Básico
- Deducción	*	*	*	*	*	*	Básico
- Otros *	*	*	*	*	*	*	*

* Es importante aclarar que esta tabla no busca limitar el buen desarrollo de la auditoría en informática. Se recomienda analizar de manera objetiva la tecnología y tipo de organización para definir la magnitud y el énfasis que debe darse a cada uno de los conceptos señalados.



involuntariamente en dicho proceso. Recuérdese que los prejuicios organizacionales hacia los procesos que impliquen revisiones, evaluaciones o tareas similares podrán perjudicar cada proyecto si no se tiene un plan que minimice y revierta esas actitudes en posiciones proactivas y de apoyo.

Proporcionar recursos económicos, humanos y materiales a los proyectos de auditoría en informática garantiza el abastecimiento de la materia para el proceso, mas no implica que el producto terminado sea de calidad y entregado con oportunidad.

El enfoque principal del presente capítulo es plantear un camino digerible y práctico para que todos los auditores en informática conozcan, desde antes del inicio de los proyectos, todos los componentes y características de logística requeridos para terminarlos exitosamente.

Los principales objetivos de la metodología de auditoría en informática son:

- Definir clara y detalladamente los requerimientos y condiciones que justifiquen cada proyecto
- Las debilidades o carencias de políticas y procedimientos existentes en las áreas relacionadas con informática que generen necesidades de una auditoría
- Responder a una solicitud expresa de la alta dirección para auditar la función de informática en alguno de sus componentes
- Definir etapas o secuencias del proyecto (evaluación preliminar, adecuación, justificación, formalización, desarrollo, implantación)
- Especificar funciones y responsabilidades del personal que participará en los proyectos de auditoría en informática (usuarios, líder y personal o áreas de apoyo al proyecto y auditor en informática)
- Definir técnicas y herramientas mínimas para cada etapa del proyecto de auditoría en informática (muestreos, entrevistas, cuestionarios, inspección/observación, documentación, software de auditoría, análisis de procesos de negocios, análisis de sistemas, lenguajes de programación, paquetes computacionales de oficina, equipo de cómputo)

Entre sus herramientas se pueden enumerar:

- Auditorías periódicas establecidas en la empresa formalmente
- Auditorías emanadas de manera excepcional de factores no considerados en el plan de auditoría en informática desde el inicio
- Actividades de apoyo a la auditoría tradicional en la revisión de sistemas de información, aspectos de seguridad, etcétera

Es necesario remarcar que los elementos que intervienen en cada proyecto que vaya a ejecutar el auditor en informática deberán orientarse desde su inicio a conjuntar tanto aspectos metodológicos (la estructura geográfica, por así decirlo) como los

recursos humanos, económicos y materiales que representan la parte motora del mismo.

Por último, se hará que la dirección de la empresa y todos los involucrados de alto nivel tomen conciencia de que todo lo planteado en cada proyecto de auditoría recibirá la formalidad y apoyo necesarios para su culminación.

Preguntas clave

1. ¿Qué abarca la metodología de una auditoría en informática?
2. Mencione los principales objetivos de la metodología de auditoría en informática.
3. Enumere los beneficios de la metodología de auditoría en informática.
4. ¿Qué aspectos negativos pueden presentarse al auditor en informática si no cuenta con una metodología formal para desarrollar sus proyectos?
5. ¿Qué circunstancias o elementos deben acompañar a la metodología de auditoría en informática en los proyectos para que éstos sean exitosos?
6. ¿Cuáles son las etapas de la metodología de auditoría en informática? Menciónelas en la secuencia correcta.
7. Enumere las técnicas y herramientas mínimas que utiliza el auditor en informática durante el desarrollo de sus proyectos.
8. ¿Qué personal mínimo debe participar durante un proyecto de auditoría en informática? Mencione los nombres genéricos comúnmente aceptados.
9. ¿Podría describir brevemente la responsabilidad de cada uno de los participantes mencionados en su respuesta anterior?

Etapas preliminar o diagnóstico de la situación actual

7.1 Diagnóstico del negocio: alta dirección y áreas usuarias

Es el primer paso práctico del auditor en informática dentro de las empresas o instituciones al efectuar un proyecto de auditoría en informática. Se busca la opinión de la alta dirección para estimar el grado de satisfacción y confianza que tiene en los productos, servicios y recursos de informática del negocio; asimismo, es posible detectar 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 son las áreas de oportunidad que tiene informática para hacer más competitivo y rentable el negocio, sea este soporte directo o indirecto, en alto o menor grado.

Es conveniente aclarar que no se debe tratar esta etapa 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 débiles y fuertes de la función de informática desde un punto de vista de los usuarios clave y la alta dirección.

Tareas, productos terminados, responsables e involucrados

Todas las actividades del auditor en informática deben estar claramente definidas en todos los componentes formales que integran cualquier trabajo dentro de una organización. En la figura 7.1 se presenta toda la información detallada que lo guiará en esta etapa.

Los aspectos por evaluar son al menos los tres mencionados a continuación. Ahora bien, si el auditor considera que la complejidad del negocio, la fusión o compra de la empresa, la informalidad palpable en informática o alguna consideración específica

Etapas	Tareas	Productos	Responsable	Involucrados
Diagnóstico preliminar	1. Diagnóstico de negocio	1.1 Misión y objetivos de negocio	LP/RAI	AD
		1.2 Organización de informática	LP/RAI	AD
		1.3 Grado de apoyo al negocio	LP/RAI	AD/PU
	2. Diagnóstico de informática	2.1 Misión y objetivos de la función de informática	LP/RAI	RI
		2.2 Organización de informática	LP/RAI	RI
		2.3 Control (formalidad)	LP/RAI	RI/PI
		2.4 Productos y servicios	LP/RAI	RI
	3. Detectar área de oportunidad	3.1 Área de oportunidad para mejoras inmediatas	LP/RAI	AD/PU/RI

Nomenclatura: AD = alta dirección; PU = personal usuario; RI = responsable del área de informática; PI = personal de informática; RAI = responsable del área de auditoría en informática; LP = líder del proyecto de auditoría en informática; AI = auditor de informática

Fig. 7.1 El proceso metodológico de la auditoría en informática: un enfoque práctico.

para el líder de proyectos o a petición de la alta dirección requieren más puntos por considerar y un tiempo más prolongado, conviene que los integre en esta fase, ya que aquí se detectan los primeros síntomas de informática que, a la postre, pueden ser los más relevantes.

Nota: Dado que en capítulos anteriores y a lo largo de los restantes se hace referencia al líder de proyecto de manera frecuente, conviene definirlo: es quien se encarga de coordinar y supervisar los proyectos de auditoría en informática; organizacionalmente le reporta al responsable de la función de auditoría en informática y puede tener a su cargo uno o más auditores en informática en los proyectos que estén bajo su responsabilidad.

Conocimiento del negocio

El auditor en informática debe conocer el tipo de organización: la misión, estrategias, planes (de ser posible, o al menos los proyectos globales) y nivel jerárquico de 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 ha de solicitar el auditor en informática para su análisis preliminar y que emanan de este punto son:

- Misión del negocio
- Áreas 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 y proveedores, por ejemplo)
- Organigrama
- Políticas referentes a informática
- Otros de interés para el auditor en informática de acuerdo con las características del proyecto

Apoyo al negocio

El auditor en informática debe obtener una idea global del grado de apoyo y satisfacción que existe en el negocio y al menos estimar hacia dónde se orienta el soporte de la función de informática:

- Apoyo a la alta dirección (por ejemplo: sistemas de información estratégica, tecnología)
- Apoyo a las gerencias (sistemas de información integrales, tecnología, etcétera)
- Apoyo a niveles operativos (sistemas de información básicos, tecnología, entre otros)

Debe conocer de manera general los siguientes aspectos:

- Participación de la función de informática en los proyectos clave del negocio
- Difusión de las políticas y planes de informática en los niveles estratégico, táctico y operativo del negocio
- Imagen de informática ante la alta dirección y los responsables de cada área del negocio
- Grado de satisfacción que existe por cada servicio prestado por la función de informática
- Expectativas que tiene el negocio referentes a informática
- Fortalezas de informática
- Debilidades de informática
- Áreas de oportunidad (propuestas ya sea por la alta dirección, usuarios o informática)
- Otros de interés específico del auditor en informática

Áreas de oportunidad

Aquí se detectan todas las características que facilitarán la implantación de soluciones brindadas por informática y que tendrán un impacto relevante en alguna función o gerencia del negocio; de igual manera, pueden proponerse acciones inmediatas o a corto plazo que redunden en el corto, mediano o largo beneficios directos para la alta dirección. Dichas acciones pueden encaminarse a aprovechar por ejemplo alguna de las siguientes áreas de oportunidad:

- Reubicación de la función de informática en la estructura organizacional
- Capacitación a los niveles ejecutivos o a los usuarios clave de las aplicaciones instaladas
- Actualización tecnológica
- Sistematización de algunas áreas de negocio
- Creación de algún comité de informática
- Formalización y divulgación de políticas y planes de informática en el negocio
- Otras

No hay que confundir la fase preliminar con la fase de desarrollo e implantación; en la primera el estudio es corto en tiempo y general en su investigación. Se menciona aprovechar las áreas de oportunidad que no requieren la terminación de la auditoría en informática para comenzar su implantación. Es conveniente recordar que se carece de mucho soporte documental y detallado en este momento, por lo que la sugerencia de áreas de oportunidad utópicas puede crear cierta incredulidad y rechazo hacia el auditor en informática.

Para concluir sólo resta mencionar que las áreas de oportunidad pueden emanar de la alta dirección, de los usuarios, del responsable de informática o del mismo auditor en informática; sin embargo, todas las propuestas deben ser analizadas y documentadas antes de ponerlas en práctica.

7.2 Diagnóstico de informática: responsables de la función

Aquí el auditor en informática se coordina directamente con el responsable de la función de informática.

Conocimiento de la función de informática

En esta parte el auditor conocerá:

- La estructura interna de informática
- Funciones
- Objetivos
- Estrategias
- Planes
- Políticas

La tecnología de software y hardware es en la que se apoya para llevar a cabo su función dentro del negocio.

Otros de interés específico para él

Se busca también obtener la información relacionada con algunos aspectos indagados entre los usuarios y la alta dirección con objeto de encontrar la congruencia o discrepancia entre una opinión y la otra.

Las entrevistas deben efectuarse con el responsable de informática y ocasionalmente con los encargados directos de las funciones clave de esta área. Es indispensable hacerles entender la importancia que brinda su apoyo a este tipo de proyectos. El auditor en informática debe ser profesional y ético en su trabajo para brindarles la seguridad de que al final todo beneficiará a todos los involucrados (dirección, usuarios e informática).

Lograr un equipo de trabajo unido es un aspecto muy positivo en cualquier proyecto y los de auditoría en informática no son la excepción; se requiere que el líder del proyecto desarrolle una buena comunicación con el personal de informática en la etapa preliminar. Esto es viable si entiende los logros, debilidades y fortalezas tecnológicas, humanas y organizacionales del personal que integra la función de informática.

En caso de que el auditor revise vaga e informalmente la información aquí recomendada u omita su búsqueda, corre el riesgo de planear o sugerir proyectos sin el alcance requerido para asegurar que todas las áreas de oportunidad y aspectos de riesgo sean contemplados o evaluados.

Servicios

Un aspecto clave que se tiene que considerar en la etapa preliminar es la evaluación general de los servicios que presta informática a las diferentes áreas del negocio y en los distintos niveles organizacionales.

El auditor en informática ya puede formarse un juicio inicial de la congruencia entre las áreas usuarias y el responsable de informática; aquí se detecta por lo general qué servicios ya son aceptados en el negocio como estratégicos y cuáles sólo son operativos o necesarios para llevar a cabo tareas que no producen valor agregado.

El responsable de informática no debe ser su propio juez; pero al menos puede brindar su opinión personal de lo que considera que es su grado de apoyo al negocio; asimismo puede manifestar o comprobar el grado de apoyo que brindan sus servicios al negocio mediante minutas, memorandos, reconocimientos, etc., de los usuarios y de la alta dirección.

El objetivo de conocer su opinión al respecto es encontrar la congruencia entre su función y lo que dice la alta dirección que debe ser. No se busca crear controversias ni encontrar fallas personales.

El auditor en informática tiene la responsabilidad moral de dar un sentido crítico y práctico a todas las áreas del negocio para encontrar un mejor modo de hacer las cosas desde el punto de vista profesional en el campo de informática y, de ser posible, en las áreas del negocio involucradas en este tipo de proyectos.

Los servicios que generalmente brinda 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 cómputo
 - Paquetes de software (como procesadores de palabras, hojas de cálculo)

- Equipos de telecomunicaciones
- Lenguajes de programación
- Mantenimiento
 - Sistemas de información
 - Base de datos
 - Equipos de cómputo
 - Equipo de telecomunicaciones
 - Redes locales
- Soporte a usuarios
 - Capacitación
 - Asesoría
- Investigación
 - Tecnología (equipos de cómputo, comunicaciones, CASE, EDI, etcétera)
 - Aplicaciones en el mercado
- Plancación de informática
- Auditoría en informática
- Soporte a la alta dirección
- Otros de acuerdo con el tipo de negocio

Nota: Los servicios pueden ser ejecutados por externos y coordinados por informática. En algunas ocasiones el usuario recibe ciertos servicios de personal externo, los contrata y coordina. El auditor en informática ha de encontrar las causas y el efecto que esto causa en el negocio.

Es muy recomendable que en esta tarea el auditor en informática documente todas las observaciones relevantes expuestas por el responsable de informática en relación con los servicios que proporciona, con la finalidad de cruzarlas con las hechas por la alta dirección y los principales usuarios de la organización.

Aspectos de control

Otra actividad de la etapa preliminar es evaluar el grado de formalidad y cumplimiento que se da a políticas, controles y procedimientos relativos a cada área de informática.

Una manera de obtener dicha información es a través de la entrevista que concede el responsable de informática al líder de proyecto; pero el camino más directo es entrevistar al encargado de cada área que conforma la función de informática, evitando caer en el detalle y ocupar mucho tiempo en las entrevistas.

Algunos aspectos que se deben considerar son los siguientes:

- 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 interés específico del auditor en 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.

Áreas de oportunidad

Aquí se detectan todas las circunstancias que facilitarán la puesta en marcha de soluciones brindadas por informática y que tendrán un impacto relevante en alguna función o gerencia del negocio; de igual manera, cabe proponer acciones inmediatas o a corto plazo que redunden en el corto, mediano o largo beneficios directos para la alta dirección; dichas acciones pueden encaminarse a aprovechar por ejemplo alguna de las siguientes áreas de oportunidad:

- Capacitación o actualización profesional del personal de informática
- Creación y difusión de nuevos servicios de informática al negocio
- Reubicación de la función de informática en la estructura organizacional
- Capacitación a los niveles ejecutivos o a los usuarios clave acerca de las aplicaciones instaladas
- Actualización tecnológica
- Sistematización de algunas áreas de negocio
- Creación de algún comité de informática
- Formalización y divulgación de políticas y planes de informática en el negocio
- Otras

Como se ha mencionado antes el responsable de la función de informática puede detectar y recomendar las áreas de oportunidad. En los proyectos es cuando se aprovechan las oportunidades de ofrecer al negocio posibilidades de mejoramiento que antes no pudieron llevarse a la práctica por diversas causas.

La etapa de justificación (que es la que sigue después de terminar la presente) puede contemplar entre sus tareas la revisión o evaluación de opciones emanadas de las áreas de oportunidad detectadas en el diagnóstico de negocio y de informática.

Otros de interés para el auditor en informática de acuerdo con las características del negocio

El criterio de un auditor en informática puede incrementar o reducir el alcance de la etapa preliminar dependiendo de las características del negocio, así como de las restricciones o facilidades al proyecto en factores críticos (como tiempo, presupuesto o los objetivos buscados por la alta dirección o el responsable de la función de auditoría en informática).

Con base en lo anterior es recomendable acompañar los aspectos complementarios con cuestionarios o preguntas específicas para tal fin.

Cuestionario para el diagnóstico actual (etapa preliminar)

A continuación se proporciona el cuestionario detallado que apoyará al auditor en informática para obtener la información mencionada; esto es, los diagnósticos de negocio y de informática (tablas 7.1 a 7.9).

El cumplimiento total y secuencial del cuestionario es recomendable; sin embargo, el criterio del líder de proyecto y las circunstancias particulares del proyecto pueden variar el grado de uso del mismo; ahora bien, no es conveniente iniciar las etapas posteriores sin haber aplicado la etapa preliminar con los responsables e involucrados correspondientes.

Resumen

Una vez que el auditor define las etapas, tareas, responsables e involucrados, técnicas, herramientas de trabajo y el plan global de los proyectos (a corto, mediano y largo plazo) conforme la metodología planteada en el capítulo anterior, se inicia de manera formal la auditoría en informática en la empresa.

La metodología de la auditoría en informática establece como primer paso ejecutar la etapa preliminar o de diagnóstico de la situación actual.

Para el auditor en informática es muy aventurado iniciar un proceso de revisión de cierto componente de informática sin analizar con anterioridad el entorno del negocio y la función de informática.

Ha de efectuarse un estudio global de la empresa y del área de informática antes de empezar directamente a auditar aspectos relativos de informática como seguridad o sistemas de información en operación.

El diagnóstico inicial del negocio reflejará como grandes puntos al menos lo siguiente:

- Giro de la empresa
- Áreas organizacionales y procesos básicos que componen la empresa

Tabla 7.1 Cuestionario de diagnóstico actual (etapa preliminar), aspectos del negocio

Concepto	Descripción	Comentarios
Giro y misión del negocio (solicitar organigrama)		
Áreas del negocio * * *		
Macroproyectos del negocio * * *		
Objetivos del negocio * *		
Políticas referentes a la función de informática * * *		
Áreas de oportunidad que se derivan de informática * * *		

Tabla 7.2 Soluciones de informática (diagnóstico de negocio)

¿Cuáles de las siguientes soluciones le han sido proporcionadas por informática y cómo las califica?	E = Excelente B = Buena R = Regular D = Deficiente			
	E	B	R	D
• Soluciones de consultoría – Asesoría y soporte en la definición, evaluación y selección de estrategias para la obtención de soluciones de negocio	()	()	()	()
• Soluciones de sistematización de procesos de negocio – Instalación de sistemas requeridos en el desarrollo de sus funciones operativas, tácticas y estratégicas	()	()	()	()
• Soluciones de desarrollo tecnológico – Evaluación y selección de tecnología de vanguardia; definición de nuevos enlaces con otras empresas vía telecomunicaciones, automatización de oficinas, etc.	()	()	()	()
• Servicios operativos – Instalación de equipo de cómputo y telecomunicaciones – Capacitación en el uso de la tecnología – Atención a fallas de software y aplicaciones – Atención a fallas en equipos de cómputo y comunicaciones	() () () ()	() () () ()	() () () ()	() () () ()

Tabla 7.3 Cuestionario de diagnóstico actual (etapa preliminar), aspectos administrativos de informática

Concepto	Descripción	Comentarios
Misión de informática (solicitar organigrama)		
Funciones o áreas de informática * *		
Macroproyectos de informática * *		
Objetivos de la función de informática * *		
Políticas referentes a cada función de informática * * *		
Áreas de oportunidad que se derivan de informática * *		

Tabla 7.4 Paquetes de software instalados (diagnóstico de informática)*

	Original (Sí/No)	Número de instalaciones
Procesador de palabras Nombre(s)	()	()
Hojas de cálculo/graficadores Nombre(s)	()	()
Lenguajes/manejador de bases de datos Nombre(s)	()	()
Presentador/textos Nombre(s)	()	()
Correo electrónico/control de proyectos Nombre(s)	()	()
Interfase gráfica Nombre(s)	()	()

* Es importante verificar el tipo de software que existe en la empresa antes de aplicar el cuestionario a cada gerente o subordinado que conozca bien esta información.
El auditor en informática deberá tomar sólo un muestreo aplicando el cuestionario a usuarios que considere clave y al responsable de informática (para verificar congruencia).

Tabla 7.5 Sistemas de información instalados (diagnóstico de informática) *

	Sí	No
Sistemas estratégicos de información Nombre(s)	()	()
Sistemas tácticos de información Nombre(s)	()	()
Sistemas operativos de información Nombre(s)	()	()

* Los sistemas estratégicos de información apoyan directamente a la alta dirección en la toma de decisiones. Los sistemas tácticos apoyan al nivel gerencial en el desempeño de sus funciones administrativas y de toma de decisiones. Los sistemas operativos de información apoyan las actividades operativas diarias del negocio.

Tabla 7.6 Software instalado (diagnóstico de informática)

	A = usado por dirección B = usado por las gerencias C = usado por jefaturas D = usado por el nivel operativo			
	A	B	C	D
Procesador de palabras Nombre(s)	()	()	()	()
Hojas de cálculo/graficadores Nombre(s)	()	()	()	()
Lenguajes/manejador de bases de datos Nombre(s)	()	()	()	()
Presentador/textos Nombre(s)	()	()	()	()
Correo electrónico/control de proyectos Nombre(s)	()	()	()	()

Tabla 7.7 Hardware instalado (diagnóstico de informática)

	A = usado por dirección B = usado por las gerencias C = usado por jefaturas D = usado por el nivel operativo			
	A	B	C	D
Microcomputadoras Cantidad Modelo(s)	()	()	()	()
Portátiles Cantidad Modelo(s)	()	()	()	()
Minicomputadoras Cantidad Modelo(s)	()	()	()	()
Redes locales Cantidad Modelo(s)	()	()	()	()
Mainframes Cantidad Modelo(s)	()	()	()	()
Redes remotas Red MAN o WAN Satélite () Microondas () Telefónica ()	()	()	()	()
Interfase Nombre(s)	()	()	()	()

Tabla 7.8 Capacitación/actualización (diagnóstico de informática)

E = Excelente B = Buena R = Regular D = Deficiente				
	E	B	R	D
Sistemas estratégicos de información Nombre(s)	()	()	()	()
Sistemas tácticos de información Nombre(s)	()	()	()	()
Sistemas operativos de información Nombre(s)	()	()	()	()

Tabla 7.9 Capacitación/actualización (diagnóstico de informática)

E = Excelente B = Buena R = Regular D = Deficiente				
	E	B	R	D
Procesador de palabras Nombre(s)	()	()	()	()
Hojas de cálculo/graficadores Nombre(s)	()	()	()	()
Lenguajes/manejador de base de datos Nombre(s)	()	()	()	()
Presentador/textos Nombre(s)	()	()	()	()
Correo electrónico/control de proyectos Nombre(s)	()	()	()	()
Interfase Nombre(s)	()	()	()	()

* Es recomendable que los cuestionarios se apliquen tanto a usuarios seleccionados como al responsable de informática para validar la congruencia de los datos.

- Planes o proyectos del negocio que involucren a informática
- Cultura organizacional
- Imagen del desempeño del departamento o área de informática ante la alta dirección
- Apoyo de la dirección a informática
- Parámetros de medición para evaluar informática
- Fortalezas y debilidades de informática, según la alta dirección

Por su parte, el diagnóstico inicial de la sección de informática al menos reflejará como grandes puntos lo siguiente:

- Estructura
- Puestos y funciones globales, servicios relevantes, planes o proyectos del área cultural de trabajo
- Consideraciones del responsable de informática relativas al apoyo que recibe de la alta dirección de la empresa
- Fortalezas y debilidades del área, según el responsable de informática

En esta fase del proceso metodológico se estiman las áreas de informática que deben auditarse y se bosquejan los tiempos, costos y recursos inherentes a dicha revisión.

Los aspectos tecnológicos, administrativos, culturales y financieros — entre otros — brindan al auditor en informática un panorama real del escenario donde desarrollará su trabajo.

Hay que considerar que los factores meramente técnicos y económicos pierden mucha relevancia si se olvida que los aspectos humanos y culturales desempeñan una trascendental función en las organizaciones.

Aspectos como reestructuraciones organizacionales, auditorías, procesos de optimización de procesos — por nombrar algunos de uso común en las empresas — suelen generar resistencia y temor; por lo tanto, el auditor en informática ha de evaluar la madurez de la empresa ante el proceso de auditoría, así como el grado de apoyo que brindarán los niveles de mando superior a este tipo de proyectos.

Preguntas clave

1. ¿Qué condiciones deben existir antes de que el auditor en informática inicie la primera etapa de la metodología de auditoría en informática para el desarrollo de sus proyectos?
2. ¿Cómo definiría la etapa de evaluación preliminar?
3. Existen dos tipos de diagnóstico que emanan de esta etapa, ¿cuáles son?
4. ¿Qué resultados mínimos ha de arrojar cada uno de tales diagnósticos?

5. ¿Quiénes deben ser las personas de parte de la empresa que estarán involucradas en esta etapa y cuál será su función en la misma?
6. Indique la función de cada uno de los siguientes integrantes de la función de auditoría en informática en la primera etapa (evaluación preliminar):
 - Responsable de la función de auditoría en informática
 - Líder del proyecto de auditoría en informática
 - Auditor en informática
7. ¿Cuáles de las siguientes técnicas y herramientas debe utilizar el personal del área de auditoría en informática durante dicha etapa?:
 - Muestreo
 - Análisis
 - Observación/inspección
 - Documentación
 - Análisis costo/beneficio
 - Software de auditoría
 - Software para oficina (procesadores de palabra, hojas de cálculo, presentadores)
 - Microcomputadoras
8. Mencione brevemente qué aplicación y beneficios brinda en la etapa de evaluación preliminar cada una de las técnicas y herramientas que seleccionó en la pregunta anterior
9. ¿Qué restricciones se pueden presentar en la etapa de evaluación preliminar y qué acciones debe ejecutar el personal de auditoría en informática para eliminarlas o al menos minimizarlas a fin de asegurar el éxito del proyecto?
10. ¿Qué problemática se puede presentar a los auditores en informática si se omite el desarrollo de la etapa de evaluación preliminar?
11. ¿Qué ventajas tiene llevar a cabo de manera íntegra y oportuna la evaluación preliminar?



Etapa de justificación

Una vez que se ha concluido la etapa preliminar (cuando todas las tareas se han terminado satisfactoriamente y se obtuvieron los productos terminados para esa fase) se procede a continuar con la etapa de justificación, la cual se explica a continuación.

- Etapa preliminar (terminada)
- Etapa de justificación (en ejecución)
- Etapa de adecuación (posterior)

Nota: Es factible que el líder del proyecto de auditoría en informática desee realizar algunas actividades en paralelo, lo cual es muy válido y justificado si se cuenta con los recursos necesarios y la experiencia en este tipo de proyectos.

Se sugiere trabajar primero con las etapas aquí recomendadas para su asimilación o adecuación a las características propias de cada institución o negocio donde se intente trabajar con ellas.

En la etapa de justificación 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 en informática
3. Compromiso ejecutivo

Cada uno forma parte esencial del proceso metodológico. El primero porque define las áreas 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 líder de proyecto para continuar con las siguientes etapas contempladas en el plan general.

En la tabla 8.1 se detallan las tareas, productos terminados, responsables e involucrados de la etapa preliminar.

8.1 Áreas de oportunidad para la función de informática

En el capítulo anterior se comentó que uno de los aspectos relevantes del diagnóstico actual es que orienta al auditor en informática a vislumbrar ciertas áreas de oportunidad para el mejoramiento de alguna función específica del negocio a través de informática y, en ocasiones, el beneficio es directo para el área de informática.

Aquí se comienza a conformar una parte del plan de auditoría en informática debido a que las áreas de oportunidad que ven los entrevistados en la etapa preliminar (que consideran provechosas y de alto beneficio) no han sido implantadas y urge aprovecharlas.

Existen muchas razones para que el auditor en informática tome en cuenta las áreas de oportunidad expresadas por la alta dirección, los usuarios clave y el responsable de informática; la principal es que todas esas personas viven y dedican gran parte de su tiempo al negocio, por lo cual conocen mejor que nadie sus fortalezas, debilidades y tipo de soluciones.

No significa que el auditor en informática se comprometa a efectuar todas las tareas y actividades sugeridas por ellos. La deducción y objetividad empiezan a ser un factor clave en este momento; se revisarán o auditarán sólo las funciones o áreas relacionadas con informática que se enfoquen en la misión del auditor en informática;

Tabla 8.1 Proceso metodológico de la auditoría en informática: un enfoque práctico

Etapa	Tareas	Productos	Responsable	Involucrados
Justificación	1. Hacer matriz de riesgos	1.1 Matriz de riesgos	LP/AI	RAI
	2. Justificar la auditoría por cada área de revisión	2.1 Justificación de la matriz de riesgo	LP/AI	RAI
	3. Hacer un plan de auditoría en informática (global)	3.1 Plan general de informática	LP	RAI/AI
	4. Aprobación del plan	3.4 Plan aprobado	LP	RAI/RI

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



Contenido

Introducción, ix

1. Antecedentes, 1

2. Terminología de la auditoría en informática, 11

2.1 Informática, 11

2.2 Auditoría, 16

2.3 Auditoría en informática, 17

3. La auditoría en informática y su entorno, 21

3.1 El entorno en la informática, 22

4. Organización, 31

4.1 Estrategias y cursos de acción para la implantación formal de la función de auditoría en informática, 31

4.2 Estructura organizacional y funciones de la auditoría en informática, 33

4.3 Administración de la función de auditoría en informática, 43

4.4 Elementos de la administración de la función, 45

4.5 Hacia una auditoría en informática eficiente, 47

5. Planeación, 53

5.1 Proceso de planeación del negocio, 55

5.2 Proceso de planeación en informática, 56

5.3 Proceso de planeación de la auditoría, 56

5.4 Proceso de planeación de la auditoría en informática, 58

6. Metodología para el desarrollo e implantación de la auditoría en informática, 71

6.1 Proceso metodológico de la auditoría en informática, 73

6.2 Métodos, técnicas y herramientas por área de revisión, 74

7. Etapa preliminar o diagnóstico de la situación actual, 81

7.1 Diagnóstico del negocio: alta dirección y áreas usuarias, 81

7.2 Diagnóstico de informática: responsables de la función, 85

8. Etapa de justificación, 99

- 8.1 Áreas de oportunidad para la función de informática, 100
- 8.2 Matriz de riesgos, justificación por área de revisión, 102
- 8.3 Plan general del proyecto de auditoría en informática, 107
- 8.4 Compromiso ejecutivo, 109

9. Etapa de adecuación, 115

- 9.1 Definición y formulación de objetivos y requerimientos de éxito por cada área que se va a auditar, 117
- 9.2 Actualización del plan general, 117
- 9.3 Plan detallado del proyecto de auditoría en informática, 118
- 9.4 Aspectos por evaluar en cada área de revisión, 123
- 9.5 Definición de técnicas y herramientas por área de revisión, 123
- 9.6 Definición o actualización de estándares, políticas y procedimientos por área de revisión, 124
- 9.7 Elaboración o actualización de cuestionarios por área de revisión, 127

10. Etapa de formalización, 131

- 10.1 Verificación de prioridades, restricciones y alcances del proyecto, 133
- 10.2 Actualización del plan de la auditoría en informática, 134
- 10.3 Presentación formal del plan de auditoría en informática, 134
- 10.4 Aprobación formal del proyecto de auditoría en informática, 134
- 10.5 Compromiso ejecutivo, 135

11. Etapa de desarrollo, 139**12. Etapa de implantación, 153****Apéndice A: Uso práctico de la metodología, 161****Apéndice B: Cuestionarios para efectuar la auditoría en informática por áreas de revisión, 179****Apéndice C: Auditoría durante el ciclo de desarrollo e implantación de sistemas de información (soluciones de negocio), 211****Apéndice D: Mantenimiento, 235****Apéndice E: Auditoría de redes locales y telecomunicaciones, 249****Apéndice F: Auditoría del hardware, 267****Apéndice G: Auditoría del software, 277****Apéndice H: Auditoría de seguridad, 285****Apéndice I: Investigación tecnológica, 307****Apéndice J: Informe de auditoría en informática, 311****Bibliografía, 315**

Introducción

Llevé a la realidad el presente trabajo debido en gran parte a cinco factores:

1. Transmitir honesta y profesionalmente lo que he asimilado a lo largo de mis años como estudiante y profesionista en el campo de la auditoría en informática para facilitar e impulsar el desempeño formal de la misma en todos los negocios e instituciones educativas donde se encuentre la tecnología de informática.
2. A la gran inquietud y necesidad que veo latente en los medios educativos y de negocios de contar con un proceso de auditoría en informática digerible, práctico y eficiente para la evaluación de la función de informática que facilite tanto el planteamiento oportuno de las recomendaciones como los cursos de acción requeridos para dar una solución integral de informática aprovechando las áreas de oportunidad que emergen de dicho proceso.
3. Para brindar un esfuerzo más de mi parte que apoye a esa gran cantidad de estudiantes, profesores, profesionistas, etc., que se encuentran convencidos de que los recursos de informática deben ser evaluados, protegidos y administrados como cualquier otro activo importante o estratégico del negocio.
4. El deseo de superación que motivaron en mí los maestros C.P. Alejandro L. e Ing. Antonio Q.; mis colegas o compañeros de trabajo Ing. Carlos U., Lic. José Antonio V., Gerardo D., C.P. Jesús M., Ing. Jaime R., C.P. Carlos S., C.P. Ramiro S., C.P. César R., Ing. Gerardo L., Ing. Carlos T., Ing. Rogelio V., Ing. Manuel H., Ing. César Fausto G., Ing. Servando J., Ing. Leticia N., Lic. Alejandro J., Ing. Humberto G., Ing. Mario R., Ing. Emilio L. e Ing. Rubén E., así como otros no menos importantes que guardo en mi memoria.
5. El apoyo y confianza permanente que me brindaron en la concepción, elaboración y reproducción del presente trabajo: Lic. Claudia M., Ing. Luis G., Ing. Carlos U., Ing. Luis G., Lic. Gerardo L., mi esposa, Lic. Vicky M., mis padres, hermanos, amigos y cuñados.

Desarrollé el proceso metodológico aquí planteado con base en una extensa aplicación de la auditoría en informática en diferentes giros y tamaños de empresas, tratando siempre de cumplir con los estándares y procedimientos recomendados por las asociaciones nacionales e internacionales relacionadas con este campo.

Asimismo, se realizó una investigación detallada del material existente a nivel nacional e internacional relacionado con la auditoría en informática. La presente obra está integrada también por cuestionarios y formatos prácticos que brindarán a los auditores en informática elementos para cubrir de manera satisfactoria los temas de auditoría, seguridad y control inherentes a la función de informática.

Se buscó darle un enfoque práctico sin caer en falsas afirmaciones o debilidades de carácter ético o profesional.

De igual manera, se afirma y trata de explicar a lo largo del libro que el éxito de una auditoría en informática depende de la aplicación de otros factores aparte de una metodología; dichos factores son:

- Uso de estándares y políticas recomendados por asociaciones
- Actualización permanente en los campos de la auditoría y la informática
- Apoyo de la alta dirección y conocimiento del negocio
- Valores morales y habilidades personales
- Otros que se mencionarán a lo largo de los capítulos del libro

He ido formando y actualizando este proceso metodológico de manera constante a través del ejercicio de la auditoría en informática en empresas privadas y gubernamentales, así como en mi práctica docente ante una gran cantidad de alumnos de nivel licenciatura y de posgrado a los que he impartido las materias relacionadas con los temas tratados en este libro (auditoría en informática, administración de proyectos de informática, metodología de desarrollo de sistemas, planeación de informática, administración de centros de cómputo, seminario de informática, etcétera).

Se han desarrollado proyectos relacionados con las mismas en negocios de los diversos sectores, concluyendo con acciones y recomendaciones de mejoramiento y reposicionamiento de la función de informática con una aprobación formal de los responsables de dicha función o de la alta dirección.

Los cuestionarios y formatos presentados a lo largo del libro son resultado de un análisis detallado asimilado a través de los años y tienen una estructura lógica y clara.

No busqué descubrir el hilo negro; más bien orienté mi esfuerzo a conseguir un método ordenado para guiar paso a paso a todos los interesados en evaluar y revisar los diferentes aspectos de la informática.

Se trata de llevar una secuencia lógica y práctica a lo largo de cada capítulo, donde se consideran los siguientes aspectos:

- **Antecedentes:** orígenes e importancia de la auditoría en informática
- **Terminología:** conceptos y criterios personales acerca de la auditoría en informática
- **Organización:** estructuras organizacionales, funciones, etc., de la función
- **Planeación:** de negocios, auditoría, informática y de auditoría en informática

- **Matriz de riesgos:** clasificación y propuesta de las áreas que serán auditadas
- **Proceso metodológico:** etapas, tareas, etc., sugeridas para ejecutar la función
- **Técnicas y herramientas:** apoyo requerido para ejecutar el método recomendado
- **Cuestionarios:** un detalle clasificado de los aspectos clave que se deben cuestionar o validar en cada área auditada
- **Fuentes de información:** dónde y cómo obtener la información que fortalezca y actualice al auditor en informática
- **Informe de auditoría:** qué presentar al final de la auditoría y cómo hacerlo

Antecedentes

Desde que la informática se enfocó hacia el apoyo de la sistematización en las áreas del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nómina, etc., lo cual originó lo que se conoce como Auditoría a sistemas de información.

Posteriormente, el uso de la informática cubrió las áreas de negocio en todos los niveles con productos y servicios muy variados; proliferaron las minicomputadoras o equipos departamentales; después llegaron las microcomputadoras o computadoras personales y entraron de lleno las redes locales, la integración empresarial a través de las telecomunicaciones y un gran número de componentes de tecnología. Tal tecnificación del medio imposibilitó al responsable de informática y a los auditores de sistemas tradicionales seguir evaluando este campo con métodos y procedimientos anticuados.

Se hizo necesario un replanteamiento del fondo y forma de la auditoría en informática.¹ Este trabajo busca, entre otras cosas, dar una dimensión más realista y adecuada a la auditoría en informática.

El ejercicio práctico y formal de la auditoría en informática brindará a sus ejecutantes y a los negocios un sentimiento de satisfacción justificado por el entendimiento y compromiso que implica asegurar el uso correcto de los recursos de informática para el logro de las estrategias.

Este libro no pretende ser la varita mágica que solucione los problemas que aquejan a la informática, sino convertirse en uno de los motores que impulsen a los

¹ También conocida por muchos como auditoría de sistemas; empero, este término se refiere a la revisión de los sistemas de información en desarrollo, operación y mantenimiento; por lo tanto, el concepto es inadecuado porque los elementos de informática susceptibles de revisión y control son muchos y de diversas complejidades. La definición correcta para quienes evalúan y verifican políticas, controles, procedimientos y seguridad en los recursos dedicados al manejo de la información es auditoría en informática.

negocios para obtener los resultados esperados de dicha tecnología en los tiempos, costos, beneficios y calidad esperados.

Todo lo que se planea ha de ejecutarse con formalidad y oportunidad, lo cual se relaciona con el hecho de que toda organización quiere tener sus activos en las mejores condiciones posibles y salvaguardar su integridad.

La función del auditor en informática no es ser un capataz o policía del negocio, como tantas veces se ha planteado de manera sarcástica o costumbrista en las organizaciones. Este profesionista se orienta a que sea un punto de control y confianza para la alta dirección, además de que busque ser un facilitador de soluciones.

Por analogía, el auditor es como el doctor que evalúa al paciente y le recomienda el tratamiento idóneo para estar en óptimas condiciones de salud. Según la situación del enfermo, recomendará tratamientos ligeros o fuertes y estrictos.

Lo importante es lograr que el paciente sepa que puede mejorar su salud. Esa es la orientación del auditor en informática: conducir a la empresa a la búsqueda permanente de la salud óptima de los recursos de informática y de todos aquellos elementos que se relacionan con ella.

No hay que pensar que este proceso cambiará la cultura organizacional, los métodos de trabajo, la mala calidad ni la improductividad en las áreas relacionadas con la informática de la noche a la mañana; es un elemento estratégico directo que apoya la eliminación de cada una de las debilidades mencionadas; sin embargo, ha de coexistir con personal responsable y profesional, así como con directores y accionistas comprometidos con la productividad, calidad y otros factores recomendados para ser empresas de clase mundial.

Se espera que cada auditor sea un profesional, un experto; pero sobre todo, que sea un ser flexible, humano, que entienda el contexto real del negocio. Su principal objetivo es dar la dimensión justa a cada problemática, convirtiéndola en área de oportunidad y orientándola a una solución de negocio.

Conviene recordar que en las empresas existen objetivos comunes a todas las áreas respecto de los recursos de informática; por ejemplo, el máximo uso y aprovechamiento de la tecnología mediante políticas, procedimientos y métodos apropiados. En este sentido, la función de la auditoría en informática es uno de los medios más importantes y especializados para lograr dicho fin.

Un poco de historia y un poco de actualidad...

En los años cuarenta empezaron a darse resultados relevantes en el campo de la computación, con sistemas de apoyo para estrategias militares; posteriormente se incrementó el uso de las computadoras y sus aplicaciones y se diversificó el apoyo a otros sectores de la sociedad: educación, salud, industria, política, banca, aeronáutica, comercio, etcétera.

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

En el presente la informática se ha extendido a todas las ramas de la sociedad; es decir, resulta factible controlar un vuelo espacial por medio de una computadora así como seleccionar las compras del hogar en una microcomputadora.

Esta rapidez en el crecimiento de la informática permite 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 mejoría en la imagen o satisfacción del cliente, pero ambos con la misma importancia para seguir impulsando la investigación y actualización constante de la tecnología.

La idea de que se obtienen mayores beneficios que antes no está muy lejos de la realidad; sin embargo, también es válido afirmar que los costos han sido altos y en muchas ocasiones han rebasado los límites esperados, ocasionando grandes pérdidas y decepciones en los negocios.

Las empresas y organismos interesados en que la informática siga creciendo para beneficio de la humanidad (educación, productividad, calidad, ecología, etc.) desean que este crecimiento sea controlado y orientado de manera profesional; esto es, se debe obtener el 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 y, de igual manera, es responsabilidad de la dirección no aprobar proyectos que no aseguren la rentabilidad de la inversión.

Con el paso de los años la informática y todos los elementos tecnológicos que la rodean han ido creando necesidades en cada sector social y se han vuelto un requerimiento permanente para el logro de soluciones.

A continuación se mencionan algunas consideraciones que corresponden a una necesidad real y no a una tendencia:

- Todas las actividades de la sociedad buscan apoyarse de alguna forma en la tecnología de informática.
- Tanto los equipos de cómputo de diferentes marcas y capacidades como las bases de datos y los sistemas de información deben ser una solución integrada.
- La capacitación tiene que ser permanente en el uso de la tecnología de informática debido a su constante crecimiento y actualización.
- Hardware, software, telecomunicaciones y otros medios electrónicos han de estar interrelacionados para explotar al máximo sus capacidades y dar soluciones a todos los sectores de la sociedad.
- Integrar a la comunidad de manera permanente al campo de la informática.

- La gran penetración de la informática en todos los niveles del sector educativo, así como en los sectores social y cultural.
- El control y seguridad sobre todos los recursos de informática es una necesidad.
- Se debe evaluar de manera formal y periódica la función de informática.
- El proceso de planeación de los negocios ha de integrar de manera permanente la función de informática.
- Otros.

El incremento permanente de las expectativas y necesidades relacionadas con la informática, al igual que la actualización continua de los elementos que componen la tecnología de este campo, obligan a las entidades que la aplican a contar con controles, políticas y procedimientos que aseguren a la alta dirección que los recursos humanos, materiales y financieros involucrados son protegidos adecuadamente y que se orientan a la rentabilidad y competitividad del negocio.

¿Por qué preocuparse de cuidar esa caja etiquetada con el nombre de informática?

Si la respuesta que brinde a cualquiera de las siguientes preguntas es negativa, le convendría reafirmar o considerar la necesidad de asumir la responsabilidad de controlar y brindar seguridad permanente a los recursos de informática:

- ¿Los usuarios y la alta dirección conocen la situación actual de la función de informática en la empresa (organización, políticas, servicios, etcétera)?
- ¿Se aprueba formal y oportunamente el costo/beneficio de cada proyecto relacionado en forma directa con la informática?
- ¿La informática apoya las áreas críticas del negocio?
- ¿El responsable de la informática conoce los requerimientos actuales y futuros del negocio que necesitan apoyo de los servicios y productos de su área?
- ¿Todos los elementos del negocio conocen las políticas y procedimientos inherentes al control y seguridad de la tecnología de informática?
- ¿Existen dichas políticas y procedimientos de manera formal?
- ¿Hay un plan de seguridad en la informática?
- ¿Se ha calculado el alcance e impacto de la informática en la empresa?
- ¿Hay un plan estratégico de informática alineado al negocio?
- ¿Existen responsables que evalúen formal e imparcialmente la función de la informática?
- ¿Se cuenta con un control formal de cada proyecto relativo al área?
- ¿Es importante para usted la informática?
- ¿Evalúa periódica y formalmente dicha función de la informática?
- ¿Auditan sólo sistemas de información y no otras áreas de la informática?

Cada una de estas preguntas encierra una importancia específica para el buen funcionamiento informático en cualquier negocio; todas están interrelacionadas y la

negación de alguna es una pequeña fuga de gas que — con el tiempo y un pequeño chispazo — puede 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 clave del negocio, improductividad y baja calidad de los recursos de informática, planes de informática no orientados a las metas y estrategias de negocio, piratería de software, fuga de información a la competencia o proveedores, entre otros daños.

La improductividad, el mal servicio y la carencia de soluciones totales de la función de informática fueron, son y pueden seguir siendo mal de muchas organizaciones. El problema real radica en que todos los proyectos prioritarios hacen gala de sentirse apoyados por la informática; entonces, ¿por qué no cuidarla?

En seminarios, pláticas de comedor o pasillo en empresas (así como en instituciones de gobierno y escuelas universitarias) y aun en las mismas áreas o departamentos de informática se relatan los problemas más comunes de los usuarios y del personal. Sin embargo, parece ser que un gran porcentaje de tales interlocutores no se percata o no desea reconocer que esta problemática se ha venido planteando desde hace muchos años por las mismas causas y con los mismos efectos negativos para la organización. La diferencia puede ser que ahora los individuos que cometen estas fallas o debilidades funcionales están dispersos por toda la organización utilizando tecnología supuestamente más eficiente y, por supuesto, más cara. Algunos problemas de esta índole son:

- Debilidades en la planeación del negocio al no involucrar la informática.
- Resultados negativos (improductividad, duplicidad de funciones, etc.) en el desarrollo, operación y mantenimiento de sistemas de información.
- Falta de actualización del personal de informática y técnico donde se encuentran instalados los sistemas y las soluciones del negocio.
- Mínimo o nulo involucramiento de los usuarios en el desarrollo e implantación de soluciones de informática.
- Capacitación deficiente en el uso de los sistemas de información, el software (procesadores de palabras, hojas de cálculo, graficadores, etc.) y el hardware (impresoras y otros periféricos, teclado, etc).
- Administración débil o informal de proyectos.
- Carencia de un proceso de análisis costo/beneficio formal previo al arranque de cada proyecto de informática.
- Metodologías de planeación y desarrollo de sistemas informales no estandarizadas y en muchos casos inexistentes.
- Uso y entendimiento mínimo o inexistente de técnicas formales para el desempeño de funciones en las áreas de informática:
 - Análisis.
 - Entrevistas.

- Cuestionarios.
- Modelación de datos.
- Costo/beneficio, etc.
- Falta de un proceso formal de planeación de informática.
- Involucramiento mínimo o informal de la alta dirección en los proyectos de informática.
- Proyectos de auditoría o evaluación de informática esporádicos e informales.
- Otros.

La importancia de la auditoría en informática

La tecnología de informática, traducida en hardware, software, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, EDI, telecomunicaciones, servicios y organización de informática es una herramienta estratégica que brinda rentabilidad y ventaja competitiva a los negocios frente a sus similares en el mercado; pero puede originar costos y desventajas competitivas si no es bien administrada y dirigida por el personal encargado.

Dados los extremos señalados, surgen de inmediato un par de preguntas:

¿Cómo saber si estoy administrando y dirigiendo de manera correcta la función de la informática?

La respuesta siempre ha existido: mediante evaluaciones oportunas y completas de dicha función por personal calificado (o sea consultores externos, auditores en informática), o evaluaciones periódicas realizadas por el mismo personal de informática, entre otras estrategias.

¿Es necesario auditar o evaluar la función de informática y quiénes lo harían?

Aquí la respuesta depende de cada organización y de sus necesidades por conocer el estado real de su tecnología en informática.

Lo que resulta innegable es que la informática se convierte cada día en una herramienta permanente de los procesos principales de los negocios, en una fuerza estratégica, en un aliado confiable y oportuno. Todo lo anterior es posible tenerlo en la empresa si se implantan los controles y esquemas de seguridad requeridos para su aprovechamiento óptimo.

Hay personal especializado en informática y auditoría que se encuentra profesional y moralmente preparado para auditar en este campo. Lo primero que tienen que hacer las organizaciones es reconocer la necesidad de contar con una función que evalúe de manera satisfactoria los recursos de informática, así como todos los elementos inherentes a ellos.

Una vez que la alta dirección tome conciencia de lo saludable y productivo que es contar con un área independiente que asegure y promueva el buen uso y aprovechamiento de la tecnología de informática, el siguiente paso es delegar la responsa-

bilidad en personal altamente capacitado para ejercer la auditoría en informática dentro de la organización de manera formal y permanente.

Resumen

Siempre ha existido la filosofía de las organizaciones con respecto a llevar controles y procedimientos de todos los procesos, productos y datos considerados como activos estratégicos. En el terreno de los sistemas de información y tecnología, un alto porcentaje de las empresas tiene problemas en el manejo y control tanto de los datos como de los elementos en que almacena, procesa y distribuye la información.

Esta situación genera tiempos de respuesta inadecuados en la recopilación, proceso y entrega de resultados; asimismo, origina incertidumbre acerca de la productividad de los recursos involucrados en la operación diaria de los datos y cuestiona de manera permanente la rentabilidad de la informática. Es una voz de alerta que se debe escuchar.

En forma adicional, cabe señalar que muchas compañías sólo creen que es necesario proteger la información que se maneja por medio de recursos tecnológicos, mas no por ello están dispuestas a invertir dinero, tiempo y compromiso para minimizar o eliminar dicha problemática.

A lo anterior hay que agregar la presencia de dos grandes grupos de problemas:

1. Falta de conocimiento del alcance de los sistemas de información, que en la práctica se traduce en meras actividades "apaga fuegos", falta de estándares en software y hardware, así como usuarios valientes que desarrollan soluciones por su cuenta sin los requisitos metodológicos necesarios.
2. Capacitación inadecuada a los usuarios y casi nula al personal de informática respecto del uso de metodologías de planeación y desarrollo para la administración de sus funciones; insatisfacción de los usuarios clave del negocio por los resultados producidos por el departamento de informática, que termina calificada como "mala, vanidosa y cara".

Lo anterior se repite en gran número de compañías; por lo tanto, la pregunta inminente es: ¿por qué si gasta tanto en informática y no da resultados no se deciden a desecharla o a usarla como debe ser? Simplemente porque no saben qué hacer con ella. Unos la desprecian porque no la entienden y otros, que le temen por su incapacidad para usarla y administrarla, le dan el beneficio de la duda.

Por ello, se concluye que el primer paso para detectar el grado de confianza, disponibilidad y rentabilidad de la información y de los recursos de informática es la aceptación de la dirección o accionistas de los beneficios que brinda dicha tecnología; el segundo es asegurar la custodia y protección de la misma.



Se requiere además la dimensión real del escenario tecnológico y del control existente a través de un estudio preliminar o diagnóstico de la situación actual. Después, todo recaerá en el compromiso que la alta dirección y los empleados asuman para dar solución oportuna a las debilidades o carencias que emanen de dicho análisis.

Debido a que la alta dirección debe contar siempre con la certidumbre respecto de la integridad y disponibilidad de la información y los recursos de informática, es necesario formalizar un proceso de auditoría en informática en la organización. La orientación de dicha función es clara: eliminar o al menos minimizar en lo posible los riesgos y circunstancias dañinos a los elementos mencionados.

La historia da muestra clara de ello a partir de la creación de funciones de supervisión, auditoría y evaluación tanto de las áreas financieras y productivas como de la misma administración.

Es importante recalcar que también se requiere la reunión — en tiempo y lugar — de los siguientes aspectos para que tengan éxito la evaluación de los recursos informáticos y la administración de la información en el negocio:

- a) Compromiso de todos los individuos relacionados.
- b) Continuidad en el proceso de evaluación y control.
- c) Especialización de parte de quienes llevan a cabo dicha función.
- d) Conocimiento del negocio a través de un involucramiento permanente en las etapas de planeación.
- e) Enfoque preventivo, no correctivo.
- f) Facilitar soluciones, no limitar la operación de la compañía implantando un exceso de controles.
- g) Estudio del medio tecnológico y organizacional por parte de los encargados de la función.
- h) Trabajar con base en requerimientos y riesgos propios del negocio y no según criterios de mercado.
- i) Evaluar para resolver y proteger, sin entorpecer y burocratizar las funciones.
- j) Lograr que el personal de las organizaciones advierta que las medidas preventivas son parte importante del trabajo diario y que incumben a todos por igual.

Preguntas clave

1. Desde su punto de vista, ¿la tecnología de informática debe considerarse un activo en las empresas? ¿Por qué?
2. ¿Cuáles son las áreas o departamentos de negocios que de manera tradicional han implantado sistemas de información para soportar sus operaciones y administrar la información que emanaba de las mismas?

3. ¿Por qué se volvió necesario auditar los sistemas computarizados?
4. ¿Tiende la información a incrementar o decrementar la administración de los datos y sus procesos a través de los recursos informáticos? ¿En qué se basa su respuesta?
5. ¿Cuáles acontecimientos llevaron a las empresas a formalizar, en algunos casos, el proceso de evaluación de las áreas de informática?
6. ¿Qué eventos y escenarios negativos deben presentarse en una organización para que se origine la necesidad (y concientización) de formalizar un proceso de evaluación de informática?
7. ¿Cuál cree que debe ser el perfil de un auditor en informática? Mencione tres características inherentes a su función.
8. ¿Qué aspectos relevantes de la tecnología de informática son una realidad en la sociedad y no una tendencia?
9. ¿Cree que sea necesario auditar la función de informática? ¿Por qué?
10. ¿Cómo puede saber la alta dirección si se está administrando correctamente la función de informática?

Terminología de la auditoría en informática

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

Las actividades profesionales o estudiantiles que dieron la pauta para definir de manera personal los aspectos relevantes de cada uno de los puntos tratados en este capítulo fueron principalmente las siguientes:

- Estudios de licenciatura y posgrado.
- Cursos y seminarios nacionales e internacionales.
- Reuniones y juntas con responsables de áreas de negocio.
- Consultorías a empresas en proyectos de informática y auditoría en informática.
- Impartición de cursos en universidades e institutos tecnológicos.
- Impartición de conferencias de auditoría en informática e informática.

2.1 Informática

La informática se desarrolla con base en normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional.

De acuerdo con lo anterior, sólo se mencionarán algunos aspectos de informática necesarios para su entendimiento (supuestamente asimilado por los usuarios de este libro); sin embargo, se recomienda leer los textos sugeridos en la bibliografía, así como las participaciones más directas y activas en los institutos o asociaciones relacionados con el campo de la informática.

Con base en lo expuesto, la informática es el *campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionados con las computadoras y el manejo de la información por medios electrónicos*, el cual comprende las áreas de la tecnología de información orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya (entidades internas y externas de los negocios) de manera oportuna, veraz y confiable; además, es el *proceso metodológico que se desarrolla de manera permanente en las organizaciones para el análisis, evaluación, selección, implantación y actualización de los recursos humanos* (conocimientos, habilidades, normas, etc.), *tecnológicos* (hardware, software, etc.), *materiales* (escritorios, edificios, accesorios, etc.) y *financieros* (inversiones) *encaminados al manejo de la información, buscando que no se pierdan los propósitos de calidad, confiabilidad, oportunidad, integridad y veracidad, entre otros propósitos*.

Hardware se refiere a los componentes físicos y tangibles de las computadoras, generalmente clasificados en cuatro grandes ramas:

- Microcomputadoras o computadoras personales.
- Redes (locales, abiertas, etc.).
- Minicomputadoras.
- Supercomputadoras (*mainframes*).

Software implica la parte no física de las computadoras. Esto significa que es la porción intangible de los equipos de cómputo, es decir, programas con orientaciones específicas para la administración de la información y el uso eficiente de los recursos de cómputo. Su clasificación se puede resumir en los siguientes términos:

- *Software de aplicaciones* (sistemas de información):
 - Administrativos.
 - Financieros.
 - De manufactura.
 - Otros.
- *Software de paquetes computacionales* (paquetería):
 - Hojas electrónicas.
 - Procesadores de palabras.
 - Otros.
- *Software de programación*:
 - Lenguajes de tercera generación.
 - Lenguajes de cuarta generación.
- *Software de sistemas operativos*:
 - Para microcomputadoras.
 - Para minicomputadoras.
 - Para supercomputadoras.

- *Productos CASE (Computer Aided Software Engineering):*
 - Para planeación de sistemas de información.
 - Para análisis de sistemas de información.
 - Para diseño de sistemas de información.
 - Para todo el ciclo de desarrollo e implantación de sistemas de información (CDISI).
- *Para propósitos específicos:*
 - Arquitectura.
 - Auditoría.
 - Ingeniería.
 - Medicina.
 - Otras ciencias.

Sistemas de información: Son el conjunto de módulos computacionales o manuales organizados e interrelacionados de una manera formal para la administración y uso eficiente de todos los recursos (humanos, materiales, financieros, tecnológicos, etc.) de un área específica de la empresa (manufactura, administración, dirección, etc.) con la finalidad de representar los procesos reales del negocio, y orientar los procedimientos, políticas y funciones inherentes para el logro de las metas y objetivos del negocio.

Los sistemas de información pueden orientarse al apoyo de los siguientes aspectos:

- Niveles operativos del negocio.
- Niveles tácticos del negocio.
- Niveles estratégicos del negocio.

Sistemas de información estratégica (SIE): Son aquellos que de manera permanente proporcionan a la alta dirección una serie de parámetros y acciones encaminadas a la toma de decisiones que apoyarán al negocio en el seguimiento de la rentabilidad y competitividad respecto de la competencia.

Metodología: Es un conjunto de etapas (fases o módulos) formalmente estructurados, de manera que brinden a los interesados los siguientes parámetros de acción en el desarrollo de sus proyectos:

- Plan general y detallado.
- Tareas y acciones.
- Tiempos.
- Aseguramiento de calidad.
- Involucrados.
- Etapas (fases o módulos).
- Revisiones de avance.
- Responsables.

- Recursos requeridos.
- Otros.

Nota: Una buena metodología debe responder a los siguientes cuestionamientos: ¿qué hacer?, ¿dónde debo hacerlo?, ¿cómo plantearlo?, ¿por qué aprobarlo?, ¿cuándo revisarlo?, ¿cuándo empezarlo?, ¿quién debe hacerlo?, ¿por qué debo hacerlo?, ¿cómo aprobarlo?, ¿quiénes deben comprometerse?, ¿por qué revisarlo?, ¿cuándo terminarlo?, ¿cómo justificarlo?, etc.

Ejemplos de metodologías:

- De planeación de sistemas.
- De desarrollo de sistemas.
- De calidad.
- De auditoría en informática (como la propuesta de este libro).
- De productividad.
- De reingeniería.

Técnicas: Es el conjunto de procedimientos y pasos ordenados que se usan en el desarrollo de un proyecto con el propósito de finalizar las etapas, fases o módulos definidos en el proceso metodológico.

Algunas de las técnicas generalmente aceptadas son:

- Análisis estructurado.
- Diseño estructurado.
- Análisis costo/beneficio.
- Gráficas de Pert.
- Gráficas de Gantt.
- Documentación.
- Programación estructurada.
- Modelación de datos y procesos (pueden aparecer en el análisis).
- Entrevistas.
- Otras.

Nota: Las técnicas son el conjunto de pasos ordenados lógicamente para apoyarse en la terminación (cómo hacerlo) de todas las acciones o tareas estimadas en el proyecto emanado de la metodología.

Herramientas: Es el conjunto de elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica. Antes del auge de las computadoras, así como de otros elementos tecnológicos relacionados con la ingeniería, arquitectura, etc., dichas herramientas eran simples máquinas o utensilios manuales que apoyaban el desarrollo de las tareas de cada uno de los proyectos. Algunos ejemplos ilustrativos son los siguientes:

Los diagramas de flujo de un sistema de información se elaboraban con figuras inmersas en una tabla de plástico o cartón; algunos profesionistas o estudiantes más vanguardistas se apoyaban en paquetes computacionales, como los primeros diagramadores de flujo que salieron al mercado al mismo tiempo que las microcomputadoras.

En su mayoría, los diagramas eran validados de manera superficial y sin que los analistas de sistemas buscaran la congruencia de esos dibujos con la realidad que deseaban representar; con el tiempo, lo anterior produjo un desarrollo de sistemas de información insatisfactorio para los usuarios y un número elevado de recursos involucrados con el mantenimiento de dichos sistemas.

Las gráficas de Gantt y de Pert se hacían a mano o con el apoyo de algunos utensilios específicos para el dibujo; asimismo, los cálculos relacionados con dichas técnicas eran desarrollados mentalmente o con una simple calculadora; en ocasiones se confiaban dichos cálculos a la buena memoria o experiencia práctica, con el consecuente nivel de error y de frustración en los resultados.

La mayoría de empresas realiza actualmente la etapa de análisis de sistemas, el proceso de planeación de sistemas y las evaluaciones de los recursos computacionales sin un plan pre-elaborado, sin involucrar los recursos humanos afectados directamente en dichos proyectos, esto tal vez por el desconocimiento de las técnicas requeridas para ello: entrevistas, cuestionarios, análisis y trabajo de equipo, etc. Los resultados son conocidos a lo largo y ancho de las empresas: altos costos sin beneficios tangibles al término o cancelación de los mismos, un grado de insatisfacción muy palpable de los usuarios y la alta dirección, etc.

Existen más y más ejemplos que podrían ilustrar el grado de complejidad y de improductividad que se genera cuando no se cuenta con las herramientas de productividad disponibles para el desarrollo eficiente de los proyectos.

Herramientas de productividad: Ayudan a optimizar el tiempo de los recursos en el desarrollo de un proyecto; asimismo se encaminan a proporcionar resultados de alta calidad, por ejemplo:

- Procesadores de palabras (documentación, entrevistas, cuestionarios, entre otros).
- Diagramadores (diagramas de flujo, diagramas organizacionales, etc.).
- Gráficos (estadísticas, estimación de actividades en tiempo, costos, etc.).
- Productos CASE (modelación de datos, modelación de procesos, validación de datos y procesos, generadores de diccionarios de datos, generadores de código, documentación, por citar algunos casos).
- Impresoras (láser, por ejemplo).
- Microcomputadoras.
- Otros.

Nota: Las herramientas de productividad no se asocian necesariamente con inversiones elevadas en la compra de hardware y software especializado; se relacionan con los recursos manuales o automatizados que apoyan al personal en la obtención de productos de calidad en niveles de productividad aceptados por los líderes de proyectos o definidos por los estándares de trabajo del negocio.

2.2 Auditoría

La auditoría se desarrolla con base en normas, procedimientos y técnicas definidas formalmente por institutos establecidos a nivel nacional e internacional; por lo tanto, sólo se expondrán algunos aspectos necesarios para su entendimiento; no obstante, se sugiere leer los libros listados en la bibliografía, así como la participación directa y activa en los institutos o asociaciones relacionados con el campo de la especialidad.

Auditoría es un proceso formal y necesario para las empresas con el fin de asegurar que todos sus activos sean protegidos en forma adecuada. Asimismo, la alta dirección espera que de los proyectos de auditoría surjan las recomendaciones necesarias para que se lleven a cabo de manera oportuna y satisfactoria las políticas, controles y procedimientos definidos formalmente, con objeto de que cada individuo o función de la organización opere de modo productivo en sus actividades diarias, respetando las normas generales de honestidad y trabajo aceptadas. Por otra parte, es el conjunto de tareas realizadas por un especialista para la evaluación o revisión de políticas y procedimientos relacionados con las siguientes áreas:

- Administrativas.
- Financieras.
- Operativas.
- Informática.
- Crédito.
- Fiscales (efectuadas por disposición gubernamental).

Por todo lo expresado, se concluye que es un proceso formal que se efectúa por requerimientos de las empresas o del gobierno en periodos establecidos con anterioridad por los interesados, con objeto de verificar el cumplimiento oportuno de las políticas y procedimientos relacionados con cada una de las actividades de la organización.

Tareas principales de la auditoría:

- Estudiar y actualizar permanente las áreas susceptibles de revisión.

- Apegarse a las tareas que desempeñen 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 o responsables directos del negocio.
- Elaboración del informe de auditoría (debilidades y recomendaciones).
- Otras recomendadas para el desempeño eficiente de la auditoría.

2.3 Auditoría en informática

La auditoría en informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, nada más se señalarán algunos aspectos básicos para su entendimiento; sin embargo, conviene leer los libros sugeridos en la bibliografía, así como la participación más directa y activa en los institutos o asociaciones relacionados con el campo de la auditoría en informática.

Así, la *auditoría en informática* es:

- a) Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente.
- b) Las actividades ejecutadas por los profesionales del área de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.). Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual ha de contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y optimización permanente de la tecnología de informática en el negocio.
- c) El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que pasa por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.
- d) Proceso metodológico que tiene el propósito principal de evaluar todos los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opera con un criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad de la organización.



Resumen

La sistematización de las áreas administrativas y productivas de la empresa se conceptualiza como la disciplina y ordenamiento estructurado y lógico de las actividades necesarias para el manejo de las transacciones y movimientos que afectan la situación financiera y operacional de la organización.

Dichas transacciones están enmarcadas dentro de nombres de áreas o procesos específicos: contabilidad, producción, recursos humanos, logística, ventas, cobranzas, finanzas, etc. Cada una reconoce rápidamente la necesidad de incrementar la productividad del negocio y brindar una calidad real en los servicios al cliente. Para ello basan la operación y administración eficiente de los sistemas de información y recursos tecnológicos involucrados en las siguientes consideraciones:

- a) Documentación, aprobación y difusión formal de:
 - Flujos de datos
 - Flujos de operaciones, procesos y actividades
 - Responsabilidades
- b) Documentación, aprobación y difusión formal de:
 - Políticas
 - Procedimientos
- c) Administración de los recursos de informática:
 - Justificación
 - Evaluación
 - Compra
 - Operación
 - Reemplazo
- d) Supervisión y evaluación de:
 - Realización de actividades.
 - Registro de transacciones (autorizadas, exactas, totales, actualizadas).

Nota: Según políticas de cada empresa, los responsables de cada área pueden encargarse de esto último (inciso d); sin embargo, lo ejecutan de manera formal auditores externos o internos.

En la actualidad, la informática se divide en grandes ramas o se integra a otros elementos tecnológicos y administrativos para fortalecer las empresas. Algunos de ellos son:

- Sistemas de información
- Redes locales
- Bases de datos
- Planeación de informática

- Desarrollo de sistemas
- Soporte a usuarios
- Investigación de nuevas tecnologías

La auditoría tradicional ha evaluado los procesos del negocio según enfoques financiero operacional y administrativo; por otra parte, en las instituciones del ramo financiero se contemplan aspectos relacionados con crédito; asimismo, el gobierno efectúa revisiones fiscales, entre otras operaciones.

Las últimas décadas marcaron una pauta en las empresas al incorporar aspectos tecnológicos que les permitieron implantar procesos básicos en sistemas de información computacionales. Esto motivó a los auditores a especializarse dentro del campo de la informática, otros han buscado hacer equipo con los expertos de dicha área para garantizar que los controles y procedimientos continúen llevándose formalmente.

Una función que proviene de la mezcla de dos especialidades como informática y auditoría es la auditoría de sistemas, la cual era válida para los individuos que se dedicaban a la revisión de los sistemas de información en desarrollo, operación y mantenimiento.

Hoy ese término es insuficiente, ya que los elementos de informática susceptibles de revisión y control son muchos y de diversas complejidades. La definición formal para quienes evalúan y verifican políticas, controles, procedimientos y seguridad en los recursos dedicados al manejo de la información es auditoría en informática.

Nota: Estos títulos pueden variar de un país a otro y, a veces, de una empresa a otra; lo importante radica en entender que quien se encuentre en una organización para salvaguardar y proteger la información lo haga con base en un proceso metodológico y formal de revisión.

Los auditores en informática deben encauzar las normas y procedimientos dictados tanto por los institutos de contadores como por las asociaciones de auditoría en informática, que son las instituciones indicadas para normar dicha función.

La seguridad es un conjunto de políticas y procedimientos bien definidos, orientados a proteger el negocio y enfrentar posibles contingencias que pudieran afectar la continuidad de las operaciones o la integridad de los recursos.

Preguntas clave

1. ¿Cómo definiría un sistema de información?
2. ¿Qué es un sistema de información computacional?
3. ¿Qué es auditoría tradicional desde su punto de vista y qué aspectos evalúa?
4. ¿Por qué nace el concepto auditoría de sistemas?
5. ¿Qué es auditoría en informática? Mencione al menos dos definiciones y diga qué áreas evalúa.

6. ¿Cuáles son los alcances de la auditoría tradicional y cuáles los de la auditoría de sistemas?
7. ¿Cuáles son los alcances de la auditoría de sistemas y cuáles los de la auditoría en informática?
8. ¿Qué técnicas utiliza el auditor tradicional?
9. ¿Son válidas en la auditoría en informática? (Explique su respuesta.)
10. ¿En qué radica la importancia de que la auditoría tradicional se especialice en ciertas áreas de la informática?
11. ¿En qué estriba la importancia de que cierto personal de informática se especialice en los aspectos de control comúnmente aceptados para los sistemas de información?
12. ¿Qué habilidades debe tener un auditor en informática? ¿Por qué?
13. ¿Qué técnicas de la auditoría tradicional tiene que conocer y utilizar un auditor en informática?

La auditoría en informática y su entorno

Las actividades de un negocio u organización tienen un efecto directo sobre sectores específicos de la sociedad; de igual manera, los hechos 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; asimismo, una gran cantidad de ellos se han adaptado a los cambios sufridos por los elementos externos y obtenido ventajas competitivas de dichas variaciones que les permiten liderar o al menos mantenerse en el mercado.

El medio suele marcar las pautas y caminos estratégicos en los diferentes aspectos que contempla un negocio y los factores que lo afectan pueden ser:

- Económicos
- Políticos
- Culturales
- Tecnológicos
- Ecológicos
- Sociales
- Organizacionales
- Otros factores

Para los negocios es importante evaluar en forma constante cada factor externo que predomine o los afecte de manera trascendente, con la finalidad de instituir las acciones necesarias para minimizar su impacto negativo o sacar ventaja estratégica del mismo.

Las estrategias de los negocios son definidas formalmente en un proceso de planeación mediante un proceso en que se involucran accionistas, alta dirección y, en

algunas ocasiones, consejeros o consultores expertos en esta relevante actividad para cualquier ente organizacional.

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

Dado que la auditoría en informática es un proceso básico de evaluación y control en el uso de los recursos tecnológicos para el logro de las estrategias, debe contemplar el entendimiento del entorno del negocio como parte de sus actividades primarias.

En ocasiones, la función de auditoría en informática se ve relacionada de modo directo o indirecto con las acciones definidas por la alta dirección, ya sea porque será la responsable de llevarlas a cabo o porque dará seguimiento formal a su cumplimiento. Se dará una explicación a manera de ejemplo en la tabla 3.1.

La forma en que se difunden estas tendencias es variada, aunque por lo general es mediante estándares internacionales o nacionales (asociaciones profesionales nacionales o internacionales), leyes gubernamentales, tratados comerciales entre países, estrategias sugeridas por líderes mundiales de mercado, entre otras instancias.

Es importante señalar que la mayoría de las organizaciones carecen de la función de auditoría en informática y tampoco contratan auditores externos, lo que causa un alto porcentaje de las irregularidades u omisiones que se presentan con relación a las estrategias y políticas definidas por la alta dirección para la función de informática o áreas usuarias.

Los negocios, que se encuentran seguros de adaptarse u obtener ventajas de los factores externos, cuentan con personal especializado en los diferentes aspectos del medio ya mencionado, así como un proceso de planeación formal y actualizado que les permite ser líderes en el ramo específico de su negocio.

Existen funciones como planeación, auditoría, contraloría y auditoría en informática que verifican y aseguran el cumplimiento formal de las estrategias definidas por el negocio.

No contar con estas áreas de aseguramiento y verificación orilla a las empresas a vivir en una constante incertidumbre, ya que los problemas o deficiencias pueden aparecer en cualquier momento.

En conclusión, el medio externo puede ser un factor determinante en el progreso o debilitamiento de un negocio, por lo que es primordial no perderlo de vista.

3.1 El entorno en la informática

Son las características dominantes del mercado en cada una de las ramas o criterios relacionados con la tecnología de informática, que definen el rumbo de la misma en gran parte de los negocios.

Tabla 3.1 Entorno (factores externos)

Factor externo	Acciones de la empresa	Responsabilidad del auditor en informática	Comentarios
Reducción a las cifras monetarias en tres dígitos (por ejemplo, antes 5 000, ahora 5).	Es política de la empresa que todos los documentos y 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 del gobierno.
Auge en el uso de la tecnología de comunicaciones vía satélite.	Se define como estratégico que exista una red satelital entre empresas e entidades de la organización por este medio.	Constatar o recomendar que exista un proyecto de análisis costo/beneficio para la adquisición de los permisos de gobierno, así como la tecnología que se requiera para la implantación de dicha estrategia. Confirmar su implantación adecuada y oportuna.	Con esta acción se obtiene una ventaja competitiva. Permite una integración más eficiente entre las entidades del negocio.
Tratado de libre comercio con uno o más países.	Se define como política de la empresa que cada área o entidad del 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.*	Aparecen en el mercado competidores de alto nivel; los usuarios de los servicios obtienen productos y servicios de mayor calidad, las empresas buscan el liderazgo internacional.

* Aplica para la función de auditoría en informática.

La función de informática ha de estructurar sus servicios y proyectos con base en los requerimientos específicos del negocio, apoyándose en la tecnología de vanguardia que domina el mercado, así como en las tendencias de la misma. El grado de apoyo que se buscará en el medio tecnológico depende en gran medida de la orientación y justificación que se le asigne al enfocarlo a cada estrategia del negocio.

No todo lo que ofrece el mercado como estándares y soluciones tecnológicas garantiza el desempeño eficiente de la función de informática en una organización; el

auditor en informática deberá verificar la existencia de un análisis costo/beneficio en cada proyecto de inversión orientado a la adquisición de nueva tecnología o estándares (normas) para el uso y manejo de la misma. Además, la auditoría en informática mantendrá un proceso de seguimiento de los recursos de tecnología, metodologías, técnicas, procedimientos y políticas de informática que aseguren calidad y productividad en esta área.

El medio informático sufre cambios continuos en algunos de sus elementos, ya sea en hardware, software, telecomunicaciones, etc., debido a la búsqueda constante de soluciones más eficientes en aspectos relativos a desempeño y costos, entre otros. En consecuencia, cualquier área que tenga como objetivo operar o evaluar (que es el caso en estudio), estará dispuesta a ejecutar las acciones pertinentes que aseguren su entendimiento y aprovechamiento para brindar a la organización resultados de alta calidad y la confianza de que la información seguirá cumpliendo los requisitos de control esperados: exactitud, totalidad, autorización, actualización, etc.

En las últimas décadas, el entorno de la informática ha sido uno de los campos con mayor ritmo de crecimiento en todas sus áreas de acción, por lo cual existen:

- a) Mejores equipos de cómputo, ya que cuentan con características nunca antes proporcionadas, como conectividad, escalabilidad, etc.
- b) Lenguajes de programación y paquetes de software más flexibles y dinámicos, que permiten a los desarrolladores de aplicaciones ser más productivos; además de ofrecer 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 e imágenes. Con ello, se ha logrado enlazar diferentes empresas con clientes y proveedores a través de redes locales (LAN), redes metropolitanas (MAN) y redes abiertas (WAN) (siglas en inglés). Se ha obtenido la capacidad de manejar grandes volúmenes de información, velocidad de transmisión y protección de los datos con la aparición del cable coaxial y la tecnología de redes digitales integradas, por ejemplo.
- d) Metodologías, técnicas y herramientas para la administración de la función de informática y la planeación y desarrollo de sistemas que han venido formalizándose y apegándose a los estándares 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 a la misma auditoría en informática.
- e) La integración de especialidades profesionales (ingeniería, auditoría, informática, etc.) en asociaciones profesionales reconocidas formalmente a nivel nacional, como la Asociación Mexicana de Auditores en Informática (AMAI) e internacional, como la Auditors Association, Inc. (EDP) entre otras. Dichas asociaciones proporcionan la oportunidad a las instituciones y organizaciones privadas y de gobierno de tener un contacto directo y oportuno con los

conocedores o impulsores de las tendencias dominantes del medio en sus áreas económica, social y tecnológica, por mencionar sólo algunas.

La tabla 3.2 de la siguiente página presenta algunos comentarios relevantes sobre las características y aportaciones que han surgido en la tecnología de informática, mismos que los negocios deben evaluar para su posible implantación a fin de lograr el máximo de beneficios.

En esta tabla también se lista la contribución e impacto que ha tenido la tecnología de informática en su campo de acción.

Así como el negocio se ve afectado por el entorno tecnológico, lo está también por la política, la economía, la cultura, la ecología, etc., de tal modo que se hace imprescindible que la función de auditoría en informática tome conciencia de la importancia de mantenerse actualizada y enterada del entorno que rodea a los negocios. Para lo anterior se sugiere documentarse mediante:

- Acceso a bases de datos nacionales e internacionales
- Conferencias
- Lecturas de boletines, periódicos o revistas especializadas
- Incorporación a asociaciones o colegios especializados
- Contacto permanente con proveedores líderes de productos y servicios de la tecnología de informática
- Análisis permanente de los procesos básicos de negocio y de sus competidores clave
- Otros

Objetivo(s) del auditor en informática al estudiar el entorno y su impacto en el negocio

La finalidad principal del auditor es evaluar y dar seguimiento oportuno al conjunto de proyectos de auditoría en informática que serán ejecutados en un plazo determinado con el fin de apoyar directa o indirectamente 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 contacto directo o indirecto con la tecnología informática.

Garantizar el apoyo directo a las estrategias del negocio

La auditoría en informática se enfoca en evitar la interrupción de las operaciones del negocio y, al mismo tiempo, busca salvaguardar los activos relacionados de manera natural con el campo de acción de la informática.

Tabla 3.2 Características e impacto de la tecnología informática en el campo de la auditoría

Concepto	Características	Impacto en el proceso de auditoría en informática
Hardware • Mainframes • Minicomputadoras • Microcomputadoras • Portátiles • Impresoras • Dispositivos de almacenamiento • Otros • Telecomunicaciones - Voz - Datos - Imagen - Video	• Elementos físicos y tangibles de la tecnología 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 ha disminuido y sus características de desempeño y portabilidad han mejorado de manera sorprendente: - Almacenamiento - Procesamiento - Portabilidad - Escalabilidad - Conectividad - Otros	Cuando empezaron a surgir las primeras computadoras y se implantaron los sistemas financieros y contables, el auditor utilizó los equipos de cómputo para consulta, captura, proceso y generación de reportes a fin de evaluar y diagnosticar la situación que guardaban dichos sistemas. Actualmente los equipos de cómputo brindan más facilidades al auditor en informática, ya que se pueden evaluar sistemas de información y otros aspectos de interés a través de accesos remotos y en línea. Se pueden utilizar equipos portátiles que permiten auditar cada tarea en el lugar de los hechos. Las facilidades que brindan las comunicaciones y los equipos de cómputo permiten al auditor registrar y monitorear gran cantidad de actividades inherentes al uso de las computadoras y equipos de telecomunicaciones.

(continúa)

Los auditores en informática dirigirán la participación directa y entusiasta del personal de informática y de los usuarios involucrados durante la auditoría.

Cada proyecto de la auditoría se orienta al cumplimiento de normas, procedimientos y estándares, tanto de auditoría como de informática, comúnmente aceptados.

El responsable de la función de auditoría en informática (externo o interno) que revise las diferentes áreas de informática se ha de coordinar con el responsable de la auditoría tradicional (operativa, administrativa, financiera, etc.), la alta dirección (director o gerente general, por ejemplo) y con el responsable de informática mediante reuniones formales y periódicas con objeto de lograr objetivos comunes para el bien del negocio.

Tabla 3.2 Características e impacto de la tecnología informática en el campo de la auditoría (continuación)

Concepto	Características	Impacto en el proceso de auditoría en informática
Software <ul style="list-style-type: none"> • Procesadores de palabras • Hojas de cálculo (u hojas electrónicas) • Graficadores • Diagramadores • Presentadores • Especializado <ul style="list-style-type: none"> - Auditoría - Seguridad - Desempeño • CASE <ul style="list-style-type: none"> - Método - Técnica - Herramienta 	<ul style="list-style-type: none"> • Son los elementos lógicos de la computadora. • Por medio de este elemento se ha logrado la sistematización computacional de los procesos de negocio (tareas operativas, tácticas y estratégicas). • En un nivel más especializado, con la ingeniería de software se ha logrado la sistematización de las actividades del desarrollo de sistemas a través de las computadoras y en gran medida la planeación de sistemas mediante CASE (ingeniería de software asistida por computadora). 	<p>Al surgir la necesidad de evaluar sistemas computacionales que guardaban datos de los estados financieros y contables de la empresa, el auditor se apoyó en personal con especialización en informática, ya que la programación (en lenguajes como COBOL) y el manejo de los equipos de cómputo requería conocimientos específicos.</p> <p>El apoyo que se brindó al auditor fue programar rutinas de control y evaluación de procesos en los sistemas computacionales, o para generar reprocesos y respaldos de la información por auditar.</p> <p>Al aparecer el auditor en informática, éste se perfila como el individuo que domina ambos campos, la auditoría y la informática. Es el enlace ideal para la evaluación, no sólo de sistemas de información, sino también del uso eficiente de todos los recursos, servicios y productos de informática en el negocio.</p>

Resumen

Gran número de empresas ha despertado de su letargo tecnológico y administrativo; han comprendido que el mundo de hoy no sólo exige deseos de hacer las cosas, sino que es un requisito hacerlas.

Todo el trasfondo de esta afirmación lleva a pensar en un cambio de estado organizacional, cultural y tecnológico en cada compañía u organización que presume de serlo.

El primer estado (organizacional) influye directamente en los niveles jerárquicos con sus islas de poder, burocracia o paternalismo correspondientes; impacta de igual manera en las funciones y tareas de los recursos humanos. En la actualidad se requiere



especialización y, también, multihabilidades (es decir, flexibilidad); asimismo, hay que evitar la dependencia y convertirse en autoadministrado.

Deben existir metas con acciones prácticas y redituables a corto plazo, como adelgazar para estar sano, eliminar niveles que generen cuellos de botella, desaparecer los tiempos muertos y convertir las juntas de “yo-yo” en trabajo de equipo, es decir, tomar decisiones de grupo.

El segundo estado (cultural) transforma valores, además de alterar y eliminar mitos, costumbres e ideas regionalistas. Obliga a confrontar marcos de referencia culturales respecto de otras regiones del planeta y tomar decisiones sobre un cambio o estatismo en el ambiente de la organización.

El tercer estado (tecnológico) —que es el estudiado— implica la decisión de invertir y optimizar para crecer.

Entender que se necesita fortalecer la compañía a nivel tecnológico para lograr el avance es una idea muy válida, pero deducir que hay que prevenir y planear para no gastar y fracasar es doblemente aceptable.

No se afirma que si se invierte más en tecnología se llegará más lejos; tan sólo se expone que, al menos, los negocios deben considerarla para permanecer en el mercado. No se puede alcanzar el éxito sin aceptar que las empresas gordas han de adelgazar, que los regionalismos tienen que adaptarse a la globalización y que la informática debe integrarse a la tecnología de clientes, proveedores y, a veces, de ciertos competidores.

El camino ya está marcado: hay que continuar modificando las estructuras organizacionales a estructuras por procesos, reafirmar los valores tomando en cuenta los provenientes de otras culturas y fortalecer la infraestructura y administración de la función de informática.

Por último, hay que considerar algunos elementos que de aplicarse formal y oportunamente facilitarán el reposicionamiento de los negocios:

- Planeación estratégica
- Evaluación permanente de los procesos y flujos de datos del negocio a través de controles inmersos en los sistemas y apoyados en la convicción de que “más vale prevenir que lamentar” impresa en todos los individuos de la organización
- Investigación de mercado
- Estudio y asimilación del aspecto social, cultural, político, económico y tecnológico del entorno
- Compromiso de todos los niveles de la empresa con la calidad y la satisfacción del cliente
- Orientar los recursos a los procesos fundamentales del negocio
- Ver el recurso humano como la pieza clave de la organización

Para finalizar, hay que tener en cuenta que las empresas observan de cerca los pasos de cada uno de sus competidores; aunado a esto, debe considerarse que los

clientes comparan los servicios y productos que les ofrece el mercado con un enfoque crítico y frío.

Si bien el auditor de informática no hará labor de investigación de mercado y probablemente nunca le dará el producto al cliente, contribuye con su granito de arena brindando el siguiente apoyo:

- Evaluación y análisis de la tecnología del medio para facilitar información y, en su caso, sugerir mejoras a la función de informática que sean justificables y redituables
- Estudio de nuevas alternativas del mercado en cuanto a tecnología (nuevo hardware, software, comunicaciones, etc.) que le permitan seguir asegurando y mejorando los controles y procedimientos encaminados a proteger la información y recursos relacionados con la informática

Preguntas clave

1. ¿Qué factores dominantes existen en el medio tecnológico actual que impactan de manera real y significativa los negocios? ¿En qué aspectos lo hacen?
2. ¿Qué tendencias tecnológicas afectarán el ambiente de las empresas en los próximos años y en qué aspectos?
3. ¿Qué beneficios relevantes pueden obtener las empresas de los elementos que brinda la informática en la actualidad?
4. ¿Qué factores del ambiente de negocios (organización, ingeniería, finanzas, etc.) pueden combinarse con la tecnología informática para hacer empresas más competitivas y rentables? Mencione cómo podrían darse dichas relaciones y en qué tipo de empresas.
5. ¿Considera que el auditor en informática debe dedicar parte de su tiempo al análisis de los macrofactores del entorno tecnológico externo que impacten a los negocios? ¿Por qué?
6. ¿Qué acciones recomienda para que los auditores en informática hagan, de ser necesario, un estudio del ambiente tecnológico?
7. ¿El auditor de informática debe analizar las tendencias tecnológicas? ¿Por qué?
8. ¿Cuáles han sido las etapas tecnológicas del hardware? Mencione tipos, generaciones, características, etc.
9. ¿Qué beneficios ha obtenido el auditor de dicha evolución? Lístelos en orden cronológico.
10. ¿Cuáles han sido las etapas principales del software? Enumere tipos, generaciones, características, etc.
11. ¿Qué beneficios ha obtenido el auditor de tal evolución? Anótelos en orden cronológico.

Organización

4.1 Estrategias y cursos de acción para la implantación formal de la función de auditoría en informática

Estrategias

- I) Formalizar la auditoría en informática en la organización a través de:
 - a) Cursos de acción que justifiquen el desarrollo de la función de auditoría en informática en el negocio
 - b) Presentación a la alta dirección del documento de justificación
 - c) Aprobación del proceso por la alta dirección
 - d) Difusión de la auditoría en informática en las áreas relacionadas directa e indirectamente con informática
 - e) Desarrollo del proceso de auditoría en informática en el negocio
- II) Proporcionar a la empresa o institución un proceso de auditoría en informática permanente con el objeto de garantizar a la alta dirección:
 - a) Que la seguridad, políticas y procedimientos que se orientan hacia los recursos de informática y a la información que éstos manejan sean eficientes y confiables
 - b) Apoyo a los objetivos del negocio al tomar decisiones con base en información que cumpla con los requisitos mínimos exigidos por auditoría, como exactitud, totalidad, autorización, actualización, etc. Asimismo, se cumplirán los requerimientos exigidos de calidad y oportunidad
 - c) La verificación del uso de tecnología de vanguardia que requiere y justifica cada área y nivel organizacional dentro del negocio
 - d) La existencia de un proceso de evaluación y justificación de cada proyecto de inversión relacionado con la función de informática

- e) La elaboración y desarrollo formal de un proceso de planeación en informática que se oriente al plan del negocio
- f) El uso formal de metodologías, técnicas y herramientas por el personal de informática para el desempeño eficiente de sus tareas y generador de productos de calidad
- g) Promover que el personal de informática se desarrolle en un ambiente de profesionalismo y de alta productividad tomando como base sus habilidades, conocimientos y perfiles requeridos por la organización

Cursos de acción

1. Lograr que la alta dirección, las áreas o departamentos usuarios y el personal de informática tomen conciencia de la necesidad de contar con una función de auditoría en informática que asegure y oriente el uso eficiente de los recursos involucrados con la misma.
2. Formalizar un procedimiento que contemple la divulgación, asimilación de los planes, objetivos, beneficios y áreas de oportunidad que representa la auditoría en informática para la organización.
 - 2.1 También debe hacerse del conocimiento de los usuarios y del personal el grado de compromiso y participación que se requiere por parte de todos los involucrados en un proyecto de auditoría en informática.
3. Una vez aprobada la creación o contratación de externos para el proceso de auditoría en informática, se procede a la planeación y desarrollo formal del mismo.
4. El proceso de planeación de la auditoría en informática ha de reflejar proyectos que contemplen prioridades para la alta dirección, áreas de oportunidad para el negocio y evaluaciones que la función de auditoría en informática considere fundamentales para el aseguramiento de la calidad y uso eficiente de los recursos de informática y de la información manejada por dichos recursos.
 - 4.1 Los proyectos tienen que cubrir las expectativas que justificaron este proceso en el negocio, lo cual se obtiene involucrando en la planeación de cada trabajo de auditoría en informática a las áreas usuarias y al personal de informática, con el fin de asegurar su entendimiento y compromiso en los proyectos.
 - 4.2 El auditor en informática debe planear, en forma detallada, los proyectos en los cuales será el responsable directo y ponerlos a consideración del responsable del área de auditoría en informática para que les dé su aprobación formal.
 - 4.3 El responsable de la función de auditoría en informática ha de preparar una presentación ejecutiva para que la alta dirección conozca todos los proyectos del área.
 - 4.4 Llevar a cabo una reunión formal con la alta dirección (al menos se incluye al gerente de cada área del negocio y al responsable de más alto nivel de la

función de informática), a fin de presentar cada proyecto de auditoría en informática, que considere los siguientes puntos:

- Antecedentes
 - Justificación
 - Objetivos y alcances
 - Etapas
 - Productos terminados
 - Fechas de revisiones formales e informales
 - Funciones y responsabilidades
 - Costos/beneficios (cantidades aproximadas)
 - Otros que se consideren relevantes para el auditor en informática
5. Coordinar formalmente las visitas y reuniones necesarias con el personal usuario y de informática involucrado en cada proyecto.
 6. Ejecutar de manera formal y oportuna cada proyecto de acuerdo con lo planeado.
 7. Entregar a la alta dirección informes ejecutivos y detallados de cada proyecto aprobados por el comité de trabajo.
 8. Lograr que todas las áreas y niveles involucrados en los proyectos de auditoría en informática reconozcan la importancia que representa el apoyo formal y oportuno que requiere este tipo de proyectos para la implantación de las soluciones emanadas del proceso.
 9. Investigar, analizar, actualizar y formalizar la metodología de auditoría en informática utilizada por el personal de la función, con objeto de orientar los requerimientos actuales y futuros de la organización, tomando en cuenta las políticas, procedimientos y estándares recomendados a nivel nacional e internacional por las asociaciones y entidades profesionales especializadas en el campo.
 10. Capacitar de manera permanente al personal de auditoría en informática.
 11. Desarrollar cada proyecto de auditoría en informática dentro de las normas y estándares nacionales e internacionales sugeridos.
 12. Orientar los esfuerzos de la función de auditoría en informática hacia la búsqueda y logro de soluciones que apoyen los objetivos del negocio.

4.2 Estructura organizacional y funciones de la auditoría en informática

Ubicación jerárquica de la función

La alta dirección de cualquier organización tiene que estar consciente de que la función de auditoría se debe ejercer con el criterio básico de independencia personal

jerárquica, es decir, que el desempeño de las actividades profesionales en el proceso de evaluación y control no debe verse afectado por aspectos emocionales ni de autoridad emanados de los responsables e involucrados en el momento de la auditoría.

En la medida en que la dirección establezca políticas claras que especifiquen que la función del auditor es asegurar el control y la seguridad de todos los elementos relacionados con la informática y que responde a una necesidad de la alta dirección, el apoyo y participación de todas las áreas del negocio fluirá de manera natural. Asimismo, se evitará que esto se convierta en un proceso tenso y complicado, o en una actividad burocrática e improductiva.

Se recomienda ubicar la función de auditoría en informática en un nivel organizacional que le asegure la independencia y soporte requerido de la alta dirección, a fin de contar con una entidad confiable y eficiente.

La falta de una posición organizacional adecuada a las características específicas que la rodean, puede convertirla en foco de frustración e incertidumbre con el paso del tiempo.

El control y la seguridad no pueden establecerse ni supervisarse desde los niveles inferiores de una empresa; su posición debe ser estratégica o por perfiles especiales del negocio, táctico. Nunca se ejercerán desde un nivel operativo; la alternativa es que los haga personal profesional externo.

Si la auditoría en informática es ejercida por personal externo a la empresa, se recomienda que el seguimiento, coordinación, apoyo y aprobación del trabajo efectuado por los asesores externos sea llevado a cabo por la alta dirección (director o gerentes de auditoría y del área de informática).

Tipos de estructuras donde se ubica la auditoría en informática

La auditoría en informática se debe considerar en un alto nivel organizacional, de igual manera que cualquier otra rama de la auditoría tradicional.

La ubicación deseable es subordinada jerárquicamente a una dirección o subdirección, ya sea una dirección administrativa o de informática.

El objetivo primordial para la alta dirección del negocio es asegurar que el desempeño de las actividades de auditoría en informática se ejecuten oportuna y eficientemente, de manera que se logre que los auditores cuenten con:

- Independencia funcional
- Libertad de acción
- Facultad para la toma de decisiones
- Negociación con los niveles gerenciales
- Involucramiento en proyectos de alto impacto en el negocio

En la tabla 4.1 se muestra un panorama general de las características y consideraciones que pueden darse al estructurar formalmente la función de auditoría en informática en la organización.

Tabla 4.1 Grado de soporte por parte de la función de auditoría en informática

Nivel	Características	Ventajas	Desventajas
Nivel estratégico (equipo de apoyo de la dirección)	<ol style="list-style-type: none"> 1. Independencia funcional 2. El proceso de auditoría opera estratégicamente 3. Existe un compromiso permanente con la alta dirección 4. Por lo general se haya en instituciones financieras, de crédito y en varias dependencias de gobierno 5. Personal de auditoría con visión del negocio 	<ol style="list-style-type: none"> 1. Comunicación formal y permanente entre la alta dirección y los responsables de auditoría en informática 2. Apoyo y soporte constante de la alta dirección a la función 3. Objetividad en el desempeño de la función 4. Se establecen de manera formal y a niveles directivos las políticas, controles y procedimientos sugeridos por la función de auditoría en informática 	<ol style="list-style-type: none"> 1. El seguimiento del desempeño de la función por parte de la alta dirección puede ser un proceso complejo 2. En gran parte de las empresas no se acepta la auditoría en informática 3. No existen muchos profesionales con la experiencia, técnicas y habilidades requeridas para ejercer la función de auditoría en informática a un nivel estratégico
Nivel táctico (gerencias, jefaturas)	<ol style="list-style-type: none"> 1. No hay independencia funcional respecto a otras direcciones o gerencias 2. Se encuentra en los diversos sectores de la comunidad, con frecuencia en ciertas instituciones financieras, de crédito, gubernamentales y en un grado menor en el sector industrial y educativo 3. Se limita mucho al estilo de trabajo del nivel superior al que le reporta 	<ol style="list-style-type: none"> 1. La alta dirección la considera una función indispensable para observar el cumplimiento de políticas y procedimientos de informática en el negocio 2. La función tiene contacto con los responsables para la toma de decisiones 3. Existen asociaciones, consultores y escuelas profesionales que impulsan diariamente la formalización de la función, al menos a un nivel táctico 	<ol style="list-style-type: none"> 1. Se debilita el compromiso y soporte de la alta dirección hacia la función 2. El porcentaje de empresas que considera importante contar con una función a este nivel es mínimo 3. No existen muchos profesionales con la experiencia, técnicas y habilidades requeridas para ejercer la función de auditoría en informática a un nivel táctico

Las dimensiones de las estructuras mencionadas en dicha tabla podrán variar de acuerdo con el giro de cada organización, el grado de penetración que tengan los servicios y productos de la función de informática y el estilo de operación de la organización.

Es importante resaltar que en la actualidad existe muy poca difusión y aún menor aceptación por parte de las empresas de la necesidad de contar con una función de auditoría en informática; sin embargo, es factible pronosticar — con un alto grado de certidumbre — que el crecimiento acelerado de las inversiones y proyectos de informática, donde se involucran todas las empresas, forzará a que se tome una decisión al respecto, aunque a la auditoría en informática se le llame aseguramiento de calidad, evaluación de informática o auditoría de sistemas y sea ejercida por personal externo o interno de la empresa.

Una cantidad considerable de empresas aún cuestiona la rentabilidad y productividad de la función de informática. Prueba de ello son las empresas e instituciones donde la función de informática depende de la dirección o las gerencias de recursos humanos, finanzas, manufactura (empresas industriales), etc. y en algunos casos — que resultan increíbles en estos tiempos —, de alguna jefatura de contabilidad o de los usuarios.

Lo anterior muestra la dificultad que encuentra la función de auditoría en informática para ubicarse de manera formal en las empresas, pues la informática, área sobre la cual operar, se encuentra débilmente ubicada.

Estructura organizacional

A menudo la función de auditoría en informática se encuentra ubicada dentro del área de auditoría y en un número menor de empresas o negocios en la función de informática. Es importante señalar lo anterior, ya que el auditor en informática tendrá diferentes alcances y enfoques en el momento de ejecutar su trabajo. Las mismas áreas del negocio tienen una visión distinta de la función, de acuerdo a la dirección o gerencia donde se encuentran (véase tabla 4.2).

Las figuras 4.1 a 4.4 presentan algunas variantes organizacionales donde se puede ubicar la función de auditoría en informática. Los nombres de direcciones, gerencias, jefaturas, etc., son sólo ilustrativos, pues éstos varían de acuerdo con cada negocio.

Funciones de la auditoría en informática

En cualquiera de las estructuras mencionadas hay que asegurar al negocio un conjunto de acciones mínimas que vuelvan rentable la auditoría en informática.

Funciones mínimas

- a) Evaluación y verificación de los controles y procedimientos relacionados con la función de informática dentro de la organización.

Tabla 4.2 Probables escenarios de la función de auditoría en informática

Área de quien depende la función de auditoría en informática	Consideraciones clave de la función en el entorno del negocio	Ventajas/áreas de oportunidad	Desventajas/restricciones
Dirección o gerencia de auditoría (estructura I)	<ol style="list-style-type: none"> 1. Independiente de la función de informática y de las otras áreas de la empresa donde se dará la auditoría en informática 2. Integración de los controles y políticas de informática a los establecidos para las otras áreas del negocio 	<ol style="list-style-type: none"> 1. Objetividad en el desempeño de las auditorías 2. Hay una planeación y desarrollo conjunto de proyectos con las otras áreas de auditoría 3. Se asegura control y seguimiento sobre todos los recursos y proyectos de informática 	<ol style="list-style-type: none"> 1. Las áreas del negocio no aceptan con facilidad ser auditadas o evaluadas por personal de la misma empresa 2. Se corre el riesgo de desconocer el alcance y misión de la informática en el negocio y el apoyo requerido por dicha área
Dirección o gerencia de informática (estructura II)	<ol style="list-style-type: none"> 1. Hay dependencia de tipo funcional hacia el director o gerente de informática 2. El director o gerente de informática debe ser negociador y facilitador para impulsar el proceso de auditoría en informática en todo el negocio, no sólo en su área 	<ol style="list-style-type: none"> 1. Se facilita en alto grado el nivel de apoyo de informática y auditoría en informática 2. Conocimiento formal y oportuno de los proyectos e inversiones de informática 3. Se agiliza el proceso de concientización en el personal de informática en el cumplimiento de políticas y controles 	<ol style="list-style-type: none"> 1. Incertidumbre acerca de que anomalías, carencias e incumplimiento de la función de informática se hagan del conocimiento de la alta dirección de manera formal y oportuna 2. El enfoque de la auditoría en informática es limitarse a ser una entidad que "sugiere, no que controla y asegura"
Personal de apoyo de la dirección general (estructura III)	<ol style="list-style-type: none"> 1. La función se ubica como una entidad estratégica dentro del negocio 2. El responsable de la función debe tener una visión de negocio 3. Hay un compromiso de dar resultados que generen valor agregado 	<ol style="list-style-type: none"> 1. Apoyo permanente de la alta dirección en la difusión e implantación de políticas, controles y procedimientos 2. Las áreas del negocio se comprometen a cumplir las políticas y controles inherentes a informática de una manera formal 3. Se justifica el perfil de ejecutivo del auditor en informática 	<ol style="list-style-type: none"> 1. La alta dirección debe dar seguimiento y autorización formal al desempeño de informática con conocimiento de causa 2. Se reduce el margen de error en cada uno de los proyectos de auditoría en informática al ser evaluados por la alta dirección 3. Se orientan los proyectos de informática

(continúa)



Tabla 4.2 Probables escenarios de la función de auditoría en informática
(continuación)

Área de quien depende la función de auditoría en informática	Consideraciones clave de la función en el entorno del negocio	Ventajas/áreas de oportunidad	Desventajas/restricciones
Función de auditoría en informática ejercida por externos (estructura IV)	1. Los proyectos con los asesores externos deben ser coordinados por la dirección o gerencia de auditoría o informática 2. Se da cuando se carece de la función de informática, o si ésta existe se busca asegurar o validar información relevante para la alta dirección 3. El personal externo ha de contar con amplia experiencia en este ramo y ser reconocido por su trayectoria en el mercado regional o nacional al menos 4. Debe evaluarse su desempeño una vez terminado su trabajo	1. Los despachos o asesores externos por lo general se apoyan en métodos, técnicas y estándares de auditoría en informática comúnmente aceptados a nivel nacional e internacional 2. Son personal de un nivel profesional más que aceptable, debido a su experiencia y constante actualización 3. Existe un compromiso moral y profesional del auditor en informática para ejercer la asesoría de manera ética e independiente 4. Se exigen resultados y beneficios desde el inicio de los proyectos	1. Pueden darse fugas de información 2. Costos altos y difíciles de controlar 3. El tiempo de asimilación de lo que es el negocio puede prolongarse 4. A veces las soluciones y recomendaciones no son las adecuadas para el negocio 5. Si es contratado por el responsable de informática puede estar influido en el momento de elaborar y entregar el informe final de trabajo 6. Se requiere compromiso y participación formal de todos los involucrados

- b) La validación de los controles y procedimientos utilizados para el aseguramiento permanente del uso eficiente de los sistemas de información computarizados y de los recursos de informática dentro de la organización.
- c) Evaluación, verificación e implantación oportuna de los controles y procedimientos que se requieren para el aseguramiento del buen uso y aprovechamiento de la función de informática.
- d) Aseguramiento permanente de la existencia y cumplimiento de los controles y procedimientos que regulan las actividades y utilización de los recursos de informática de acuerdo con las políticas de la organización.
- e) Desarrollar la auditoría en informática conforme normas y políticas estandarizadas a nivel nacional e internacional.
- f) Evaluar las áreas de riesgo de la función de informática y justificar su evaluación con la alta dirección del negocio.

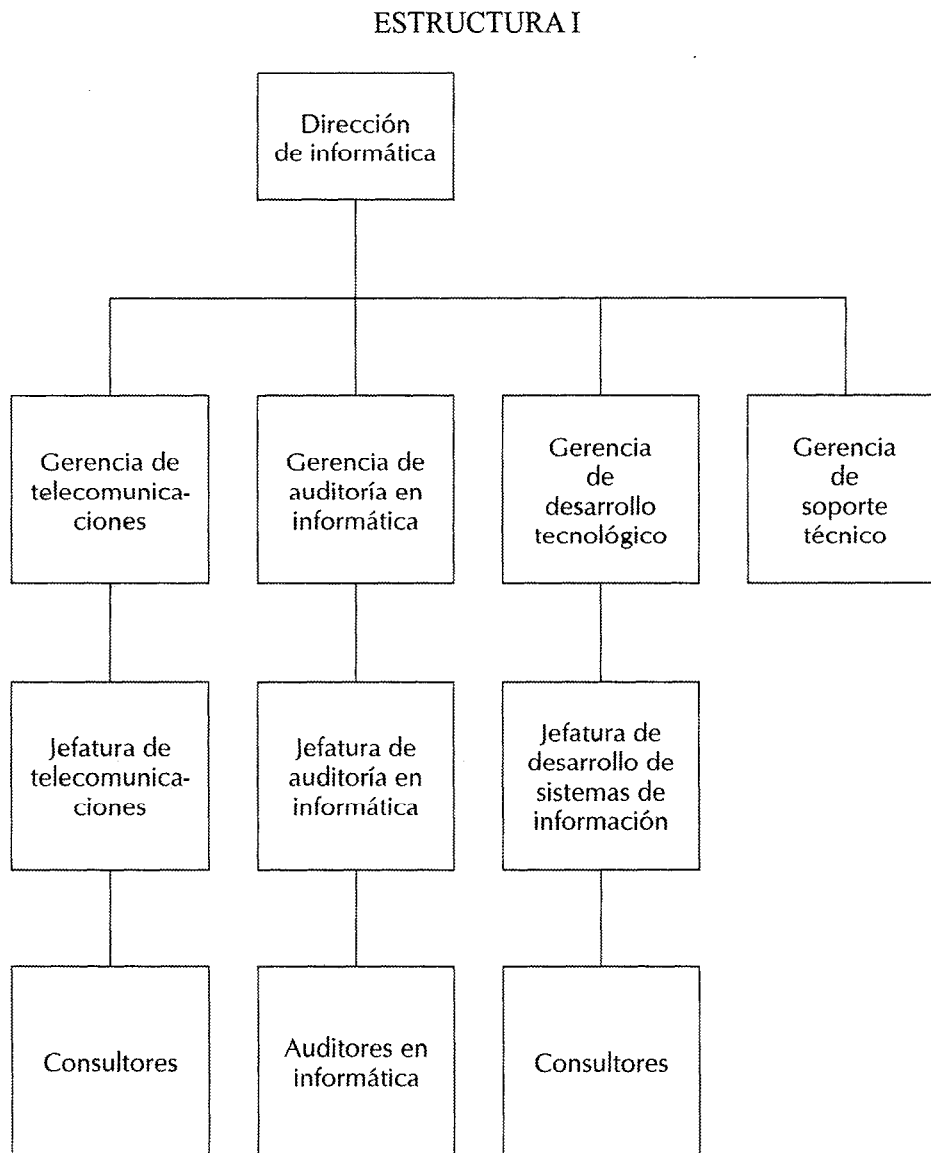


Figura 4.1 Estructura organizacional y funciones de la auditoría en informática.
Soporte al director de informática (estructura I).

ESTRUCTURA II

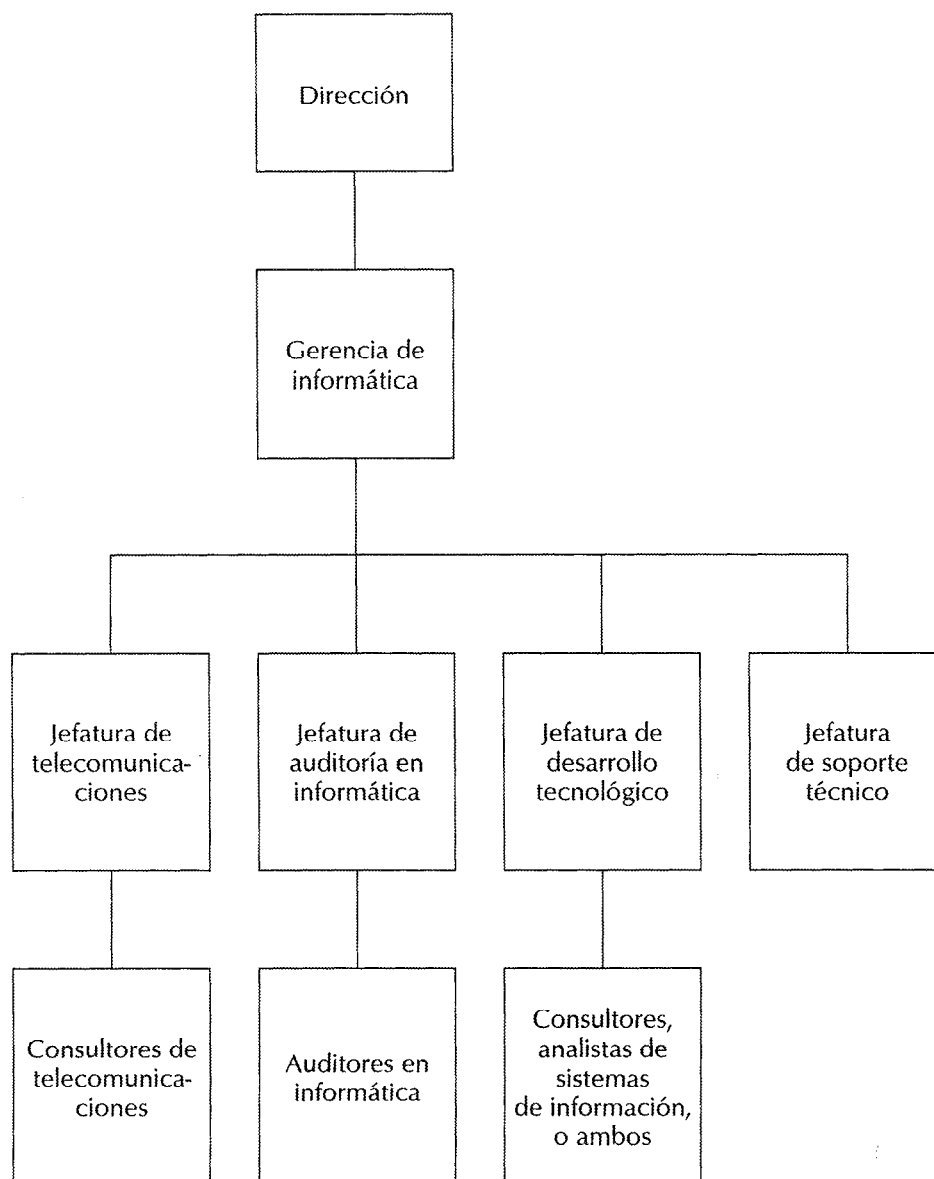


Figura 4.2 Estructura organizacional y funciones de la auditoría en informática. Soporte directo al nivel gerencial de informática (estructura II).

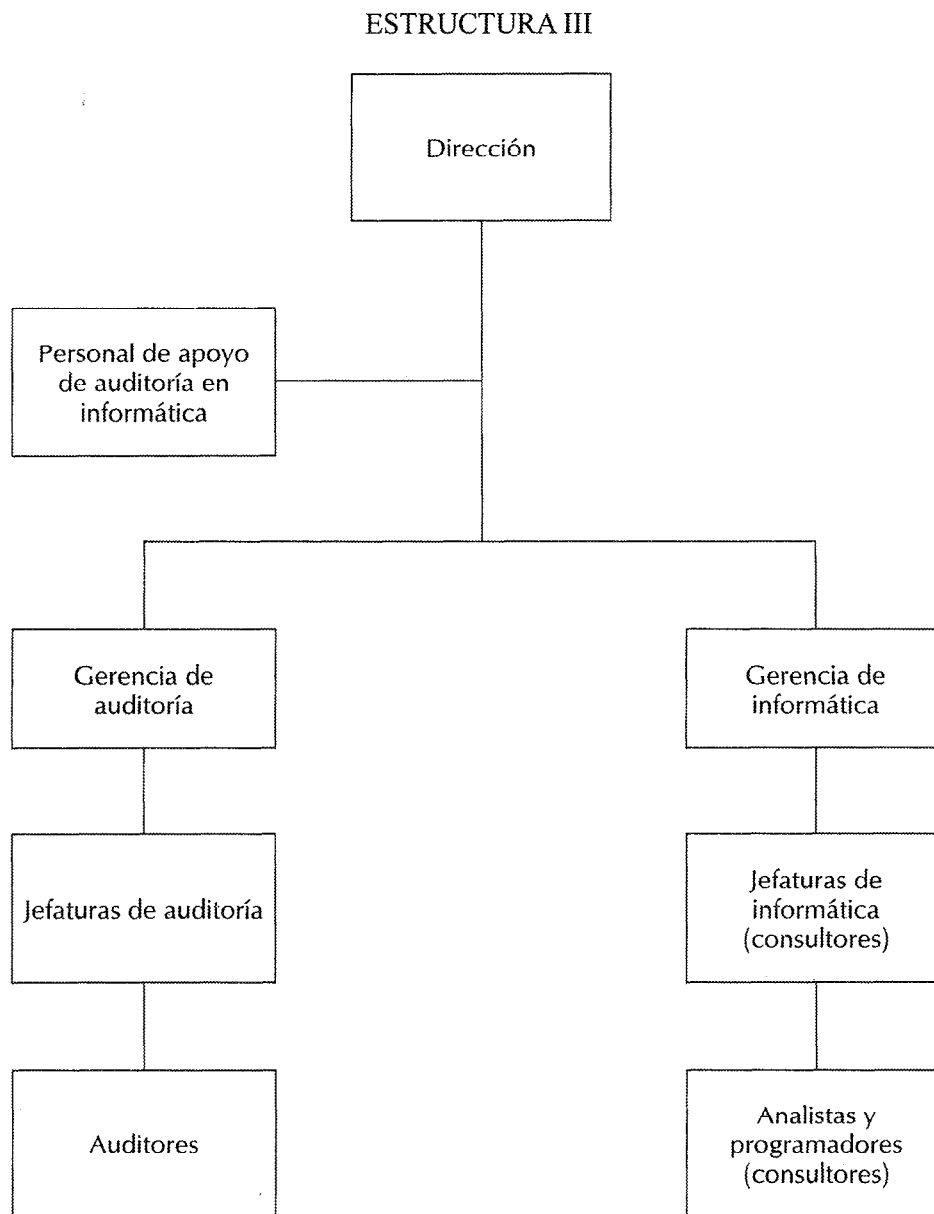


Figura 4.3 Estructura organizacional y funciones de la auditoría en informática. Asesoría y soporte a la alta dirección (estructura III).

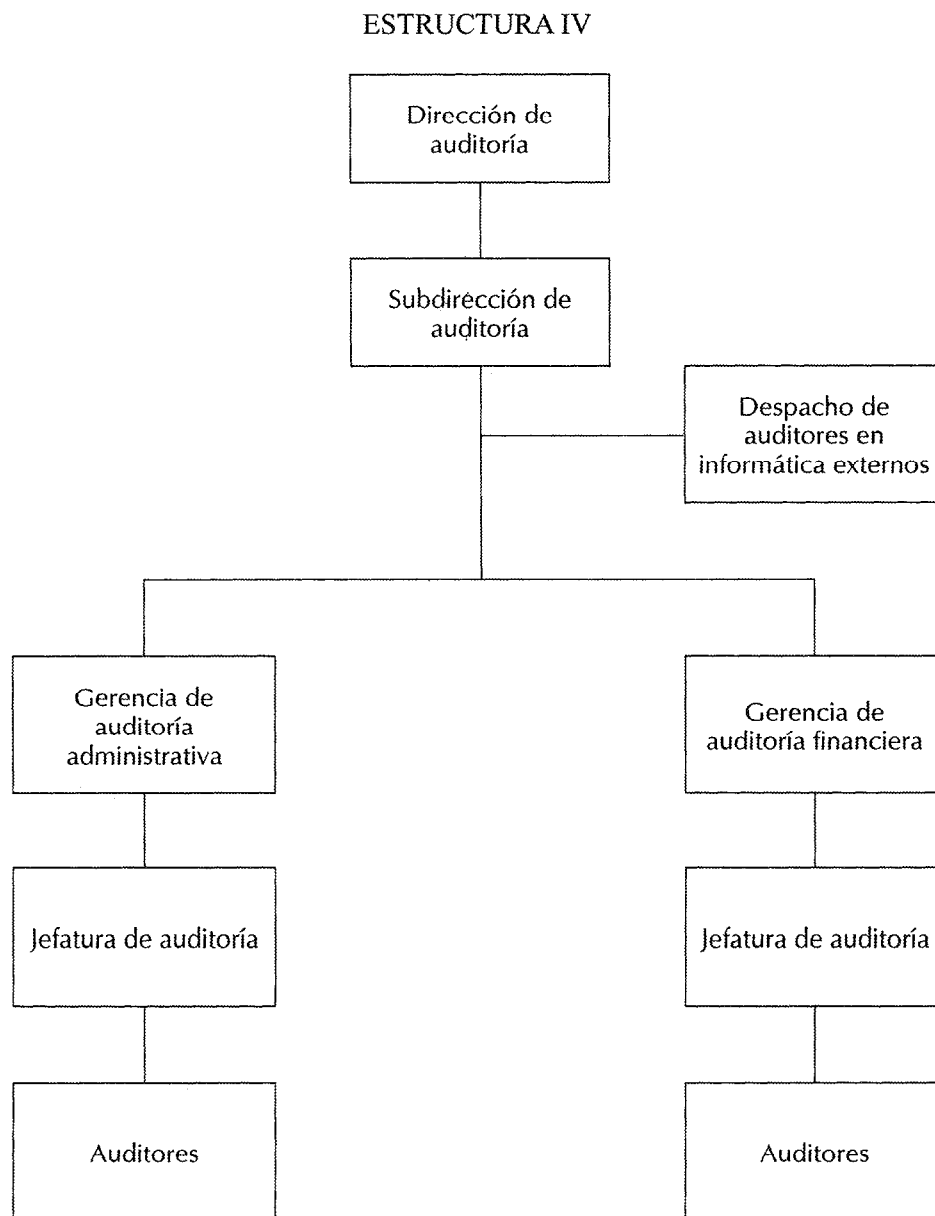


Figura 4.4 Estructura organizacional y funciones de la auditoría en informática. Soporte directo al nivel gerencial de auditoría (estructura IV).

- g) Elaborar un plan de auditoría en informática en los plazos determinados por el responsable de la función.
- h) Obtener la aprobación formal de los proyectos del plan y difundirlos entre los involucrados para su compromiso.
- i) Administrar o ejecutar de manera eficiente los proyectos contemplados en el plan de la auditoría en informática.

Nota: Se debe aclarar que las estructuras y funciones mencionadas sólo son sugerencias ilustrativas y enunciativas, no limitativas.

4.3 Administración de la función de auditoría en informática

Una vez formalizada la función en cualquiera de las situaciones organizacionales señaladas, se define un mecanismo de administración y control de la función.

Dicho mecanismo garantizará que todos los recursos y proyectos involucrados en el proceso de desempeño y gestión de la auditoría en informática, obedezcan los principios básicos de un proceso administrativo. Entre otros, los elementos más importantes e indispensables son la planeación, el personal, el control y el seguimiento del desempeño.

Algunos requisitos indispensables que deben cubrir el responsable y los ejecutores de administrar la función de auditoría en informática se definen en la tabla 4.3. En ésta se mencionan de manera complementaria los requerimientos que han de cumplir los encargados de supervisar y ejecutar los proyectos de auditoría en informática.

Objetivos principales de la administración de la auditoría en informática:

- Asegurar que la función de auditoría cubra y proteja los mayores riesgos y exposiciones existentes en el medio informático en el negocio
- Asegurar que los recursos de informática (hardware, software, telecomunicaciones, servicios, personal, etc.) sean orientados al logro de los objetivos y las estrategias de las organizaciones
- Asegurar la formulación, elaboración y difusión formal de las políticas, controles y procedimientos inherentes a la auditoría en informática que garanticen el uso y aprovechamiento óptimo y eficiente de cada uno de los recursos de informática en el negocio
- Asegurar el cumplimiento formal de las políticas, controles y procedimientos definidos en cada proyecto de auditoría en informática mediante un seguimiento oportuno
- Asegurar que se den los resultados esperados por el negocio mediante la coordinación y apoyo recíproco con:
 - Auditoría
 - Asesores externos

Tabla 4.3 Conocimientos o habilidades requeridos para la administración y desarrollo de la auditoría en informática

Concepto	Responsable de auditoría en informática	Supervisor de auditoría en informática	Auditor de informática
Metodología			
• Planeación de sistemas	Alto	Alto	Bueno
• Desarrollo de sistemas	Mínimo	Alto	Alto
Técnicas			
• Análisis			
– Organizacional	Alto	Alto	Regular
– Sistemas	Bueno	Alto	Alto
– Computacional	Regular	Bueno	Alto
• Diseño			
– Conceptual	Regular	Alto	Alto
– Computacional	Mínimo	Alto	Alto
• Costo/beneficio	Alto	Alto	Alto
• Modelo de datos y procesos	Mínimo	Bueno	Alto
• Documentación			
– Ejecutiva	Alto	Alto	Bueno
– Detallada	Mínimo	Bueno	Alto
• Entrevistas	Alto	Alto	Alto
• Cuestionarios	Bueno	Alto	Alto
• Otras técnicas *			
• Controles, políticas y estándares nacionales e internacionales	Alto	Alto	Alto
• Areas de especialización			
– Comunicaciones *	Regular	Bueno	Alto
– CASE *	Regular	Bueno	Alto
– EDI *	Regular	Bueno	Alto
– Multimedia *	Regular	Bueno	Alto
– Otros *	Regular	Bueno	Alto
• Habilidades o virtudes			
– Creatividad	Bueno	Bueno	Bueno
– Abstracción	Alto	Bueno	Bueno
– Responsabilidad	Alto	Alto	Alto
– Otros *			

* Se ejercerá y exigirá de acuerdo con las características de cada empresa.

- Informática
- Alta dirección

Con el fin de que los objetivos y metas de la función de auditoría en informática se lleven a cabo con éxito, es necesario considerar lo siguiente:

- Elaborar y formalizar los planes de auditoría en informática
- Organizar y administrar la función de manera eficiente
- Dirigir y controlar los proyectos de auditoría en informática con oportunidad
- Revisar y evaluar de manera periódica el desempeño de los auditores en informática
- Evaluar el desempeño de la función de informática
- Otros

4.4 Elementos de la administración de la función

Planeación

La administración de la función debe desarrollar una matriz de la planeación de auditoría en informática para determinar las áreas que serán evaluadas durante cierto período (sistemas de información existentes, desarrollo de sistemas, departamentos usuarios, adquisición e instalación de software, proveedores, etcétera).

Para lograr esto, hay que tener al alcance la información referente a los sistemas, equipos, software, planes de informática, planes de auditoría (financiera, operacional, etc.) que se encuentran contemplados en la actualidad.

Sobre todo, la administración de la función de auditoría en informática debe coordinarse con el gerente de auditoría interna o con los auditores internos para observar, comentar, definir y programar los planes de auditoría en informática conjuntos (a veces no se da tal situación si no existe buena comunicación entre dichas áreas).

De los planes de auditoría en informática emanarán los proyectos específicos para cierto periodo.

Algunos componentes para el éxito de la planeación:

- Juntas formales periódicas para discutir los planes de auditoría en informática y el alcance de los mismos
- Revisiones periódicas y seguimiento de las deficiencias y debilidades importantes que se detecten
- Intercambio de reportes de auditoría y otros documentos orientados a brindar el aseguramiento de calidad
- Proveer la capacitación conjunta necesaria
- Uso de metodologías, técnicas y herramientas comunes

Lo anterior se realiza con el objeto de minimizar la duplicación de funciones, responsabilidades y esfuerzos durante los proyectos de auditoría en informática. Por otro lado, la contratación de asesores externos en este tipo de tareas puede ser un procedimiento efectivo para reducir costos.

Personal

Cada organización debe tener políticas y procedimientos de selección y reclutamiento donde se especifiquen las habilidades y perfiles necesarios para puestos específicos en determinadas áreas de la organización; la selección específica de los auditores en informática es de especial importancia, ya que requiere un nivel de preparación suficiente y confiable en los campos de auditoría e informática. La oportunidad y el grado de evaluación con que se hagan estos procedimientos de selección, aunados a la capacitación que se le brinde al personal de esta función, determinará el grado de calidad, confiabilidad, productividad, etc., con que se ejecuten los proyectos de auditoría en informática.

Cuando se reclute personal de auditoría en informática, la administración de la función debe considerar los atributos y habilidades profesionales inherentes a este tipo de puesto, como experiencia, educación, adaptabilidad, entendimiento, determinación y diligencia.

El gerente o responsable de la función deberá estimar las horas trabajo de auditoría de cada auditor durante un proyecto de evaluación y revisión. El número de auditores se establece con base en la frecuencia de los proyectos o áreas por auditar y el número de horas de auditoría requeridas para cada proyecto.

Control

La supervisión oportuna asegura que las asignaciones a las auditorías sean planeadas apropiadamente para obtener un producto consistente y de calidad. La supervisión puede ayudar en la preparación de los planes de auditoría en informática en el desarrollo y control de los presupuestos de la función, mejorando la relación y comunicación entre las áreas involucradas en los proyectos, así como con el aseguramiento y preparación de papeles de trabajo congruentes y con calidad para elaborar reportes de desempeño.

La supervisión es un proceso continuo, que empieza en la planeación de la auditoría y termina en la entrega y aprobación formal del informe final de la auditoría en informática.

Cuando el supervisor evalúe los trabajos de los auditores en informática sobre los proyectos, debe acudir a los papeles de trabajo y verificarlos con los estándares y procedimientos de la función de auditoría en informática para comprobar el seguimiento de los mismos.

Reportes de desempeño

Son una herramienta muy importante, ya que con ellos el gerente o responsable de la función de auditoría en informática evalúa los siguientes puntos:

- Productividad y calidad de los proyectos
- Resultados
- Avances de los proyectos
- Áreas susceptibles de control y seguimiento
- Seguimiento individual y de grupo

En resumen, para que exista aseguramiento de calidad o un control eficiente de los proyectos, el gerente o responsable de la función debe revisar cada deficiencia encontrada en los reportes de desempeño o en los informes finales de una auditoría.

4.5 Hacia una auditoría en informática eficiente

Los conocimientos, habilidades y capacidades profesionales y personales del auditor en informática tienen una función clave durante el desarrollo de sus tareas.

Conocer teóricamente las normas, políticas y estándares tanto de auditoría como de informática no son garantía de seguridad ni confianza en las áreas sujetas a revisión; en todo el libro se hará hincapié en la importancia de contar con personal experimentado en el campo de la auditoría y la informática.

La experiencia se adquiere con la práctica; disciplina, orden y objetividad son — la mayoría de las veces — factores innatos. Es imposible ocultar la realidad: quien no tenga facultades apropiadas para analizar escenarios de negocio objetivamente, quien no desarrolle habilidades de comunicación y modelación conceptual, quien no sea observador de lo que se encuentre a la vista, quien no tenga capacidad para la toma de decisiones, no podrá ser un auditor en informática eficiente.

Aquí se busca motivar a los buenos analistas, auditores y consultores; es un deseo sincero motivar a quienes quieren serlo para que aprovechen el máximo de sus habilidades, capacidades y cualidades en la realización profesional y eficiente de la auditoría en informática.

Resumen

Las organizaciones, como se ha mencionado, han cambiado dinámica y significativamente la forma de hacer las cosas (enfoque operativo), esto es, de procesos cien por ciento manuales y primitivos se ha llegado a la sistematización y un número cada vez mayor de empresas está automatizando sus actividades básicas.



Se busca tener una empresa con información en línea; en otras palabras, brindar a la alta dirección todos los datos necesarios de cualquier proceso en el momento y forma adecuados para la toma de decisiones.

La manera de planear y administrar las estrategias y tácticas de la empresa (enfoque de negocio) dejó de ser un proceso lento, complejo y de un solo puñado de ejecutivos y se convirtió en un proceso administrable, dinámico, proactivo y visionario a través del apoyo de metodologías organizacionales y herramientas productivas de tecnología informática.

Antes, la planeación flotaba y deambulaba en la mente ocupada y saturada de compromisos de los líderes de la empresa; hoy, es posible tenerla estructurada y estable en una base de datos de negocios.

A simple vista, lo anterior resulta un indicio claro y contundente de que ahora es posible sentarse y disfrutar de los beneficios que la tecnología y ciertas filosofías como la calidad y la reingeniería proporcionan con sólo estirar las manos. Dichos beneficios facilitan el acceso a las empresas de clase mundial.

¿Dónde encaja el auditor en informática en este sorprendente cambio organizacional y tecnológico?

Ninguna empresa que se precie de serlo podrá omitir en el presente o futuro cercano la consideración de tener un proceso formal de auditoría en informática que le garantice todas las metas de negocios basadas en la tecnología. Se invierten muchos dólares, tiempo y riesgos en cada adquisición de los elementos que componen una arquitectura de informática (personal experto, consultores, comunicaciones, equipos de cómputo, software, etc). Las metas son claras: ser líder, mantenerse en el mercado o crecer a corto o mediano plazo a través de la eficiencia de los recursos y la especialización del personal con un enfoque claro de servicio al cliente. Las metas de informática también son claras: apoyar al negocio con una plataforma de tecnología orientada a los principios y estrategias del negocio, con personal y servicios eficientes.

Sin embargo, las metas relacionadas con la seguridad y el control de la creciente infraestructura tecnológica de las empresas y los canales de información carecen, en su mayoría, de un responsable directo.

Las siguientes preguntas podrán ilustrar el comentario anterior.

¿Qué ocurre con la protección de los recursos una vez realizada cada inversión en informática?

¿Quién implantará y revisará los controles de la información alimentada, procesada, almacenada y distribuida por medio de los recursos tecnológicos?

¿Quién será el facilitador entre lo que debe ser y lo que se está haciendo en cuanto a controles preventivos y correctivos que brinden la confianza en la toma de decisiones que emana de los sistemas de información?

¿Quién proporcionará y dará seguimiento formal a la formulación, elaboración, difusión, implantación y mejora del plan total de informática?

Cuando se cuestiona sobre la función de control y demás aspectos de auditoría en informática al responsable de recursos humanos, al encargado de informática o al director de la empresa, se limitan a contestar algunas de las siguientes frases:

“No sé; ¿hay alguien que pueda recomendarme acciones al respecto?”

“¿Es necesario invertir tiempo y gente en eso?”

“Nunca lo había considerado; déjeme valorarlo.”

“Ya pensaré en hacer algo al respecto... cuando termine con los proyectos que tengo.”

“Los auditores; pero como no entienden de informática, no sé quién pueda hacerlo.”

“Tenemos confianza en que cada empleado lo haga voluntariamente.”

“Obvio, los usuarios.”

“Qué pregunta tan ingenua, debe ser el de informática.”

“Los auditores externos... o ¿a quién me sugiere?”

“Si el director no ha creado una función que lo haga, es porque no la necesitamos.”

“¿Controles? Eso es pura burocracia. No pasa nada, no se preocupe.”

“¿Seguridad? ni que estuviéramos en toque de queda.”

“Eso dejémoslo al buen criterio del personal de la empresa.”

Todo eso lleva a concluir que se está ante un problema real. Se habla de la función de control y seguridad como si se tratara de un extinguidor, de comprar un seguro médico o un cinturón de seguridad. Se sabe que se puede contar con ellos; empero, se confía en que las contingencias y problemas no le sucedan a uno.

La rutina y operación diaria absorben el tiempo; sólo un hecho negativo o la visión de un buen negocio hacen posible que tales cuestionamientos apunten al nombre correcto: auditoría en informática. Hay que crearla, formalizarla y permitir que deje descansar tranquilos a los involucrados. Basta entender que todo lo que se encuentra en la empresa tiene un valor real y hay que protegerlo como tal.

Es importante señalar que la mayoría de las empresas medianas y grandes de países desarrollados cuentan con funciones no sólo de auditoría en informática, sino con otras áreas afines como calidad y seguridad (la cual abarca todos los aspectos industriales, tecnológicos y de logística) que combinan de manera alterna. Los niveles donde se ubican tales funciones van desde direcciones hasta procesos fundamentales y confidenciales.

Sin embargo, al echar un vistazo a ciertos países latinoamericanos, sólo un bajo porcentaje de las empresas consideradas grandes cuenta con una estructura sólida y representativa de la auditoría en informática (bancos, secretarías de estado, corporativos y transnacionales). En lo que respecta a las empresas medianas y pequeñas, dicha función es ejercida esporádicamente y, en la mayoría de los casos, nunca se ejecuta. Esto se debe a que se conoce sólo a través de boletines, revistas y, por lo general, “de oídas”.

Lo importante es formalizar una función que revise, evalúe y recomiende acciones de mejora para lograr que cada recurso de informática contribuya a conseguir los objetivos de auditoría tradicionales en cuanto información:

- ✓ Totalidad de los datos
- ✓ Exactitud
- ✓ Oportunidad
- ✓ Actualización oportuna
- ✓ Autorización de las transacciones
- ✓ Seguridad

Por último, es importante señalar que para tener una estructura de auditoría informática eficiente y acorde con las necesidades del negocio, debe considerarse la organización de otras dos áreas que serán su punto de referencia:

Informática

- ☐ Servicios
- ☐ Puestos
- ☐ Funciones
- ☐ Infraestructura implantada en el negocio
 - Equipo de cómputo
 - Equipo de comunicaciones
 - Aplicaciones
 - Software
 - Sistemas en desarrollo
- ☐ Proyectos a corto y mediano plazo

Auditoría

- ☐ Tareas
- ☐ Proyectos de revisión a sistemas de información
- ☐ Apoyo requerido para la utilización de informática en las funciones de evaluación y control
- ☐ Proyectos
- ☐ Otros

Preguntas clave

1. ¿Qué obstáculos organizacionales considera que han existido o existen en las empresas que no cuentan con una función de evaluación y control como la auditoría en informática?
2. ¿Qué factores hacen que una empresa evalúe la necesidad de contar con una función de auditoría en informática?

3. ¿Cuáles deben ser los pasos para implantar un proceso formal de auditoría en informática que quede plasmado organizacionalmente como cualquier otra función del negocio?
4. ¿Qué parámetros del negocio hay que analizar a fin de establecer el alcance de la auditoría en informática?
5. ¿Qué consideraciones deben llevarse a cabo para que — una vez aprobada la función — se determine el nivel jerárquico u ubicación organizacional de la auditoría en informática?
6. ¿Cuáles son las funciones de la auditoría en informática?
7. ¿Qué puestos se requieren?
8. Defina el perfil del personal a cargo.

Planeación

La función de auditoría en informática debe generar, como todas las áreas del negocio, un plan de proyectos que justifiquen su trabajo durante cierto periodo; de igual manera, cada uno de esos proyectos tendrá que contemplar un análisis costo/beneficio y la estructura de los mismos con un enfoque metodológico con el fin de que esta función sea evaluada según su desempeño, con parámetros lo más tangibles y mensurables posibles.

Cada proyecto de auditoría en informática respalda los objetivos y requerimientos de tres entidades del negocio en alto o bajo grado:

a) Alta dirección

- Seguimiento a proyectos relacionados con tecnología informática
- Verificación y aseguramiento del cumplimiento de políticas inherentes a la tecnología informática
- Otros aspectos de interés para la alta dirección

b) Auditoría

- Apoyo en la definición, implantación y seguimiento de políticas, controles y procedimientos de auditoría financiera operativa, de créditos, fiscal, etc., relacionados directa o indirectamente con la tecnología de informática (sistemas de información, equipos de cómputo, comunicaciones, etcétera).
- Planes de capacitación en el uso y entendimiento de software de auditoría, herramientas de productividad (hojas electrónicas, procesadores de palabras, graficadores, diagramadores, etc.), bases de datos (consulta de información, por ejemplo), equipos de cómputo (micros, terminales, portátiles, etc.); otros de interés para los auditores.

Nota: La capacitación sugerida para un auditor de informática no es necesario que sea la misma para un auditor tradicional.

- Otros de interés para el desarrollo eficiente de los auditores cuando evalúan áreas del negocio que se apoyan en informática.

c) Informática

- Apoyo en la definición, implantación y seguimiento de políticas, controles, procedimientos y estándares relativos a la organización y administración de informática, el proceso de planeación, la evaluación y adquisición de nueva tecnología, la evaluación y adquisición de servicios, el desarrollo e implantación de soluciones (EDI, CASE, base de datos, telecomunicaciones, sistemas estratégicos, multimedia, etc.) y otros de interés para informática.

Lo anterior permite concluir que es muy importante la comunicación permanente entre la función de auditoría en informática y la alta dirección, así como con las direcciones o gerencias de auditoría o informática.

A continuación se enumeran algunos puntos que hay que considerar a fin de obtener un plan maestro de auditoría en informática que asegure un apoyo permanente y eficiente a las entidades del negocio antes mencionadas.

1. Crear o formalizar un comité de control y seguimiento integrado por la alta dirección y los responsables directos de auditoría, informática y auditoría en informática.

Nota: La independencia y apoyo que debe brindarse al auditor en informática depende en alto grado de la seriedad y formalización con que el negocio tome esta función; si no se le permite intervenir en las reuniones donde se originan los proyectos y compromisos relacionados con auditoría, informática y alta dirección, el enfoque del auditor puede verse seriamente limitado.

2. Analizar los proyectos de negocio, informática, auditoría y auditoría en informática de manera conjunta, con objeto de ver la relación o impacto que tienen entre sí y facilitar los compromisos que aseguren el cumplimiento de los mismos.

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

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

657-6 : 681.3.06

H55a

Auditoría en informática

Un enfoque metodológico y práctico

técnicas, el respeto a los estándares comúnmente aceptados y el apoyo de la empresa lo llevarán al éxito.

Existen funciones o áreas de informática tradicionalmente auditadas, debido al tiempo y arraigo que tienen en los negocios. Algunas de las más comunes son:

- Sistemas de información
- Planeación
- Desarrollo
- Operación o mantenimiento
- Metodología de desarrollo e implantación de sistemas de información
- Técnicas
- Herramientas
- Seguridad
- Planes de contingencia
- Planes de recuperación en casos de desastre
- Administración de la función de informática
- Planeación de informática
- Organización de informática
- Políticas y procedimientos de informática

Áreas particulares de cada empresa que se pueden auditar durante la fase de desarrollo son:

- Comunicaciones
- Redes locales
- Investigación de tecnología
- Usuarios de informática

Preguntas clave

1. ¿Qué factores debe haber antes de que el auditor en informática inicie la etapa de desarrollo de la metodología de auditoría en informática?
2. ¿Cómo define la etapa de desarrollo?
3. ¿Cuáles son las principales tareas que debe ejecutar el auditor en informática en la etapa de desarrollo?
4. ¿Qué productos importantes emanan de la etapa de desarrollo?
5. ¿En qué radica la importancia de la etapa de desarrollo respecto a las anteriores?
6. ¿Qué problemas generaría no efectuar de manera completa y eficiente la presente etapa?
7. ¿Qué acciones han de realizar los responsables de las áreas usuarias y de informática involucrados en la auditoría para que esta etapa (donde se aplican cuestionarios, entrevistas y visitas) termine con éxito?

8. ¿Es importante tomar en cuenta las políticas y procedimientos de informática comúnmente utilizados y recomendados por las asociaciones profesionales? ¿Por qué?
9. ¿Quiénes participarán en esta etapa y cuál será su función?
10. Explique la función de los siguientes integrantes de la función de auditoría en informática en la etapa de desarrollo:
 - Responsable de la función de auditoría en informática
 - Líder del proyecto de auditoría en informática
 - Auditor en informática
11. ¿Considera que debe participar en la presente etapa personal de auditoría tradicional (operativa, administrativa, financiera, entre otros)? ¿Por qué?
12. ¿Debe intervenir en la presente etapa personal externo (consultores, proveedores, clientes, etcétera)? ¿Por qué?
13. Indique qué técnicas y herramientas ha de utilizar el personal del área de auditoría en informática durante esta última:
 - Muestreo
 - Análisis organizacional/análisis de sistemas/análisis de procesos
 - Observación/inspección
 - Control de proyectos (planeación de tareas y seguimiento)
 - Documentación
 - Análisis costo/beneficio
 - Referente al software de auditoría, al software para oficina (procesadores de palabras, hojas de cálculo, presentadores) microcomputadora
14. Mencione brevemente qué aplicación y beneficios le brindan en la etapa de desarrollo las técnicas y herramientas que seleccionó en la pregunta anterior.
15. ¿Qué restricciones se pueden presentar en la etapa de desarrollo y cómo podría eliminarlas o reducirlas el personal de auditoría en informática?
16. ¿Qué elementos debe contener el plan de implantación de auditoría en informática y por qué?
17. ¿Qué requisitos deben presentarse para que el plan de implantación de la auditoría en informática sea aprobado?
18. ¿Quiénes han de aprobar el plan de implantación de la auditoría en informática y por qué?

Etapa de implantación

Esta fase determinante abarca:

- a) Definición de requerimientos para el éxito de la etapa de implantación.
- b) Desarrollo del plan de implantación.
- c) Implantación de las acciones sugeridas por la auditoría en informática.
- d) Seguimiento de la implantación.

La etapa presente es la más importante para todos los involucrados en el proyecto de auditoría en informática que, por decirlo de alguna manera, termina para los auditores y empieza para los responsables de las áreas usuarias y de informática, ya que ellos ejecutarán las acciones recomendadas en los informes de la alta dirección y detallado aprobados en la etapa anterior. La función del auditor en informática pasa a ser de seguimiento y apoyo.

Tareas, productos terminados, responsables e involucrados de la etapa de desarrollo se especifican en la tabla 12.1.

- Etapa de desarrollo (terminada)
- Etapa de implantación (en ejecución)

La participación del responsable de informática es más directa, pues tendrá la responsabilidad de coordinar a su personal, a los usuarios y quizás a los asesores externos para una implantación exitosa. Sus objetivos principales serán:

- Asegurar que las recomendaciones y plazos de terminación surgidos de los informes de auditoría en informática y aprobados por la alta dirección se lleven a cabo de manera formal y oportuna
- Utilizar los recursos necesarios para lograr una implantación exitosa
- Respetar y cumplir las políticas y procedimientos de seguridad y control emanados de los informes de auditoría en informática

Tabla 12.1 Proceso metodológico de la auditoría en informática: un enfoque práctico

Tabla 12.1 Proceso metodológico de la auditoría en informática						
Etapas	Tareas	Productos	Responsable	Involucrados		
1. Implantación	1. Definir requerimientos para el éxito del plan de implantación	1.1 Recursos requeridos para el éxito de la implantación sugerida por auditoría en informática	RI/PU	LP		
		1.2 Recursos aprobados	AD	RI/PU/LP		
		1.3 Equipo de trabajo para la implantación	RI/PU	LP		
		1.4 Equipo de trabajo aprobado	AD	RI/PU/LP		
		1.5 Funciones y responsabilidades	RI/PU	LP		
		1.6 Fechas de revisión	RI/PU	LP		
		1.7 Productos terminados	RI/PU	LP		
		1.8 Costo/beneficio revisado	RI/PU	LP		
		1.9 Costo/beneficio aprobado	AD	RI/PU/LP		
		1.10 Inicio de la implantación	RI/PU	LP		
2. Desarrollar el plan de implantación detallado		2.1 Plan de implantación revisado según los resultados de la primera tarea	RI/PU	LP/AI		
		2.2 Plan de implantación corregido y actualizado	PI	AI/PU		
		2.3 Documentar plan final	RI	AI/PU		
		2.4 Plan final aprobado	AD	PI/PU/LP		
3. Efectuar implantación sugerida por auditoría en informática		3.1 Inicio del proyecto	PI/PU	RI		
		3.2 Tareas terminadas	PI/PU	RI		
		3.3 Pendientes justificados	PI/PU	AD/RI		
		3.4 Pendientes implantados	PI/PU	RI		
		3.5 Presentación de implantación	RI	AD/RAI/LP		
		3.6 Implantación aprobada	AD/PI/PU	RI/RAI/LP		

(continúa)

(continúa)

Tabla 12.1 Proceso metodológico de la auditoría en informática: un enfoque práctico (continuación)

Etapa	Tareas	Productos		Responsable	Involucrados
Implantación	4. Seguimiento a la implantación del plan recomendado por la auditoría	4.1	Acciones de seguimiento seleccionadas	LP	RAI/AI
		4.2	Seguimiento de la implantación	LP	AI
		4.3	Revisiones informales	LP	AI
		4.4	Revisiones formales	LP	RAI
		4.5	Aseguramiento de calidad	LP	RAI
		4.6	Pendientes revisados	LP	RAI
		4.7	Pendientes aprobados	LP	RAI
		4.8	Seguimiento de pendientes	LP	RAI
		4.9	Implantación exitosa final	LP	RAI
		4.10	Implantación aprobada	RAI	RAI

Nomenclatura: AD = alta dirección, PU = personal usuario, RI = responsable del área de informática, PI = personal de informática, RAI = responsable del área de auditoría en informática, LP = líder del proyecto de auditoría en informática, AI = auditor de informática.

- Otros que el responsable de informática considere oportunos y convenientes para una implantación eficiente

Tal como se mencionó al principio de este capítulo, el auditor en informática tendrá una participación más discreta e indirecta en la etapa de implantación; sin embargo, es fundamental, ya que debe garantizar que se pongan en práctica las acciones de mejoramiento que ha sugerido y en los plazos definidos.

Nota: Cada tarea de la etapa de implantación, al igual que las de la etapa de desarrollo, se explican de una manera uniforme para hacerlas más prácticas e inteligibles; asimismo, se mencionarán las actividades más importantes que llevará a cabo el auditor en informática y los productos terminados mínimos que se deben obtener al finalizar cada una (véase tabla 12.2).

Resumen

Una vez que el auditor revisa las áreas correspondientes y tanto los usuarios como el responsable de informática aprueban formalmente el plan de implantación de auditoría en informática, se establecen políticas, procedimientos y estándares para cada recomendación del informe emanado de la etapa de desarrollo de la auditoría.

Los elementos clave de la etapa de implantación son, entre otros:

- Ejecutar las acciones en los tiempos definidos en el plan de implantación
- Asignar los usuarios o el personal de informática responsables de la implantación
- Apoyo de la alta dirección para que actúen como facilitadores de la implantación
- Seguimiento formal y oportuno de la implantación por parte de los auditores en informática
- Diferenciar y clasificar las acciones inmediatas, a corto o mediano plazo
- Brindar los recursos necesarios para la terminación exitosa de la presente etapa

Un paso anterior a la implantación es difundir en la empresa — con las medidas de confiabilidad requeridas — las principales acciones resultantes de la auditoría en informática realizada. Lo anterior se realiza con el fin de lograr que el personal involucrado en la implantación se haga consciente del objetivo primordial de las acciones correctivas y preventivas que se llevarán a cabo: salvaguardar la integridad de la información del negocio y reducir los riesgos futuros.

Por último, es necesario que los auditores de informática programen revisiones posteriores a la implantación que aseguren a la empresa que va por buen camino, al menos en cuanto al manejo y administración de los elementos de la función de informática.

Tabla 12.2 Actividades y productos terminados del auditor en informática

Tareas	Actividades principales	Productos terminados
Definición de requerimientos para el éxito de la etapa de implantación (la ejecuta el responsable de informática; de ser necesario involucra a los usuarios y auditores en informática)	Analizar qué recursos humanos (asesores internos o externos), materiales (tecnología), financieros (inversiones), etc., se necesitan para ejecutar las acciones recomendadas en los plazos determinados por auditoría en informática	Requerimientos de implantación documentados
Desarrollo del plan de implantación (a cargo del responsable de informática; si es necesario, involucra a los usuarios y auditores en informática)	Documentar dichos requerimientos y, de ser necesario, pedir la aprobación de la alta dirección	Requerimientos aprobados por la alta dirección
	Verificar que se cuente con los recursos estimados en la tarea anterior	Plan de implantación documentado
	Consultar los informes para verificar acciones y tiempos de terminación	
	Elaborar un plan de implantación que tenga al menos:	
	Tareas	
	Productos terminados	
	Responsables	
	Involucrados	
	Fechas de inicio y término	
	Fechas de revisión	
Implantación de las acciones sugeridas por auditoría en informática (la lleva a cabo el responsable de informática, aunque puede involucrar a los usuarios y auditores en informática)	Verificar tareas, productos terminados, etc., del plan de implantación	Plan de implantación ejecutado
	Ejecutar cada una de las tareas de acuerdo con el plan de implantación	

(continúa)

Tabla 12.2 Actividades y productos terminados del auditor en informática (continuación)

Tareas	Actividades principales	Productos terminados
Seguimiento a la implantación (esta tarea corresponde al auditor en informática)	Solicitar el plan de implantación para revisar su congruencia con los informes de la auditoría en informática	Seguimiento del plan de implantación
	Comprobar el cumplimiento formal de las tareas en los tiempos y formas que considere convenientes para asegurar los resultados esperados por él y la alta dirección	Anomalías y debilidades de implantación registradas y comentadas con el responsable de informática o la alta dirección
	Documentar debilidades y anomalías relevantes en la implantación	Implantación de las acciones recomendadas por la función de auditoría en informática
	Sugerir acciones para el cumplimiento de la implantación al nivel que considere pertinente	

Algunas recomendaciones para llevar a buen término dicha revisión son las siguientes:

- Estructurar un plan de visitas rápidas a las áreas más importantes de la función de informática que se evaluaron, para tomar las medidas necesarias que aseguren la correcta implantación de estándares, políticas o procedimientos relativos a informática.

Preguntas clave

1. ¿Qué factores debe haber antes de que el auditor inicie la etapa de implantación de la metodología de auditoría en informática?
2. ¿Cómo define la etapa de implantación de la auditoría en informática?
3. ¿Cuáles son las principales tareas que debe ejecutar el auditor de informática en la etapa de implantación?
4. ¿Cuáles son las principales tareas que ha de realizar el personal de la función de informática en la fase de implantación?
5. ¿Cuáles son las principales tareas que tienen que ejecutar los usuarios de informática involucrados en la auditoría en esta etapa?

6. ¿Qué productos importantes emanan de la etapa de implantación?
7. ¿En qué radica la importancia de la etapa de desarrollo respecto de las anteriores?
8. ¿Qué ocurriría de no efectuarse cabalmente esta etapa?
9. ¿Qué recomendaría para que la revisión posterior a la implantación asegure que todo está correcto?
10. ¿Es importante tomar en cuenta las políticas y procedimientos de informática emanados del proyecto para darle seguimiento? ¿Por qué?
11. ¿Cuál es la función de cada uno de los siguientes integrantes de la función de auditoría en informática en la etapa de desarrollo?
 - Responsable de la función de auditoría en informática
 - Líder del proyecto de auditoría en informática
 - Auditor en informática
12. ¿En la presente etapa debe participar personal de auditoría tradicional (operativa, administrativa, financiera, etc.)? ¿Por qué?
13. ¿Debe intervenir personal externo (consultores, proveedores, clientes, etc.) en la presente etapa? ¿Por qué?
14. Indique cuáles de las siguientes técnicas y herramientas debe utilizar el personal del área de auditoría en informática cuando lleve a cabo dicha etapa:
 - Muestreo
 - Análisis organizacional/análisis de sistemas/análisis de procesos
 - Observación/inspección del control de proyectos (planeación de tareas y seguimiento)
 - Documentación
 - Análisis costo/beneficio acerca del software de auditoría, software para oficina (procesadores de palabras, hojas de cálculo, presentadores) microcomputadora
15. Mencione brevemente qué aplicación y beneficios le brindarían en la etapa de implantación cada una de las técnicas y herramientas que seleccionó en la pregunta anterior.
16. ¿Qué restricciones se pueden presentar en la etapa de implantación y qué ha de ejecutar el personal de auditoría en informática para eliminarlas o al menos minimizarlas?
17. ¿Qué debe presentarse para que el plan de implantación de la auditoría en informática se lleve a cabo formal y oportunamente?
18. ¿Quiénes han de revisar que el plan de implantación de la auditoría se efectúe con eficiencia y por qué?

USO PRÁCTICO DE LA METODOLOGÍA

En este apéndice veremos el uso práctico de las técnicas y herramientas vistas a lo largo del libro.

La etapa de desarrollo del proceso metodológico sugerida en el capítulo 6 y especificada en el 11, así como la tarea de evaluación de las áreas por auditar (tabla 9.4) se basan en las seleccionadas en la etapa de justificación y adecuación (Caps. 8 y 9, respectivamente).

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

Los puntos más relevantes de cualquier metodología de trabajo se han mencionado con amplitud a lo largo de los capítulos anteriores: qué hacer (tareas); quién debe hacerlo (responsables); participantes (involucrados); cuándo hacerlo (secuencia); cómo hacerlo (procedimientos, figuras, comentarios, etc), y dónde hacerlo (diagnóstico de negocio y de informática, matriz de riesgos).

En los apéndices encontraremos información práctica complementaria relacionada con cada una de las áreas de informática que en la actualidad y en los próximos años continuarán siendo valiosas o indispensables en los negocios.

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

Los nombres de las mismas pueden ser similares a los de cualquier organización o incluso idénticos; el aspecto clave es que todo lo que se menciona es lo menos que se ha de buscar en cada una de las áreas que se vayan a auditar dentro de la informática en los negocios.

Una función del auditor en informática es actualizar y adecuar los procedimientos, políticas, estándares, métodos de trabajo, herramientas de productividad, técnicas, etc., a la medida del negocio en que ejerce, con objeto de brindar los resultados requeridos en ese momento.

Componentes que se evaluarán por área de revisión

Los componentes de las áreas de revisión son los inherentes a cada una de las áreas que serán auditadas (véase matriz de riesgos, Cap. 8). La información mínima que ha de buscar el auditor en informática en cada componente comprende:

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

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

En el momento de evaluar los componentes mediante entrevistas, visitas y cuestionarios, se van detectando las áreas de oportunidad emanadas principalmente de las debilidades, carencias o incumplimiento de políticas, procedimientos, métodos y técnicas, entre otros puntos.

Sin embargo, los objetivos principales del auditor son:

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

Políticas y procedimientos por área de revisión

Las políticas y procedimientos de informática son los elementos o dispositivos que al ser ejecutados formal y oportunamente garantizan que las funciones y servicios relacionados con informática se lleven a cabo con eficiencia para el apoyo estratégico, táctico y operativo que requiere el negocio.

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

Tanto las políticas como los procedimientos y acciones mínimas que deben existir en las diferentes áreas o funciones relacionadas con informática se sugieren en la hoja de políticas y procedimientos de control requeridos por área (tabla A.1).

La tabla A.1 sirve de lista de verificación de las políticas y procedimientos que existen en áreas similares de la función de informática dentro del negocio auditado en ese momento.

Nota: El auditor en informática debe tomarla como una referencia y utilizar su criterio y experiencia para saber si los conceptos de la tabla se aplican por completo o hay necesidad de adecuarlos.

Los datos manejados en la hoja de políticas y procedimientos de control por área son los siguientes:

- Acciones recomendadas
- Políticas recomendadas
- Procedimientos recomendados
- Acciones obligatorias
- Políticas obligatorias
- Procedimientos obligatorios

Métodos y técnicas

El auditor debe especificar los métodos y técnicas requeridos para evaluar de manera completa y eficiente las áreas de informática seleccionadas (véase tabla B.1).

Tabla A.1 Políticas y procedimientos de control requeridos por área

Área de revisión:	Nomenclatura (función responsable):	
Administración de informática	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Difundir la misión, objetivos y planes de informática en todo el negocio	O	I
Debe existir un organigrama y una descripción de puestos	O	I
Debe haber un manual de políticas de la función de informática	O	I
Capacitación permanente del personal de la función de informática	R	I
Programas de calidad y productividad por puesto, función y servicio	R	I
Uso de metodologías, técnicas y herramientas estándares a nivel de función	R	I
Elaborar un documento que tenga los parámetros de medición por función	O	I
Evaluar permanentemente cada puesto de acuerdo con los parámetros de medición	O	I
Informática ha de participar en el proceso de planeación del negocio	O	AD/U
Involucrar activamente a la dirección en la planeación de informática	O	I
Elaborar un análisis costo/beneficio por cada proyecto de informática	O	I
Informática debe elaborar un informe de avance a la alta dirección	O	I
Tiene que existir un comité formal de informática, alta dirección y usuarios	O	AD/I/U

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Dirección y niveles ejecutivos	I = informática AD = alta dirección	U = usuarios E = externo
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Misión, objetivos y planes formales del negocio	O	AD
Difusión y entendimiento de los organigramas y funciones del negocio	O	AD/U
Ubicación de la función de informática a un nivel estratégico	R	AD
Involucramiento de la dirección en el proceso de planeación de informática	O	AD/I/U
Políticas y procedimientos de alta dirección para la función de informática	R	AD/I
Comité formal de informática y alta dirección	R	AD/I
Calendario formal de reuniones del comité y resultados esperados	O	AD/I
Parámetros de medición de la función de informática	O	AD/E
Posición formal de la función de informática en la organización	O	AD/E
Funciones y alcances formales de las áreas de informática	O	I/E
Metas, objetivos y planes formales de informática	O	I/AD
Divulgación y aprobación de los planes de informática por la alta dirección	R	AD/I/U
Evaluación periódica del trabajo hecho por la función de informática	R	AD/U

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión: Control interno	Nomenclatura:	
	I = informática AD = alta dirección	U = usuarios E = externo
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Procedimientos formales para el procesamiento de información	O	I/E
Funciones definidas formalmente para el área de informática y los usuarios	O	I/U/E
Procedimientos formales de supervisión permanente de la ejecución de funciones	O	I/U/E
Procedimientos formales que aseguren la totalidad de la información	O	I/E
Procedimientos formales que aseguren la exactitud de la información	O	I/E
Procedimientos formales que aseguren la autorización de la información	O	I/E
Procedimientos formales que aseguren el mantenimiento de la información	O	I/E
Procedimientos formales que aseguren la actualización de la información	O	I/E
Procedimientos formales para el uso adecuado de hardware, software y aplicaciones	O	I/E
Políticas y procedimientos que regulen el uso de recursos externos	O	I/U/AD
Políticas y procedimientos formales para la operación de la información	O	I/E
Procedimientos formales de evaluación y seguimiento de las funciones definidas	O	I/U
Procedimientos formales de evaluación del hardware, software y aplicaciones	O	I/E

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión: Ciclo de desarrollo e implantación de sistemas de información	Nomenclatura:	
	I = informática AD = alta dirección	U = usuarios E = externo
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Metodología formal para el desarrollo de sistemas de información	O	I/E
Técnicas formales para el desarrollo de sistemas de información	O	I/E
Herramientas formales para el desarrollo de sistemas de información	O	I/E
Definición formal de las etapas del desarrollo emanadas de la metodología	O	I/E
Tareas y actividades formales emanadas de la metodología	O	I/E
Funciones y responsabilidades formales emanadas de la metodología	O	I/E
Productos terminados formales emanados de la metodología	O	I/E
Puntos de revisión y aceptación de los productos terminados por etapa	O	I/E
Procedimientos formales para la capacitación en el uso de la metodología	R	I
Capacitar formalmente al personal involucrado en el desarrollo de sistemas	R	I
Procedimientos que aseguren la liga entre planeación y desarrollo	O	I/E
Evaluaciones periódicas de la metodología de desarrollo	R	I/E
Actualización formal y oportuna de la metodología de desarrollo	R	I/E

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión: Sistemas de información	Nomenclatura: I = informática U = usuarios AD = alta dirección E = externo	
	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Uso formal del desarrollo de sistemas de metodología estándar	O	I/E
Uso formal del desarrollo de sistemas de técnicas estándares	O	I/E
Uso formal del desarrollo de sistemas de herramientas estándares	O	I/E
Procedimiento formal para autorizar el desarrollo de cada sistema	O	I/U
Procedimiento que asegure que cada desarrollo emana de la planeación	R	I
Técnicas de análisis y diseño estructurado	R	I/E
Técnicas de programación estructurada para la construcción de sistemas	R	I/E
Técnicas y herramientas para la prueba de sistemas	R	I/E
Procedimiento formal de aceptación de usuarios del sistema desarrollado	O	I/U
Procedimiento formal para la revisión posinstalación del sistema	R	I/E
Formalizar el uso de manuales técnicos, de operación y del usuario	O	U
Procedimientos de captura, validación, actualización y mantenimiento de datos	R	I/E
Procedimientos de evaluación y compra de sistemas hechos externamente	R	I/E

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Mantenimiento	I = informática AD = alta dirección	U = usuarios E = externo
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Registro de todo software, hardware, etc., en el negocio	O	I
Función responsable del control del inventario de informática	O	I
Programas de mantenimiento preventivo para los recursos de informática	O	I
Bitácoras de mantenimiento correctivo para hardware, software, sistemas, etcétera	O	I
Políticas y procedimientos relativos al mantenimiento de la red de comunicaciones	O	I
Procedimientos que indiquen a los usuarios cómo dar mantenimiento preventivo formal	O	I
Evaluación del costo preventivo para su justificación ante los usuarios	R	I
Estadísticas de los costos o pérdidas por falta de mantenimiento preventivo	R	I
Estadísticas que muestren los elementos que requieren más mantenimiento correctivo	R	I
Deslindar responsables directos para el seguimiento oportuno del mantenimiento	O	I
Aprobación formal del mantenimiento a sistemas de información	O	I
Lograr negociaciones con proveedores para que apoyen en el mantenimiento	R	I
Hacer que los costos de mantenimiento correctivo sean bajos y esporádicos	R	I

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Redes locales	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Justificación formal de la instalación de una red	O	I
Planeación formal de las etapas de implantación de la red	O	I
Documento que indique cómo administrar y operar la red	O	I
Presencia de un responsable directo de la administración de la red	O	I
Existencia de elementos que justifiquen el software y sistemas que habrá en la red	O	I
Instalación exclusiva de software original (legalizado) en la red	O	I
Habrà una definición formal de usuarios que tendrán acceso a la red	O	I
Procedimientos que no permitan accesos no autorizados a la red	O	I
Procedimientos de respaldo de la información manejada en la red	O	I
Procedimiento de respaldo del hardware de la red	O	I
Políticas que limiten el uso de la red por perfil de usuarios	O	I
Procedimientos de uso de la red (entrada, operación, salida)	O	I/U
Procedimientos de seguridad al conectarse con otras redes	O	I

(continúa)



Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Telecomunicaciones	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Justificación formal del uso de una red de comunicaciones	O	I/E
Planeación formal de las etapas de implantación de la red	O	I/E
Existencia de un documento que indique cómo administrar y operar la red	O	I/E
Responsable directo de la administración de la red	O	I
Debe haber datos que justifiquen la integración de un equipo a la red	O	I
Se integrarán a la red sólo equipos autorizados por el administrador	O	I
Definición formal de los usuarios con acceso a la red	O	I
Políticas de seguridad para los datos manejados en la red	O	I/E
Procedimientos de respaldo de la información manejada en la red	O	I/E
Procedimiento de respaldo de la tecnología de la red	O	I/E
Políticas que apoyen el mantenimiento y reemplazo de la red	O	I/E
Procedimientos de uso de la red (acceso, transmisión, salida)	O	I/U
Procedimientos de seguridad al conectarse con otras redes	O	I/E

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura (función responsable):	
Hardware	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Plan de evaluación, compra e instalación de hardware	O	I
Análisis costo/beneficio del hardware antes de su compra	O	I/U
Aprobación formal de la adquisición del hardware	O	AD/U
Contrato legal de la compra de hardware que proteja al negocio	O	I
Inventario formal de todo el hardware existente	R	I
Mantenimiento preventivo y un registro del correctivo	R	I
Orientación del hardware comprado para integración con otra tecnología	R	I
Políticas y procedimientos de reemplazo de equipo (justificación)	O	I/U
Políticas y procedimientos de seguridad relacionados con el hardware	O	I
Capacitación y actualización del personal en el uso del hardware	O	I/U
Función responsable de la administración del hardware	O	I
Registro de usuarios responsables del hardware	O	I/U
Registro de ubicación del hardware y los cambios del mismo	R	I

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Software	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Plan de evaluación, compra e instalación del software	O	I
Análisis costo/beneficio del software antes de su compra	O	I/U
Aprobación formal de la adquisición del software	O	AD/U
Contrato legal de la compra del software que proteja al negocio	O	I
Inventario formal de todo el software existente	R	I
Procedimiento de actualización del software y su registro	R	I
Orientación del software comprado para integración con otra tecnología	R	I
Políticas y procedimientos de reemplazo de software (justificación)	O	I/U
Políticas y procedimientos de seguridad relacionados con el software	O	I
Capacitación y actualización del personal en el uso del software	O	I/U
Políticas que verifiquen la originalidad del software instalado	O	I
Función responsable de la administración del software	O	I/U
Clasificación del software y su uso en el negocio	R	I

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Seguridad	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Plan de seguridad total relativo a informática	O	I
El plan ha de ser aprobado por la alta dirección, usuarios e informática	O	I/AD/U
Debe contemplar un plan de contingencias y un plan de reinicio de operaciones	O	I
El plan de contingencias será difundido formalmente y representado	O	I/U
Los aspectos de seguridad se deben orientar a todos los recursos	O	I
Políticas de la alta dirección que impulsen la seguridad	O	AD
Debe involucrarse a todo el negocio en la implantación de la seguridad	O	I/AD/U
Se ha de proteger la seguridad de datos, equipo, tecnología y usuarios	O	I
Las políticas y procedimientos se actualizarán de manera oportuna	O	I
Concientización permanente de la necesidad de aplicar la seguridad	R	I/AD/U
Evaluación periódica del nivel de cumplimiento de seguridad	O	I/E
El costo de la seguridad no será superior al de los recursos protegidos	R	I
Apoyarse en estándares de seguridad nacionales e internacionales	R	I/E

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)

Área de revisión:	Nomenclatura:	
Planeación de informática	I = informática U = usuarios AD = alta dirección E = externo	
Concepto	Recomendada (R) Obligatoria (O)	Función responsable del seguimiento
Comité formal de usuarios e informática	R	I/U
Proceso formal de planeación del negocio (por áreas básicas)	O	U/E
Metodología formal de planeación de informática	O	I/E
Proceso formal de desarrollo de la planeación de informática	O	I/U/E
Análisis costo/beneficio de cada proyecto emanado de la planeación	O	I/E
Aceptación formal de cada proyecto por área del negocio involucrada	O	U
Aceptación de los proyectos de la planeación por la alta dirección	O	U
Técnicas y herramientas formales para el proceso de planeación	O	I/E
Documentación formal del plan de informática	O	I/E
Difusión formal del plan de informática dentro del negocio	R	I
Administración y control formal de los proyectos del plan de informática	O	I
Procedimientos que aseguren la actualización formal de los proyectos	R	I
Involucramiento permanente y formal del comité en el proceso de planeación	O	I/U

(continúa)

Tabla A.1 Políticas y procedimientos de control requeridos por área (continuación)[illegible]

Cuestionarios por componentes

Los cuestionarios son una ayuda muy valiosa para el auditor en informática durante el desarrollo del proyecto, ya que son material elaborado, revisado, adaptado y documentado de manera previa (incluso sirve de base para auditar diferentes negocios o empresas sin perder validez).

Algunas ventajas son:

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

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

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

- Son un punto de referencia que se complementa con entrevistas, visitas para observación directa, juntas, etcétera
- Deben ser evaluados, depurados y actualizados conforme a características de las áreas de informática (planeación de sistemas, desarrollo e implantación de sistemas, investigación de tecnología, seguridad, control interno, automatización de oficinas, redes locales, telecomunicaciones, etc.) con el fin de contemplar todos los aspectos de control y seguridad requeridos justo en el momento de la auditoría en informática
- Las preguntas pueden llevarse en el orden que aparecen o bien en la secuencia y forma que el auditor en informática considere conveniente para el aseguramiento de los objetivos buscados

Se detallan a continuación los cuestionarios recomendados para cada una de las áreas y componentes sugeridos en la matriz de riesgos; sin embargo, los responsables del proyecto (auditor en informática, líder del proyecto) deben ajustarlos a sus necesidades tomando una o más de las acciones que se indican a continuación:

- Agregar una o más preguntas al cuestionario que será aplicado
- Eliminar preguntas que a su criterio no sean aplicables

- Modificar el orden de las preguntas
- Modificar alguna(s) pregunta(s) para adecuarla(s) al negocio
- Agregar algún componente o aspecto no considerado en el cuestionario. Es importante que actualice la matriz de riesgos, agregue las políticas y procedimientos correspondientes, así como los métodos, técnicas y herramientas que debe conocer el auditor en informática para evaluar ese nuevo componente
- Añadir otra(s) área(s) por auditar no considerada(s) en los cuestionarios. Es importante que actualice la matriz de riesgos, agregue las políticas y procedimientos correspondientes, así como los métodos, técnicas y herramientas que ha de conocer el auditor en informática a fin de evaluar esa(s) nueva(s) área(s)

CUESTIONARIOS PARA EFECTUAR LA AUDITORÍA EN INFORMÁTICA POR ÁREAS DE REVISIÓN

Administración de informática

1. Misión y funciones de la informática
2. Organización
3. Servicios
4. Parámetros de medición

Objetivos de esta revisión

- Verificar que exista un uso eficiente de los recursos de informática (personal, tiempo, tecnología y dinero)
- Asegurar que la función de informática cubra los mayores riesgos y exposiciones existentes en el medio informático
- Asegurar que los recursos de informática (hardware, software, telecomunicaciones, servicios, personal, etc.) estén orientados hacia los objetivos y estrategias del negocio
- Confirmar que exista:
 - Elaboración y formalización de los planes de informática
 - Organización y control formal sobre los recursos de informática
 - Dirección, coordinación y control de los proyectos de informática
- Comprobar la existencia de servicios de informática documentados y difundidos en el negocio
- Asegurar que existen parámetros de medición para el desempeño de cada una de las funciones de informática
- Verificar que se lleve a cabo de manera formal la evaluación del desempeño
- Asegurar la existencia de un comité de informática, alta dirección y usuarios clave
- Confirmar la presencia de un apoyo formal a informática de parte de la alta dirección
- Asegurar que informática elabore, formalice, difunda y aplique las políticas y procedimientos relativos a informática de manera permanente

- Verificar que existan metodologías, técnicas y herramientas para cada función
- Comprobar que haya un proceso formal de capacitación y actualización del personal
- Detectar el grado de confianza, satisfacción y respaldo que brinda al negocio la función de informática
- Confirmar que los planes y políticas de informática sean difundidos y conocidos por la alta dirección
- Evaluar el grado de compromiso de la alta dirección con informática para establecer si el apoyo que le brinda es el adecuado

Nota: Esta evaluación se aplica al responsable de informática.

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución satisfactoria de sus actividades. Algunas acciones de apoyo serían:
 - La alta dirección hace del conocimiento de las áreas por auditar que algunas de sus funciones serán revisadas y se requiere su apoyo.
 - Proporcionar la información requerida por el auditor en informática
 - Externar comentarios y sugerencias al auditor

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

Técnicas para obtener y evaluar la información (tabla B.1)

1. Misión y funciones de la informática

Aspectos clave por evaluar

1. ¿Existe un documento formal que describa claramente los siguientes aspectos?
 - Misión de la informática en el negocio
 - Estructura organizacional de la función
 - Funciones dentro de la organización
 - Funciones y actividades por cada puesto existente en el organigrama
 - Planes de informática (a corto, mediano y largo plazo)
 - Políticas y procedimientos de informática
 - Otros
- 1.1 Si no hay tal documento, ¿cuál ha sido la causa o motivo para no hacerlo formalmente (en documento)?
2. En caso de que exista dicho registro, ¿fue comentado con las áreas internas de informática, áreas usuarias y la alta dirección?
3. Si es así, ¿qué procedimiento se utilizó?
 - Juntas
 - Vía memorandos, circulares, etcétera
 - Platicado en una reunión informal
 - Inducción al momento de que el personal de informática ingresa al negocio
 - Otros
4. ¿Fue aprobado por la alta dirección?
5. ¿Está consciente el personal de informática de la importancia de orientar los esfuerzos al cumplimiento formal y oportuno de la misión, objetivos, estrategias, políticas y procedimientos de la función de informática?
6. ¿Se encuentran bien establecidas y entendidas las funciones de informática en la organización?
 - 6.1 ¿Cuáles son desde un punto de vista objetivo y práctico?
 - 6.2 ¿Las funciones ejercidas en la actualidad son las requeridas por el negocio?
 - 6.3 En caso de que se deban actualizar o complementar, ¿cómo las describiría para un apoyo más significativo al negocio?
7. ¿Existe un comité de informática?

Tabla B.1

Métodos, técnicas y herramientas requeridas	Administración de informática	Dirección y niveles ejecutivos	Usuarios de informática	Control interno
Metodología de desarrollo e implantación de sistemas	Sí	No	Sí	No
Metodología de planeación	Sí	Sí	Sí	No
Cuestionarios	Sí	Sí	Sí	Sí
Entrevistas	Sí	Sí	Sí	Sí
Observación/monitoreo	Sí	Sí	Sí	Sí
Análisis/diseño	Sí	Sí	No	No
Trabajo en equipo	Sí	Sí	Sí	Sí
Análisis costo/beneficio	Sí	Sí	Sí	No
Documentación	Sí	Sí	Sí	Sí
Pruebas de auditoría	No	No	No	Sí
Control de proyectos	Sí	Sí	Sí	No
Índices de producción (<i>benchmarking</i>)	Sí	No	No	No

7.1 ¿Quiénes lo integran?

7.2 ¿Cuáles son los objetivos y funciones principales del comité?

2. Organización

1. ¿Hay una estructura formal de informática (manual, documento, etc.) que contemple al menos lo siguiente?

- Organigrama
- Descripción de objetivos, funciones, responsabilidades y métodos de trabajo por cada puesto existente en el organigrama
- Flujos de información entre los diferentes niveles y áreas de informática
- Otros aspectos organizacionales

1.1 Si existe dicho manual o documento, indique cuáles fueron los criterios o procedimientos utilizados para su:

- Definición y elaboración
- Difusión y asimilación por el personal de informática
- Autorización por parte del responsable de informática

1.2 ¿Qué procedimiento utiliza para asegurarse de que todos los elementos señalados en dicho documento sean actualizados y autorizados formal y oportunamente de acuerdo con las necesidades del negocio?

2. ¿En el último año se han presentado cambios a nivel organizacional que afecten de manera significativa el desarrollo eficiente de las actividades de la función de informática?

2.1 Si es así, ¿qué aspectos de la función han sufrido el impacto de dichos cambios?

3. ¿El responsable de informática o la alta dirección tienen planeado algún cambio significativo en la estructura de informática para los próximos doce meses?

3.1 Si es así, ¿qué elementos de la organización de informática se verán afectados?

4. ¿Qué procedimientos se llevan a cabo para minimizar el riesgo de generar hechos negativos de la función de informática derivados de cambios organizacionales o fusiones con otras empresas?

4.1 ¿Cuáles de los siguientes factores negativos se presentan en la función de informática?

- Improductividad
- Falta de motivación

- Áreas de informática desintegradas
- Individuos reactivos y no proactivos
- Falta de planeación estratégica en informática
- Bajos sueldos
- Imagen negativa en el negocio
- Otros

- 4.2 ¿Cuáles considera que sean las causas de cada uno y cómo piensa solucionarlos?
5. ¿Existe un proceso formal de comunicación interna entre el personal de informática?
 - 5.1 ¿Cuál es el sistema?
 - 5.2 ¿Cuáles son las barreras u obstáculos principales de comunicación entre los diferentes niveles y funciones de la función de informática y cómo piensa solucionarlos?
6. ¿Qué tipo de estructura existe: jerárquica, lineal o de red?
 - 6.1 ¿Por qué se decidió que era la más adecuada?
 - 6.2 ¿No se crean cuellos de botella para la toma de decisiones debido a la estructura actual?
 - 6.3 ¿Considera que la estructura actual limita la iniciativa, creatividad y superación profesional de cada uno de los integrantes de su función? ¿Por qué?
 - 6.4 ¿Existen algunas comparaciones con estructuras de empresas similares a nivel local, nacional o internacional para la definición y actualización de su organización? ¿Por qué?
7. ¿En la organización hay áreas usuarias que desempeñen funciones correspondientes a la función de informática?
 - 7.1 Si es así, ¿cuáles son y qué acciones se toman al respecto?
8. Anote los factores básicos para el logro de una administración eficiente de la función de informática.
 - 8.1 ¿Qué acciones ejecuta para llevar a buen término cada uno de esos factores?
9. ¿Qué actividades realiza para asegurar cada uno de los siguientes aspectos administrativos?
 - Organización
 - Planeación
 - Dirección
 - Control
- 9.1 ¿Cuáles son ejecutados de manera informal? ¿Por qué? ¿Cómo piensa eliminar esa debilidad y en cuánto tiempo?

3. Servicios

1. ¿Existe un catálogo de servicios de informática?
 - 1.1 ¿Es congruente con las áreas de la función de informática?
 - 1.2 Si no existe, ¿cómo se enteran los usuarios y la alta dirección de los servicios disponibles?
2. ¿Qué procedimiento se llevó a cabo para elaborarlo?
 - 2.1 ¿Quiénes fueron los responsables?
 - 2.2 ¿Está documentado?
 - 2.3 ¿Se describen los objetivos, alcances, productos terminados, responsables y beneficios de cada uno de los servicios que proporciona informática?
3. ¿Se presentó a la alta dirección para su aprobación?
 - 3.1 ¿Fue aprobado formalmente?
 - 3.2 ¿Cómo se difunden los servicios o funciones de informática a través de la organización?
4. ¿Cuál es el procedimiento para la solicitud de servicios de informática?
 - 4.1 ¿Cómo se asegura el cumplimiento oportuno de los servicios solicitados?
5. ¿Cuál es el procedimiento para la recuperación de costos emanados de cada servicio?
 - 5.1 Cuando los servicios son ejecutados por terceros (asesores), ¿es el mismo procedimiento?
 - 5.2 Si no es así, ¿cómo se lleva a cabo la recuperación de costos?
 - 5.3 ¿La función de informática es vista en la organización como un área que debe producir ganancias o es sólo una prestadora de servicios que recupera costos originados por cada servicio?
 - 5.4 Cuando los gastos son originados por actividades internas (capacitación, equipos de cómputo, adquisición de metodologías, etc.), ¿cómo se recuperan los mismos?
6. ¿Existe un procedimiento definido formalmente para los puntos siguientes?:
 - Actualización del catálogo
 - Eliminación de algún servicio
 - Agregar un nuevo servicio
 - Modificar objetivos, alcances, productos terminados, costos, etcétera
 - Documentación de los cambios al catálogo
 - Revisión de los cambios
 - Autorización de los cambios
 - Difusión del catálogo de servicios de informática en el negocio
7. Cuando existen servicios de informática proporcionados por terceros con un alcance periódico y estratégico en el negocio (planeación de informática, desa-

rollo de sistemas, asesoría al personal usuario, alta dirección o informática, etc.), ¿se integran al catálogo de servicios?

7.1 Si es así, ¿se reflejan los datos que contienen los otros servicios del catálogo proporcionados por el personal de informática del negocio?

Nota: Aquí se le llamó catálogo de servicios por dar un **nombre formal** al documento que contiene todos los servicios (internos y externos) de informática proporcionados a los diferentes usuarios de la organización; sin embargo, el nombre puede variar según el criterio de cada responsable de informática.

4. Parámetros de medición

1. ¿Se tiene un procedimiento formal de seguimiento al desempeño y rendimiento del personal de informática?

1.1 Indique si dicho procedimiento al menos contempla los siguientes puntos:

- Parámetros de medición por puesto
- Parámetros de medición para cada una de las funciones o actividades primordiales de cada puesto
- Objetivos y alcances de cada puesto
- Resultados esperados por cada puesto
- Tiempos esperados para la ejecución formal de cada función o actividad fundamental
- Actividades de control y seguimiento requeridas para cada función (revisiones formales e informales, verificación del cumplimiento de estándares, aseguramiento de calidad, etcétera)
- Responsables de dar seguimiento a cada puesto
- Encuestas a usuarios al final de cada proyecto

1.2 ¿Se documentó formalmente dicho procedimiento?

1.3 ¿Quiénes son los responsables de elaborar, autorizar, difundir y actualizar dicho documento?

1.4 ¿El procedimiento actual fue aprobado por el responsable de la función de informática?

1.5 Si no fue así, ¿cómo se asegura su entendimiento, cumplimiento y actualización conforme necesidades específicas del negocio y del medio informático?

2. ¿Existen fechas predefinidas para la aplicación de los parámetros de medición, o éstos se aplican durante el desarrollo de cada proyecto?

2.1 ¿Se apoyan en asesores externos para la elaboración y aplicación de los parámetros de medición del desempeño de la función de informática?

- 2.2 ¿Se dan a conocer al personal de informática los resultados de las evaluaciones de desempeño, así como los parámetros con que se mide su función?
¿Por qué?
 3. ¿Las funciones de controlar y ejecutar están divididas?
 4. Cuando los servicios de informática son ejecutados por personal externo, ¿se someten a los parámetros de medición definidos en la primera pregunta?
 - 4.1 De no ser así, ¿por qué no se mide su desempeño y calidad de trabajo?
 5. ¿Existe privacidad en los resultados obtenidos de cada evaluación de desempeño?
 6. ¿El personal de informática participa directamente en el proceso de evaluación de su desempeño o sólo se le notifican los resultados de dicha evaluación?
 - 6.1 Cuando no existe un proceso formal de evaluación de desempeño, ¿cómo se justifica a los empleados el aumento de sueldos, ascensos o, en caso contrario, su despido de la empresa o la falta de incremento salarial por periodos largos?
- Nota:** Es conveniente aclarar que en muchas ocasiones los aumentos de sueldo se relacionan de manera directa con factores externos (como los índices inflacionarios) o internos (por ejemplo, aumento de salarios aprobado por la dirección en periodos y porcentajes similares para todos los empleados del negocio).
7. ¿El procedimiento actual de evaluación y seguimiento que se da al desempeño de las funciones es apropiado?
 - 7.1 Si no lo es, ¿dónde radican las principales debilidades?
 - En los parámetros de medición
 - En el cumplimiento de los objetivos, alcances, estándares, etc., de cada puesto
 - En la supervisión y seguimiento de cada puesto en el transcurso de los proyectos o ejecución de los servicios de informática
 - En la evaluación final específica para cada función
 - Otros
 - 7.2 ¿Qué acciones piensa poner en práctica para eliminar las debilidades encontradas?
 8. ¿Existe un análisis costo/beneficio (anual) de la función de informática?
 - 8.1 Si lo hay, ¿quién lo elabora y quién lo revisa?
 - 8.2 ¿Cómo se han comportado las estimaciones de inversión y gastos en los últimos años?
 9. ¿La dirección considera que el apoyo de informática es pobre? ¿Por qué?
 10. ¿Existen políticas formales en la alta dirección relativas a la administración y organización de la función de informática?
 - 10.1 Si es así, ¿quién las formuló?
 - 10.2 ¿Quién las aprobó?
 - 10.3 ¿Quién las conoce en la organización?

- 10.4 ¿Cómo se dieron a conocer?
- 10.5 ¿Las conoce el encargado de informática?
- 10.6 ¿Las acepta todo el personal de informática?
- 10.7 ¿Se actualizan formalmente cuando es necesario?
- 10.8 Se implantan con éxito?
- 11. ¿Las políticas están definidas para cada área o función de informática?
- 12. ¿Definen la pauta en el manejo de proyectos?
 - Evaluación y adquisición de hardware y software
 - Renta de equipo
 - Telecomunicaciones
 - Reclutamiento y capacitación
 - Desarrollo de sistemas
 - Otros
- 13. ¿Existen reportes de desempeño que apoyen la medición de las funciones?
 - 13.1 ¿Están orientados a obtener los siguientes parámetros de medición?
 - Productividad y calidad de los proyectos
 - Resultados
 - Avances de los proyectos
 - Áreas susceptibles de control y seguimiento
 - Seguimiento individual y de grupo

Dirección y niveles ejecutivos

Objetivos de esta revisión

- Detectar el grado de confianza, satisfacción y respaldo que brinda la función de informática al negocio
- Verificar que las bondades y limitaciones de cada uno de los sistemas de información sean percibidos conceptualmente por la alta dirección y que este entendimiento sea congruente con la realidad
- Confirmar que exista una clasificación y entendimiento de los servicios de informática para la alta dirección
- Comprobar que la tecnología de informática (hardware, software, comunicaciones, etc.) se encuentre al alcance de los niveles directivos de una manera amigable y productiva
- Asegurar que la alta dirección tenga al alcance los sistemas de información, los servicios y la tecnología de informática que requiere para la toma de decisiones, el mejoramiento de las actividades de sus funciones, la obtención de un valor agregado por el uso de informática, etcétera

- Verificar que exista un análisis costo/beneficio de la función de informática dentro del negocio
- Comprobar que los planes y políticas de informática sean difundidos y conocidos por la alta dirección
- Evaluar el grado de compromiso de la alta dirección con informática para establecer si el apoyo que le brinda es el adecuado o es limitado

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

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla B.1)

Seguimiento a la función de informática

1. ¿De qué dirección o gerencia depende la función de informática?
2. ¿Existen parámetros de medición de la función de informática (costos de informática vs. ventas, beneficios reales contra esperados, etcétera)?
 - 2.1 ¿De qué manera utiliza la dirección esos parámetros de medición?
 - 2.2 ¿La frecuencia de aplicación de esos parámetros es por proyecto terminado o por periodos?
 - 2.3 ¿Se apoyan en asesores externos para la elaboración y aplicación de los parámetros de medición del desempeño de la función de informática?
 - 2.4 ¿Se dan a conocer al responsable de informática los resultados de las evaluaciones de desempeño, así como los parámetros con que se mide su función? ¿Por qué?
3. ¿La estructura organizacional contempla de manera formal la posición de informática dentro de la empresa, negocio u organización?
4. Con base en qué criterios se ubicó a informática en esa posición?
5. ¿Son suficientes o necesarias para la dirección las funciones existentes?
6. ¿Las funciones de control y ejecución están divididas?
7. ¿Existe una descripción de puestos?
8. ¿Las funciones son congruentes con la estructura organizacional?
9. ¿Cómo se evalúa el desempeño de esas funciones?
 - 9.1 ¿Los objetivos, funciones y actividades de la función de informática son realistas y congruentes con las necesidades de la organización?
 - 9.2 ¿Los salarios corresponden a las funciones del personal de informática (tomando como referencia la responsabilidad y alcance del puesto, sueldos de los niveles similares en la organización, sueldos promedio del mercado en funciones y alcances similares)?
10. ¿La dirección aprueba los planes y avances de los proyectos de informática?
11. Mencione si el personal de informática participa en todos los proyectos relacionados con:
 - Evaluación y adquisición de hardware, software y aplicaciones
 - Definición de estrategias tecnológicas
 - Contratación de asesores externos
12. ¿Existe privacidad entre los acuerdos de la alta dirección e informática?
 - 12.1 ¿La comunicación entre ellos es formal (juntas, memorandos, etcétera)?
 - 12.2 ¿La alta dirección considera al encargado de informática en la toma de decisiones?
13. ¿Es complicado administrar y supervisar la función de informática?
14. ¿Existe un análisis costo/beneficio (anual) de la función de informática?
15. ¿Quién lo elabora y quién lo revisa?

16. ¿Cómo se han comportado las estimaciones de inversión y gastos en los últimos años?
17. ¿La dirección considera que el apoyo de informática es pobre?
18. ¿Existen políticas formales en la alta dirección relativas a la administración y organización de la función de informática?
 - 18.1 Si es así, ¿quién las formuló?
 - 18.2 ¿Quién las aprobó?
 - 18.3 ¿Quién las conoce en la organización?
 - 18.4 ¿Cómo se dieron a conocer?
 - 18.5 ¿Las conoce el encargado de informática?
 - 18.6 ¿Las acepta todo el personal de informática?
 - 18.7 ¿Se actualizan formalmente cuando es necesario?
 - 18.8 ¿Se llevan a la práctica con éxito?
19. ¿Las políticas se definen para cada área o función de informática?
20. ¿Establecen la pauta en el manejo de proyectos los siguientes puntos?
 - Evaluación y adquisición de hardware y software
 - Renta de equipo
 - Telecomunicaciones
 - Reclutamiento y capacitación
 - Desarrollo de sistemas
 - Otros

Comunicación e integración

1. ¿La alta dirección y los niveles ejecutivos conocen la misión de informática en la empresa?
2. ¿Están al tanto de las funciones de informática en la empresa?
3. ¿El área de informática notificó formalmente los conceptos anteriores a la alta dirección?
 - 3.1 ¿Están por escrito?
 - 3.2 ¿Cómo los han difundido (reuniones entre la alta dirección-informática, entre otros)?
 - 3.3 ¿Fueron aprobados formalmente?
4. ¿Existe un compromiso formal de parte de la alta dirección para brindar el apoyo necesario a la función de informática en el cumplimiento oportuno y satisfactorio de sus responsabilidades?
 - 4.1 Si es así, ¿en qué forma se da este compromiso?
 - 4.2 ¿Existe un comité integrado por la dirección e informática?
 - 4.3 ¿Se reúnen periódica y formalmente?
 - 4.4 ¿Cuáles son las funciones de dicho comité?

5. Si no hay comité, ¿quién se responsabiliza de la función de informática por parte de la alta dirección?
6. ¿El nivel del encargado de la función de informática le proporciona suficiente autoridad y proyección en la organización? ¿Lo reconocen los usuarios?
7. ¿Están formalizados estos aspectos?
8. ¿La alta dirección conoce las funciones y responsabilidades de los puestos clave (gerencias, jefaturas) del personal de informática?
9. ¿Cómo difunde la alta dirección las funciones y responsabilidades de informática a través de la organización?
10. ¿Existen sugerencias que considere la alta dirección que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la función de informática?
11. ¿Existen sugerencias para la alta dirección que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la organización por medio de los servicios de informática?
12. ¿Cómo considera el nivel de comunicación entre dirección e informática actualmente? ¿Por qué?
13. ¿De qué manera se asegura que los compromisos, planes, aprobaciones o cancelaciones de proyectos requieren el visto bueno de la alta dirección?
14. ¿Cómo se aseguran de que tanto apoyo y seguimiento como aprobación de la alta dirección a los proyectos de informática sean oportunos y formales?
15. ¿Se cuenta con la planeación estratégica de informática?
 - 15.1 Si es así:
 - ¿Quién la elaboró (participó el usuario)?
 - ¿Quién la evaluó y aprobó?
 - ¿Es a dos, tres, cuatro o cinco años?
16. ¿El plan estratégico se difundió a todos los niveles ejecutivos de la organización?
17. ¿La alta dirección toma en cuenta la planeación?
18. ¿Se entienden los objetivos y alcances del plan?
19. ¿La alta dirección sabe en qué etapa de avance se encuentra esta planeación?

Apoyo a la toma de decisiones

1. ¿Se tiene conciencia en toda la organización de que la función de informática es primordialmente proporcionar un servicio estratégico a las áreas del negocio?
2. ¿Se definieron los productos y servicios con base en las prioridades del negocio o en las prioridades de una de las áreas del negocio?
3. ¿Quiénes participaron en la definición, formalización, aprobación y distribución de los productos y servicios de la función de informática dentro del negocio?
4. ¿La alta dirección considera que los productos y servicios de informática son estratégicos?



- 4.1 ¿Informática ha brindado beneficios palpables al negocio (en ventas, producción, administración, etcétera)?
- 4.2 ¿Se pueden cuantificar los costos/beneficios de informática (por ejemplo de los últimos tres años)?
 - Costos en:
 - Tecnología (hardware, comunicaciones, EDI, entre otros)
 - Software (como paquetes administrativos, SO [sistemas operativos])
 - Sistemas de información
 - Personal
 - Asesoría externa
 - Otros
 - Beneficios en:
 - Sistemas de nivel ejecutivo
 - Sistemas integrales
 - Aumento en ventas (sistema comercial)
 - Automatización de procesos
 - Administración de personal (nómina y sistemas organizacionales)
 - Productividad y calidad
 - Disminución de costos
 - Otros
5. ¿La alta dirección considera que informática sólo apoya las funciones operativas?
 - 5.1 ¿Es una función que trabaja para las jefaturas?
 - 5.2 ¿Brinda apoyo a la toma de decisiones?
6. ¿Justifica el costo (solicitar análisis costo/beneficio)?
7. ¿A qué plazos se proyectaron los productos y servicios de informática (corto, mediano y largo plazo)?
8. ¿Utilizan productos o servicios de asesores externos?
9. ¿Apoyan éstos las estrategias del negocio?
10. ¿Los aprobó la alta dirección?
11. ¿Justifican el costo (solicitar análisis costo/beneficio)?
12. ¿La función de informática de la organización no puede proporcionar estos productos y servicios?
13. ¿Quién monitorea los servicios externos de sistemas?
14. ¿Los sistemas de información son los apropiados para el negocio?
 - 14.1 ¿Son oportunos?
 - 14.2 ¿Tienen los controles adecuados en cuanto:
 - Privacidad, actualización, autorización, totalidad y mantenimiento

- 14.3 ¿Existe un grado aceptable de automatización en los procesos de la organización?
- 14.4 ¿Qué tipo de proceso (manual o automatizado) maneja mayores volúmenes?
- 14.5 ¿Cuál es la causa principal de que los procesos manuales no se hayan automatizado?
- 14.6 ¿Se ha pensado automatizar los procesos manuales en un futuro próximo?
Si no es así, ¿por qué?
- 14.7 ¿Se ha solicitado la automatización formalmente?
15. ¿Se tienen problemas económicos, organizacionales y de otro tipo por el uso actual de informática?
16. ¿Se ha pensado prescindir de este servicio en menor medida y utilizar más los servicios externos?
17. Si el servicio es bueno, ¿se ha pensado en extender o ampliar los servicios en toda la organización?
18. Desde su punto de vista, ¿hay descontento en la empresa por los servicios que brinda informática?
19. ¿Cuál ha sido el apoyo o soporte que brinda la alta dirección a informática?
20. ¿Se involucra la alta dirección en soluciones que requiere implantar informática?
21. ¿La empresa ha brindado las facilidades económicas y tecnológicas que requiere informática?
22. Entre las estrategias del negocio, ¿está incluido el soporte a la función de informática (véanse los planes)?
23. ¿Cómo se evalúan los productos y servicios de la función de informática? ¿Cómo se van a evaluar en el futuro?
24. ¿Tienen una propuesta formal de productos y servicios para los próximos años por parte de informática?
25. ¿Los sistemas de información apoyan estratégicamente los principales procesos del negocio (producción, ventas, administración, otros)?
26. Desde su punto de vista, ¿los sistemas son flexibles y se adaptan a los cambios que requiere el negocio? ¿Su tiempo de adaptación es lento?
27. ¿Qué niveles de análisis utilizan para identificar los procesos y flujos de información relevantes de la organización?
28. ¿Se hizo un análisis costo/beneficio del plan?
29. ¿Está satisfecha la dirección con los resultados de la ejecución del plan?
30. ¿Hay requerimientos o prioridades definidos en el plan como urgentes que no haya satisfecho la función de informática?
31. Si es así, ¿esto ha afectado las estrategias de la organización?
32. ¿Quién definió las prioridades y requerimientos de los usuarios?
33. ¿Quién estableció las prioridades para la secuencia de los proyectos dentro del plan?
34. ¿El proceso de planeación fue un proceso dinámico y benéfico desde su punto de vista? ¿Por qué? ¿Qué sugerencias tiene al respecto?

Usuarios de informática

Objetivos de esta revisión

- 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
- El auditor ha de definir la calidad, oportunidad, utilidad y confiabilidad real de cada sistema de información, mismas que validarán los responsables de informática y los usuarios
- Estudiar el grado de involucramiento de los usuarios en proyectos específicos como desarrollo de sistemas, evaluación y adquisición de paquetes que serán utilizados por los mismos usuarios, etcétera
- Confirmar si existen procedimientos formales para el seguimiento de la comunicación entre los usuarios e informática
- Comprobar si se cuenta con un comité formal integrado por representantes de informática y de los departamentos usuarios
- Detectar áreas de oportunidad donde el usuario requiera el apoyo de la función de informática. Dicho apoyo puede ser por ejemplo la automatización de funciones manuales, implantación de una red, mejoras en el ambiente de telecomunicaciones, automatización de procesos, entre otros

Nota: La evaluación de la factibilidad de implantar esas áreas de oportunidad corresponde a informática y usuarios; el auditor sólo participará en la verificación del cumplimiento de las políticas relativas a este proceso de evaluación.

- Confirmar la presencia de un análisis costo/beneficio de los diferentes productos y servicios que brinda informática a los usuarios
- Constatar que los planes y políticas de informática sean difundidos y conocidos por las áreas usuarias
- Evaluar el grado de compromiso de las áreas usuarias hacia el comité de usuarios e informática (si existe)

Nota: El personal por entrevistar y visitar en esta revisión será gerentes, jefes y auxiliares de las áreas usuarias (o puestos similares) que serán auditadas.

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla B.1)

Comunicación e integración

Aspectos clave por evaluar

1. ¿Las áreas usuarias conocen la misión de informática en la empresa?
2. ¿Saben cuáles son las funciones de informática en la empresa?
 - 2.1 ¿Los usuarios están al tanto de los servicios y productos que proporciona informática?

3. ¿El área de informática ha difundido los conceptos anteriores de manera formal entre las áreas usuarias?
 - 3.1 ¿Están por escrito?
 - 3.2 ¿Cómo los ha difundido (por ejemplo, reuniones con las áreas usuarias)?
 - 3.3 ¿Fueron aprobados formalmente?
4. ¿Hay un compromiso formal por parte de las áreas usuarias para cooperar en lo necesario con la función de informática en el cumplimiento oportuno y satisfactorio de las responsabilidades de esta última?
 - 4.1 Si es así, ¿en qué forma se da este compromiso?
 - 4.2 ¿Existe un comité integrado por los usuarios e informática?
 - 4.3 ¿Se reúne periódica y formalmente?
 - 4.4 ¿Cuáles son las funciones de dicho comité?
5. Si no hay comité, ¿quién se responsabiliza de la función de informática por parte de las áreas usuarias?
6. ¿El nivel del encargado de la función de informática le proporciona suficiente autoridad y proyección en la organización? ¿Lo reconocen los usuarios?
7. ¿Están formalizados estos aspectos?
8. ¿Las áreas usuarias conocen las funciones y responsabilidades de los puestos clave (gerencias, jefaturas) del personal de informática?
9. ¿Cómo se informa a las áreas usuarias acerca de las funciones y responsabilidades de informática en la organización?
10. ¿Las áreas usuarias externan sugerencias que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la función de informática?
 - 10.1 Indique cómo se han expuesto hasta ahora las sugerencias para el mejoramiento de la comunicación e integración con la función de informática:
 - Por teléfono
 - En reuniones formales
 - Otros (especifique)
11. ¿Los usuarios han hecho sugerencias que puedan apoyar los objetivos, estrategias, funciones y responsabilidades de la organización por medio de los servicios de la informática?
 - 11.1 Mencione cómo se han dado las sugerencias para el mejoramiento de la comunicación e integración con la función de informática:
 - Por teléfono
 - En reuniones formales
 - Otros (especifique)
12. ¿Cómo considera el nivel de comunicación que existe entre ustedes e informática actualmente? ¿Por qué?

13. ¿De qué manera se aseguran de que los compromisos, planes, aprobaciones o cancelaciones de proyectos requieran el visto bueno de las áreas usuarias?
14. ¿Cómo se aseguran de que los compromisos de apoyo, seguimiento y aprobación a proyectos de informática para las áreas usuarias se lleven a cabo oportuna y formalmente?
15. ¿Se cuenta con la planeación estratégica de informática?
 - 15.1. Si es así:
 - ¿Sabe quién la elaboró o participó en este proceso?
 - ¿Sabe quién la evaluó y aprobó?
 - ¿Está al tanto de los tiempos de los proyectos (a dos, tres, cuatro o cinco años)?
16. ¿Se difundió el plan estratégico entre todas las áreas usuarias de la organización?
17. ¿Las áreas usuarias cuentan con la documentación de la planeación (al menos de los proyectos en que se involucra como usuario)?
18. ¿Se entienden los objetivos y alcances del plan?
19. ¿Las áreas usuarias saben en qué etapa de avance se encuentra esta planeación?
 - 19.1 ¿Conoce cuáles son los proyectos a corto, mediano y largo plazo donde el usuario deba involucrarse?
 - 19.2 ¿Informática ha explicado los conceptos anteriores a los usuarios?
 - 19.3 ¿Están por escrito?
 - 19.4 ¿Cómo lo ha hecho (por ejemplo, reuniones con los usuarios por escrito o telefónicamente)?
 - 19.5 ¿Fueron aprobados en términos formales?

Proyectos conjuntos

Aspectos clave por evaluar

1. ¿Existen proyectos en su área relacionados directa o indirectamente con la función de informática?
 - 1.1 Si es así, mencione qué tipo de proyectos serán o están siendo desarrollados en conjunto con informática:
 - Capacitación (equipos de cómputo, software, aplicaciones, entre otros)
 - Implantación de sistemas de información:
 - Desarrollo a la medida (*customized*)
 - Compra de un sistema desarrollado por externos
 - Compra de un sistema hecho por externos y desarrollo de módulos complementarios (requerimientos específicos)
 - Legalización del software
 - Estandarización de tecnología

- Elaboración de políticas y procedimientos
 - Otros (especifique)
2. ¿Los usuarios y el personal de informática responsable de las tareas de dichos proyectos los planearon a nivel formal?
 - 2.1 ¿Se han definido etapas, tareas, productos terminados, funciones y responsabilidades, fechas de reuniones, actividades de aseguramiento de calidad, etc., de cada uno de los proyectos?
 - 2.2 ¿El proceso utilizado para la elaboración y formalización de los proyectos se basa en alguna metodología formal empleada por informática o en las demás áreas del negocio?
 - 2.3 En caso de que exista lo cuestionado en el punto 2.1, ¿lo aprobaron todos los involucrados?
 3. ¿Los proyectos mencionados en la pregunta 1.1 concuerdan con la planeación de informática y los planes de trabajo de las áreas usuarias?
 - 3.1 ¿Qué procedimiento o actividad se realiza para verificar dicha congruencia?
 - 3.2 En caso de incongruencias entre los planes, ¿qué acciones se ponen en práctica?
 4. Mencione si existe una función responsable de los planes conjuntos de usuarios e informática para las siguientes tareas:
 - Elaboración, difusión, actualización, documentación y seguimiento de proyectos conjuntos
 - 4.1 Si es así, ¿qué actividades básicas realiza para cada una de las tareas señaladas?
 - 4.2 ¿Quién y de qué forma da seguimiento al cumplimiento oportuno y formal de tales tareas y actividades?
 - 4.3 ¿Se registran las anomalías detectadas en dicho seguimiento?
 - 4.4 En caso de que la pregunta 4 sea negativa, ¿de qué manera se asegura de que las tareas de elaboración, difusión, actualización, documentación y seguimiento de los proyectos conjuntos se ejecuten de manera formal y oportuna?
 5. ¿El proceso de planeación de proyectos conjuntos se efectuó por medio de los compromisos emanados del comité de informática?
 - 5.1 Si no hay un comité de usuarios e informática, indique cómo se integró a los equipos de trabajo para:
 - Definición de requerimientos
 - Detección de áreas de oportunidad
 - Definición de objetivos y alcances de proyectos conjuntos
 - Estimación de tareas, responsables y tiempos de cada proyecto

- Análisis costo/beneficio
 - Otros aspectos relacionados con el proceso de planeación
6. En caso de que no existan planes formales para los proyectos conjuntos de usuarios e informática, indique cuáles son los medios utilizados para:
- Comunicación de requerimientos de las áreas usuarias
 - Proyectos propuestos para el incremento de la productividad en las áreas usuarias por parte de la función de informática
 - Acciones específicas de apoyo a las diferentes funciones y niveles de las áreas usuarias del negocio
 - Otros aspectos de integración de proyectos de los usuarios e informática
7. ¿En los últimos tres años ha participado formalmente en algunos de los proyectos de informática mencionados a continuación (enciérrelo[s] en un círculo)?
- Desarrollo de la planeación de informática
 - Definición de objetivos, requerimientos y estrategias del negocio
 - Definición de la situación tecnológica actual
 - Definición de la tecnología propuesta
 - Definición de la planeación final de informática
 - Desarrollo, compra o adecuación de algún sistema de información
 - Definición del alcance del proyecto
 - Análisis y especificación de requerimientos
 - Diseño
 - Generación de códigos y pruebas modulares del sistema
 - Pruebas de aceptación del sistema
 - Liberación (transición) del sistema
 - Revisión de posimplantación
 - Proyectos de capacitación en el uso y aprovechamiento de los recursos de informática
 - Proyectos de investigación (como equipos de cómputo, software, aplicaciones de tipo específico, automatización de oficinas)
 - Evaluación y adquisición de hardware y software
 - Definición de requerimientos
 - Evaluación de las propuestas de los proveedores (sólo los puntos de interés para los usuarios)
 - Selección y aprobación de la propuesta apropiada
 - Pruebas
 - Aprobación de la implantación
 - Desarrollo de planes de contingencia y recuperación
 - Definición

- Aprobación
- Difusión
- Simulacros para probarlos
- Actualización
- Auditorías en informática (si se han aplicado a su departamento)
 - Presentación del plan de auditoría
 - Participación en el desarrollo de la auditoría
 - Asistencia a la presentación del informe final de auditoría (aplica a gerentes o subdirectores)
- Otros proyectos (especifique)

7.1 Mencione qué aspectos relevantes emanaron de esos proyectos en lo relativo a:

- Calidad esperada
- Productividad esperada
- Costos esperados
- Beneficios esperados
- Otros

7.2 Si participó en alguno de los proyectos anteriores, señale qué opina de lo siguiente:

- Su participación ¿fue oportuna y suficiente?
- ¿Se documentó, difundió y aprobó de manera formal cada proyecto?
- Indique si se especificaron claramente los siguientes puntos:
 - Objetivos y alcance del proyecto
 - Objetivos y alcance de su participación durante el proyecto
 - Etapas del mismo
 - Sus funciones y responsabilidades en cada etapa
 - Los productos terminados de cada proyecto
 - Especificaciones para la revisión y aprobación de cada proyecto
- ¿Qué beneficios obtuvo su área (funciones/tareas) al término de los proyectos?
- Si no participó formalmente en estos proyectos, ¿a qué cree que se debió?

7.3 ¿Qué podría comentar para el mejoramiento del desarrollo de dichos proyectos desde su inicio hasta la terminación?

Administración de los recursos de informática

Aspectos clave por evaluar

1. ¿Hay procedimientos relativos a la administración de los recursos de informática que se encuentran en las áreas usuarias?

- 1.1 ¿Están definidos en algún documento formal o se ejecutan de acuerdo con el criterio de cada usuario?
- 1.2 En caso de que no exista procedimiento alguno de administración o control de recursos de informática, ¿cómo se asegura la eficiencia y buen uso de los mismos?
2. Indique cuál de los siguientes recursos de informática tiene en su departamento, área u oficina:

Concepto	Cantidad
• Microcomputadoras	
• Servidores para redes locales	
• Impresoras:	
- Láser	
- De otro tipo	
• Equipos para telecomunicaciones (módems, controladores, etcétera)	
• Manuales de sistemas de información, de paquetes de software, otros)	
• Disquetes de:	
- Procesadores de palabras	
- Hojas electrónicas	
- Graficadores	
- Presentadores	
- Diagramadores	
- Otros de uso específico	
• Dispositivos de almacenamiento	
- Discos	
- Cintas	
- Otros	
• Papelería	
• Otros	

3. Indique si hay una responsabilidad directa de parte de cada uno de los usuarios en lo que se refiere a:
 - Justificación de la tecnología de informática que requiera (equipo, software, etcétera)
 - Definala
 - Verificación de que el software instalado en su equipo sea legal
 - Definala
 - Aprobación del hardware o software que se instale en su departamento, área u oficina
 - Definala
 - Actualización de los paquetes de software que maneja
 - Definala



- Actualización tecnológica del hardware
 - Definala
 - Depuración de los discos duros o espacio en disco
 - Definala
 - Respaldo de información
 - Definala
 - Otros (especifique cuáles y cómo ejecuta dicha responsabilidad)
4. En los casos de la pregunta 3, ¿qué acciones de administración se llevan a cabo para cada uno de ellos, cómo se efectúan dichas acciones y quién las realiza si el usuario no es el responsable de ellas?

Proceso	Acciones	Cómo se ejecutan	Quién las lleva a cabo
<ul style="list-style-type: none"> • Justificación de la tecnología de informática que requiera (equipo, software, otros) • Verificación de que el software instalado en el equipo sea legal • Aprobación del hardware o software que se instale en su departamento, área u oficina • Actualización de los paquetes de software que maneja • Actualización tecnológica del hardware • Depuración de los discos duros o espacio en disco • Respaldo de información • Otros (especifique cuáles) 			

5. ¿Tiene algunos comentarios o sugerencias respecto a la administración de los recursos de informática localizados en su departamento, área u oficina?

Grado de satisfacción

Aspectos clave por evaluar

1. ¿La función de informática ha difundido los productos y servicios que ofrece a los usuarios?
2. Si es así, ¿cómo los difundieron en su área?
3. ¿Utiliza actualmente alguno de esos productos o servicios?

4. ¿Qué opina de los productos o servicios que usa?
5. ¿Algún requerimiento de su departamento no es apoyado por los productos y servicios de la función de informática?
6. Si es así, ¿se ha solicitado a informática que satisfaga estas necesidades?
 - 6.1 ¿Ha sido formal esta petición (memorando, solicitud de servicio, etcétera)?
 - 6.2 Según su opinión, ¿se da atención oportuna y formal a las solicitudes de servicios que emite?
 - 6.3 ¿Cuáles motivos aduce el encargado de informática cuando el servicio no es oportuno?
 - 6.4 ¿Existe una disponibilidad aceptable por parte de informática para la implantación de soluciones requeridas y justificadas por el usuario? ¿Por qué?
 - 6.5 ¿Cuál es la principal problemática de la función de informática en cuanto:
 - El procedimiento (formal o informal) existente para la recepción de solicitudes de servicios o productos de informática
 - Tiempos de respuesta en la planeación, desarrollo e implantación de soluciones
 - Capacidad profesional por parte del personal de informática
 - Otros (especifique)
 - 6.6 ¿Considera que el personal de informática es proactivo en el desempeño de las funciones de servicio que apoyan a las áreas usuarias? ¿Por qué?
 - 6.7 ¿Tiene alguna(s) sugerencia(s) para mejorar los servicios y productos de informática?
7. Responda a la siguiente tabla con base en el servicio y facilidades que se han brindado a su departamento en los últimos dos o tres años.*
8. ¿Informática le brinda cursos de capacitación?
 - 8.1 ¿Son formales; es decir, cuentan con calendario y material de cursos, equipos de cómputo, talleres (salas, audiovisuales, etcétera)?
 - 8.2 ¿Se efectúan a solicitud expresa del usuario, como una propuesta de informática o ambos?
 - 8.3 ¿Son congruentes con los recursos y necesidades de su departamento?
 - 8.4 ¿Se programan y notifican a usted con anterioridad?
 - 8.5 ¿Tiene alguna(s) sugerencia(s) a este respecto?

Control interno

Objetivos de esta revisión

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

Concepto	Calif E R M N/A	Comentarios
a) Comunicación		
b) Difusión de planes y políticas de informática		
c) Soluciones Integradas		
d) Grado de cumplimiento de lo planeado en relación con lo implantado		
e) Entendimiento de las expectativas de los usuarios por parte de la función de informática		
f) Beneficios reales a sus funciones (información):		
1) Oportunidad		
2) Confiabilidad		
3) Privacidad		
4) Calidad		
5) Utilidad de la información para la toma de decisiones		
g) Opinión acerca de la tecnología de informática actual:		
1) Equipos de cómputo		
2) Paquetes de software		
3) Sistemas de información en operación		
4) Comunicaciones		
5) Otros (especifique)		
h) Opinión del grado de seguridad existente referente a:		
1) Equipos de cómputo		
2) Paquetes de software		
3) Información (datos)		
4) Otros recursos		
i) Solución a los problemas relacionados con el uso de la informática en su área		
j) ¿Cómo ve la evolución de la informática en los últimos años (tres o cuatro)?		
k) ¿Qué resultados ha dado su intervención en los proyectos de informática?		
l) ¿Qué calificación otorga al servicio actual que recibe de informática?		
m) ¿Cómo califica la calidad y capacidad técnica del personal de informática que le da servicio en la actualidad?		
n) ¿Cómo califica los planes y proyectos futuros de la función de informática?		

Concepto	Calif				Comentarios
	E	R	M	N/A	
o) ¿Cómo califica la tecnología de su empresa respecto a la de la competencia?					
p) ¿Cómo califica la imagen de la función de informática en el negocio?					
q) ¿Cómo califica el apoyo que brinda su departamento a la función de informática?					
r) ¿Qué tanto conoce el personal de su departamento sus funciones y responsabilidades en el manejo y administración de los recursos y datos del medio informático?					
s) Su opinión sobre los costos que se derivan del uso de los productos y servicios de informática					
t) ¿Cómo califica el grado de conocimiento que tiene la función de informática respecto de las funciones y actividades de los departamentos usuarios?					

* Véase la posibilidad de aplicarlo a varios usuarios.

+ E = excelente B = bueno M = malo N/A = no aplica (o no sabe)

- Evaluar la existencia de políticas y procedimientos requeridos para el desempeño eficiente de cada una de las funciones de informática:
 - Administración de la función de informática
 - Telecomunicaciones
 - Planeación de informática
 - Soporte a usuarios (capacitación, asesoría en hardware, software, aplicaciones, etcétera)
 - Desarrollo e implantación de sistemas de información
 - Mantenimiento de sistemas de información
 - Operación de sistemas de información
 - Investigación de tecnología relacionada con informática
 - Automatización de oficinas
 - Seguridad
 - Auditoría en informática
 - Aseguramiento de calidad
 - Otras específicas del negocio
- Verificar y asegurar el cumplimiento oportuno y formal de las políticas y procedimientos relacionados con la función de informática
- Confirmar la existencia de controles y procedimientos formales para el uso adecuado de los datos y recursos tecnológicos de informática

- Comprobar y asegurar el cumplimiento oportuno y formal de las políticas y procedimientos relacionados con el manejo de los datos del negocio a través de sistemas de información y de recursos de la función de informática como equipos de cómputo y telecomunicaciones
- Implantar y dar las recomendaciones necesarias para que se eliminen las debilidades y falta de controles detectados durante esta revisión
- Asegurar que dichos controles y procedimientos cumplan con los objetivos, propósitos y sugerencias conocidos generalmente a través de institutos y asociaciones profesionales a nivel nacional e internacional

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

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

1. Formalizar el apoyo de la alta dirección al auditor en informática con el fin de brindarle las facilidades necesarias para la ejecución de su trabajo. Algunas acciones de apoyo serían:
 - La alta dirección hace del conocimiento de las áreas por auditar que algunas de sus funciones serán revisadas y se requiere su apoyo
 - Proporcionar la información requerida por el auditor en informática
 - Externar comentarios y sugerencias al auditor

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

Técnicas para obtener y evaluar la información (véase tabla B.1)

Políticas y procedimientos

Aspectos clave por evaluar:

1. ¿Existen políticas y procedimientos formales (aprobados por el responsable de informática, la alta dirección o de la auditoría en informática relativos a la administración de cada una de las funciones de informática)?
 - 1.1 Si es así, menciónelas en el formato de la página siguiente, explicando brevemente en qué consiste cada una y las acciones que ejecuta para asegurar

Área/función	Políticas y procedimientos	Descripción y objetivos	Acciones para cumplimiento (seguimiento)
Administración de la función de informática			
Administración de telecomunicaciones			
Administración de redes locales			
Planeación de informática			
Soporte a los usuarios (capacitación, asesoría, entre otras)			
Desarrollo e implantación de los sistemas de información			
Mantenimiento y actualización de los sistemas de información			
Operación de sistemas de información			
Investigación tecnológica			
Automatización de oficinas			
Seguridad			
Auditoría en informática			
Aseguramiento de calidad			
Otras específicas del negocio			

Concepto	Acciones de control
Administración de la función de informática	
Telecomunicaciones	
Planeación de informática	
Soporte a usuarios	
Desarrollo e implantación de sistemas de información	
Mantenimiento de sistemas de información	
Operación de sistemas de información	
Investigación de tecnología relacionada con informática	
Automatización de oficinas	
Seguridad	
Auditoría en informática	
Aseguramiento de calidad	
Otras específicas del negocio	

que se difundan, se entiendan, se cumplan y se les dé seguimiento formal y oportunamente.

- 1.2 ¿Qué acciones o actividades se llevaron a cabo para asegurar que tanto políticas como procedimientos cumplan los propósitos específicos del negocio, así como los estándares, políticas y procedimientos sugeridos por las asociaciones e institutos profesionales para cada uno de los conceptos mencionados?

Nota: El auditor en informática debe evaluar el grado de estandarización y congruencia que guardan las políticas y procedimientos del negocio con las generalmente aceptadas a nivel nacional e internacional.

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, ¿cuáles son las tareas y actividades que lleva a cabo? ¿En qué periodos efectúa dicha evaluación? ¿Qué tipo de informes presenta y a quiénes los entrega? ¿Cómo se da seguimiento a sus recomendaciones?
 - 2.2 ¿Dicha función comprueba el grado de actualización que requieren esas políticas y procedimientos para satisfacer los objetivos de control requeridos por el negocio?

3. ¿Qué acciones de control se realizan cuando algunas de las siguientes funciones no cuentan con políticas y procedimientos que aseguren al negocio que la implantación, operación de tales servicios y productos no alteran la integridad, veracidad ni confiabilidad requerida en el manejo de la información del negocio?
4. ¿Existe una adecuada segregación de funciones para el desarrollo de cada uno de los conceptos mencionados?

Nota: El auditor en informática ha de apoyarse en todos los cuestionarios contemplados en este capítulo para asegurar que los datos manejados por medio de los diferentes recursos de informática aseguren la integridad, veracidad y confiabilidad de dicha información.

AUDITORÍA DURANTE EL CICLO DE DESARROLLO E IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN (SOLUCIONES DE NEGOCIO)

1. Metodología
2. Técnicas
3. Herramientas
4. Capacitación y actualización

Objetivos de esta revisión

- 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)
- Confirmar que el personal de desarrollo de sistemas de información conozca dicha metodología, con el fin de que se asegure calidad y productividad durante el desarrollo de los sistemas de información
- Evaluar el nivel de estandarización que contiene dicha metodología con respecto a las comúnmente aceptadas en el mercado para el CDISI (fases, tareas, actividades, productos terminados, funciones y responsabilidades, revisiones, aseguramiento de calidad, entre otras)
- Exponer las recomendaciones pertinentes para que dicha metodología satisfaga las necesidades de desarrollo e implantación de sistemas de información
- Comprobar que exista un proceso formal de capacitación para el entendimiento y manejo satisfactorio de la metodología por todo el personal responsable de los proyectos de desarrollo e implantación de sistemas de información (aplicable a personal de nuevo ingreso)
- Verificar que exista un curso de orientación básica enfocado al personal involucrado en los proyectos que no pertenecen al área de desarrollo y que, sin embargo, desempeñan una función importante en este tipo de proyectos (usuarios, alta dirección, auditores, por mencionar algunos)

Nota: Esta evaluación ha de aplicarse al responsable de informática o a los responsables del desarrollo e implantación de sistemas.

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (tabla B.1)

1. Metodología

Aspectos clave por evaluar

1. ¿Existe en su área una metodología formal de desarrollo e implantación de sistemas?

- 1.1 ¿Dicha metodología contempla qué hacer, quién debe hacerlo y cuándo debe hacerse durante los proyectos de desarrollo e implantación de sistemas?
2. Si es así, ¿cubre los pasos y lineamientos requeridos para la siguiente clasificación de proyectos?
 - a) Planeación de sistemas de información a desarrollar e implantar (a corto, mediano y largo plazo)
 - b) Desarrollo de sistemas
 - c) Compra de aplicaciones de mercado
 - d) Adaptación de aplicaciones adquiridas a externos (aplicaciones de mercado)
 - e) Rediseño de sistemas existentes
 - f) Implantación de sistemas
 - g) Aseguramiento de calidad
3. ¿Está documentada formalmente dicha metodología?
 - 3.1 Si es así, ¿la documentación contempla al menos cada uno de los siguientes puntos?*
 - Un panorama general de la metodología
 - Equipos de trabajo sugeridos de acuerdo con el tipo de proyecto
 - Etapas de la metodología
 - Tareas de cada etapa
 - Secuencia de las etapas y tareas
 - Responsables e involucrados en cada etapa y tarea
 - Productos terminados por cada etapa o tarea
 - Requerimientos técnicos y administrativos para el cumplimiento de cada tarea
 - Revisiones formales e informales sugeridas para cada etapa
 - Duración estimada de cada etapa
 - Consideraciones para proyectos especiales:
 - Desarrollo con productos CASE (alto y bajo nivel)
 - Implantación del sistema de información en una nueva tecnología
 - Otros
 - Otros que el auditor o el responsable de informática consideren importantes
- 3.2 ¿Cómo se asegura un compromiso formal, un desarrollo y seguimiento eficiente, así como la aprobación final de los proyectos si no se cuenta con una metodología formal que contenga lo mencionado en las preguntas 2, 3 y 3.1?
4. En caso de contar con una metodología de desarrollo e implantación de sistemas, ¿la misma fue desarrollada por el personal de informática de la empresa, fue comprada o la rentan cuando se requiere?

* El auditor en informática verificará que la documentación de la metodología abarque los diferentes proyectos mencionados en la segunda pregunta.

5. ¿Se capacitó al personal de desarrollo en el manejo y uso práctico de la misma?

5.1 ¿La capacitación fue impartida de manera formal?

- Por grupos de trabajo
- Individual
- Con casos prácticos (o proyectos piloto)
- ¿Se evaluó el grado de asimilación de la metodología? ¿Cómo?
- Otros aspectos

5.2 Si no se capacitó al personal en el uso de la metodología, ¿cómo se asegura su entendimiento y uso eficiente durante los proyectos?

6. ¿Desde cuándo la están usando?

Etapa	Tarea	Producto	Responsable
Planeación de sistemas * Nota: esta etapa puede apoyarse en el proceso de los siguientes planes: • Plan del negocio (Véase Cap. de Planeación) • Plan de informática (véase Cap. de Planeación y el cuestionario correspondiente)	1. Modelo de sistemas del negocio • Manuales • Computacionales • Interfaces 2. Datos estratégicos 3. Procesos estratégicos • Manuales • Computacionales • Interfaces 4. Tecnología 5. Organización 6. Requerimientos de sistemas de información 7. Planeación de sistemas a corto, mediano y largo plazo 8. Planes aprobados	1. Planes de sistemas de información por desarrollar e implantar a corto, mediano y largo plazo aprobados 2. Compromiso ejecutivo	Responsable de informática/líderes de proyectos Alta dirección/ responsables de las áreas usuarias
Preliminar*	1. Definición del proyecto 2. Alcance y requerimientos del proyecto 3. Etapas y duraciones estimadas 4. Productos terminados esperados 5. Análisis costo/beneficio esperado 6. Aceptación formal del proyecto 7. Elaborar el plan general del proyecto	1. Modelo conceptual del proyecto 2. Alcance del proyecto 3. Necesidades del proyecto 4. Estudio económico 5. Proyecto aprobado 6. Plan general del proyecto	Líder del Proyecto / asesores externos Alta dirección / usuarios Líder del proyecto



7. ¿Se capacita al personal de desarrollo de recién ingreso en el entendimiento y uso de la metodología? ¿Contemplan los puntos mencionados en la pregunta 5.1?
8. ¿Se actualiza la metodología cuando es necesario?
 - 8.1 ¿Qué actividades de investigación o consulta se realizan para formular cambios o adaptaciones en la metodología?
9. ¿Se documentan formalmente estos cambios?
10. ¿Quién los aprueba?

Etapa	Tarea	Producto	Responsable
Programación/ construcción Nota: pueden hacerse algunas tareas en paralelo al diseño (diseño aprobado por el líder del proyecto)	1. Programación/ construcción <ul style="list-style-type: none"> • Bases de datos <ul style="list-style-type: none"> - Atributos - Entidades - Relaciones • Programas • Procedimientos • Reportes • Pantallas • Interfaz 2. Documentación de manuales <ul style="list-style-type: none"> • Técnico (computacional) • Usuario • Operación 	1. Bases de datos, programas, procedimientos, reportes, etc., construidos 2. Manuales técnicos, de usuario y de operación	Analista/ programadores
Pruebas *	1. Capacitación <ul style="list-style-type: none"> • Plan de capacitación • Adiestramiento de usuarios e informática 2. Pruebas <ul style="list-style-type: none"> • Unitarias (por programa, procedimiento, etc.) • Modulares (subsistemas) • Totales (del sistema) • De tecnología • En el medio de producción • Aceptación de las pruebas 	1. Capacitación técnica y de uso del sistema 2. Pruebas unitarias, modulares, del sistema, de tecnología y del medio de producción 3. Pruebas aprobadas, registradas y documentadas	Líder del proyecto / asesores externos / analistas y áreas usuarias
Producción/ liberación Nota: pueden hacerse algunas tareas en paralelo al diseño (diseño aprobado por el líder del proyecto)	1. Conversión y carga inicial de datos 2. Instalación del nuevo sistema 3. Arranque y operación del nuevo sistema 4. Aprobación del sistema en operación	1. Nuevo sistema en operación 2. Manejo de datos reales en el nuevo sistema 3. Carta formal de aprobación del sistema en operación	Líder del proyecto / analistas / personal de operación / usuarios Alta dirección / usuarios

Etapa	Tarea	Producto	Responsable
Mejora/ actualización * (Son de carácter preventivo y adaptativo, no correctivo)	1. Evaluación periódica del sistema 2. Actualización y mejoramiento del sistema	1. Sistema evaluado 2. Sistema mejorado y actualizado	Líder del proyecto/ asesores externos/analistas y áreas usuarias
Tareas de complemento	1. Evaluación de proveedores de hardware, software, soluciones de mercado (aplicaciones), telecomunicaciones, CASE, EDI, etc. 2. Selección de proveedores y tecnología de apoyo y soporte a los sistemas de información de negocio que serán implantados	1. Evaluación y selección de proveedores y tecnología	Líder del proyecto, asesores externos, personal de investigación tecnológica, proveedores de tecnología de informática, etc.

* Esta información es enunciativa, no limitativa. Las metodologías sugeridas en universidades, las propuestas por asesores externos y las desarrolladas por el personal de informática pueden enriquecer este proceso metodológico y adecuarlo a las necesidades del negocio. El auditor en informática puede apoyarse en metodologías comúnmente aceptadas en el medio informático.

11. ¿Capacitan formalmente al personal requerido en la actualización de la metodología?
12. ¿Existe una congruencia de la metodología CDISI con las metodologías recomendadas como estándar en el mercado ?
13. ¿Cómo se asegura que las metodologías de desarrollo e implantación compradas o rentadas a externos satisfagan los requerimientos específicos del negocio ?
14. Comprobar, de acuerdo con las siguientes tablas, que las etapas, tareas, productos terminados y responsables de la metodología de CDISI se encuentren descritos para todo tipo de proyectos relativos al desarrollo e implantación de sistemas de información:

2. Técnicas

Aspectos clave por evaluar

1. ¿El personal de informática conoce cuáles son las técnicas requeridas para el desarrollo, seguimiento y documentación formal de las etapas del CDISI antes mencionadas?

2. ¿Existen dichas técnicas para el CDISI formal en la empresa?
3. ¿Se capacita formalmente al personal de desarrollo de sistemas en el uso y aplicación de estas técnicas?
4. ¿Se capacita al personal de desarrollo de sistemas recién contratado en el manejo de estas técnicas?
5. ¿Qué procedimiento se utiliza para la capacitación del personal de desarrollo en el uso de metodologías y técnicas?
6. Explique cuáles de las técnicas siguientes son usadas por su empresa en el desarrollo de sistemas:

Técnica	SÍ	NO	Etapas donde se aplica
Listas de verificación			
Entrevistas			
Listas de verificación para el aseguramiento de calidad			
Control de proyectos			
Análisis y diseño estructurado			
Análisis costo/beneficio			
Documentación			
Diagramación			
Modelación de datos y procesos			
Programación estructurada			
Manejo de equipos de trabajo			
Otros (especifique)			

7. ¿Quiénes y cómo determinaron cuáles eran las técnicas requeridas para el desarrollo e implantación de sistemas de información en el negocio?
- 7.1 ¿Su uso es general en la empresa? ¿Cómo se aseguran de que se aplique?

3. Herramientas

Aspectos clave por evaluar

1. ¿Existe una clasificación de las herramientas de productividad utilizadas en el desarrollo e implantación de sistemas de información de la empresa? (Entiéndase por herramientas de productividad los medios computarizados [hardware/software] o manuales [instrumentos de medición, diagramación, etc.] que usa el personal de informática en el CDISI.)

2. Si es así, ¿podría indicar cuáles de los siguientes se utilizan en la empresa?

Concepto	Hardware	Software	Herramientas manuales
Procesadores de palabras			
Hojas electrónicas			
Graficadores			
Diagramadores			
Presentadores			
Generadores de aplicaciones			
Generadores de bases de datos			
Ingeniería de software			
Índices de referencia (<i>benchmarks</i>)			
Otros (especifique)			

3. ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique?

4. Capacitación y actualización

Aspectos clave por evaluar

- Investigue si existen procedimientos formales para capacitar al personal de desarrollo de sistemas de información (o puestos equivalentes) en:
 - Entendimiento y aplicación de:
 - Metodología de CDISI
 - Técnicas para efectuar las etapas del CDISI
 - Herramientas de productividad requeridas en el CDISI
- ¿Existe una documentación formal de dichos procedimientos?
- ¿Se cuenta con un responsable directo de elaborar, actualizar, documentar y definir dichos procedimientos de capacitación?
- ¿Cómo se asegura el cumplimiento oportuno de tales procedimientos?

5. Si existen los procedimientos, ¿al menos contemplan lo siguiente?
- Calendarios de los cursos
 - Responsables de impartir los cursos (personal externo o interno)
 - Puestos o funciones que requieren dichos cursos
 - Costos estimados de los cursos
 - Beneficios esperados de cada curso
 - Parámetros de medición para asistentes y expositores
 - Material requerido para cada curso
 - Responsables de la organización de los cursos
6. Si no existe un proceso formal de capacitación, ¿cómo se da seguimiento al entendimiento, uso y actualización oportunos de la metodología, técnicas y herramientas de productividad requeridas por parte del personal durante el CDISI?
7. ¿El responsable de informática está consciente de la importancia que tiene la actualización y mejoramiento continuos del personal de desarrollo de sistemas de información para la implantación de soluciones en el negocio?
8. Cuando se involucran terceros (personal externo) en proyectos de desarrollo e implantación de sistemas de información, ¿cómo se aseguran de que su metodología, técnicas y herramientas de productividad correspondan por lo menos con el estándar o norma de la empresa? ¿Qué se hace si la empresa no tiene definidos dichos estándares?

Sistemas de información

Planeación y desarrollo
Operación
Soluciones de mercado

Objetivos de esta revisión

Planeación y desarrollo

- Verificar que los sistemas de información desarrollados e implantados se deriven del proceso formal de planeación de sistemas
- Asegurar que los sistemas de información por desarrollar cuenten con el involucramiento y aprobación de la alta dirección y las áreas usuarias correspondientes
- Comprobar que existan y se lleven a cabo las funciones, estándares y procedimientos requeridos durante el desarrollo de un sistema de información

- Verificar y asegurar que se utilice la metodología del CDISI en cada proyecto de implantación de sistemas de información (véase el cuestionario del Ciclo de Desarrollo e Implantación de Sistemas de Información)
- Confirmar que el personal de desarrollo de sistemas de información ejecute de manera total la metodología de CDISI, con el fin de que se asegure calidad y productividad durante el desarrollo de los sistemas de información
- Evaluar el nivel de estandarización que se utiliza en el desarrollo de sistemas con respecto a la metodología de desarrollo de sistemas; si no se cuenta con ella, comprobar el apego a los estándares aceptados en el CDISI
- Hacer las recomendaciones pertinentes para que dicho desarrollo satisfaga las necesidades de los requerimientos planteados en la planeación inicial del proyecto
- Verificar que el desarrollo de sistemas de información se elabore en condiciones de alta calidad y productividad

Nota: Es necesario que el auditor en informática evalúe proyecto(s) donde se desarrollen e implanten sistemas de información para confirmar los puntos mencionados. Por otro lado, la auditoría debe aplicarse al personal involucrado durante el desarrollo e implantación de los sistemas de información (líder de proyecto, analistas, programadores, administradores de bases de datos, auditores internos o externos, asesores externos, encargados del área de mantenimiento y producción de sistemas, entre otros).

Objetivos de esta revisión

Operación

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

- Satisfacción de los requerimientos de usuarios
- Procedimientos que aseguren la continuidad de la operación
- Seguridad en la operación de los sistemas
- Totalidad, mantenimiento, actualización, autorización, exactitud y registro de datos

Nota: Aquí se auditan las funciones y responsabilidades de los usuarios y personal de sistemas responsables de los sistemas en operación.

Objetivos de esta revisión

Soluciones de mercado

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

Nota: Aquí se evalúan las funciones y procedimientos de los involucrados en todo el proyecto de evaluación y selección de soluciones de mercado (sistemas de información hechos por terceros).

Principales actividades para auditar esta área

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



Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla C.1)

Planeación y desarrollo

Aspectos clave por evaluar:

1. ¿Se cuenta con un plan de proyectos de desarrollo de sistemas a inmediato o corto plazo?
2. Si es así, ¿se ha contemplado la posibilidad de integrar a los equipos de proyectos funciones que aseguren la aplicación formal de los estándares y procedimientos contemplados en la metodología de CDISI?
 - a) Auditor en informática
 - b) Consultor externo
 - c) Otro (especifique)
- 2.1 Si no se involucran funciones de aseguramiento de calidad, ¿qué procedimientos y qué personal de informática garantiza el cumplimiento de los proyectos y compromisos hechos en la etapa de planeación de sistemas de información por desarrollar?
3. ¿Qué sistemas se encuentran en desarrollo?
 - 3.1 ¿Tales sistemas surgen de la planeación de sistemas?
 - 3.2 Si no es así, ¿qué criterios y argumentos justificaron su desarrollo?
 - 3.3 ¿Los sistemas que empiezan a desarrollar se integran a la documentación de la planeación de sistemas de información en caso de que no se hayan registrado en esa etapa?
 - 3.4 ¿Quién autoriza el desarrollo de sistemas de información cuando éstos no fueron planeados formalmente?
 - 3.5 ¿Es una autorización formal? ¿Existen registros de todas estas autorizaciones?

Tabla C-1

Métodos, técnicas y herramientas requeridas	Ciclo de desarrollo e implantación de sistemas de información	Sistemas de información	Mantenimiento	Redes locales
Metodología de desarrollo e implantación de sistemas	Sí	Sí	Sí	No
Metodología de planeación	Sí	Sí	Sí	Sí
Cuestionarios	Sí	Sí	Sí	Sí
Entrevistas	Sí	Sí	Sí	Sí
Observación / monitoreo	Sí	Sí	Sí	Sí
Análisis / diseño	Sí	Sí	No	No
Trabajo en equipo	Sí	Sí	No	No
Análisis costo / beneficio	Sí	Sí	Sí	No
Documentación	Sí	Sí	Sí	Sí
Pruebas de auditoría	Sí	Sí	No	Sí
Control de proyectos	Sí	Sí	No	No
Índices de producción (benchmarking)	Sí	No	No	Sí

- 3.6 ¿Qué actividades se llevan a cabo cuando se cancelan proyectos de desarrollo de sistemas de información planeados formalmente? ¿Se registran estas actividades?
- 3.7 ¿Quién autoriza la cancelación de estos proyectos? ¿Qué sucede con estos proyectos?
- 3.8 ¿Qué actividades se realizan cuando no se cumplen las fechas de proyectos de desarrollo de sistemas de información planeados formalmente (inicio, terminación)? ¿Se registran estas actividades? ¿Quiénes verifican el cumplimiento de los planes de desarrollo?
4. ¿Qué proyectos de desarrollo de sistemas de información hay actualmente?

Sistema de información	Usuarios Responsables	Comentarios
1.		
2.		
Otros		

- 4.1 ¿En qué estado se encuentran?

Sistema de información	Etapas del CDISI	Porcentaje de avance real
1.		
2.		
Otros		

5. ¿Existen algunas dificultades o contratiempos que afecten de manera significativa algunos proyectos en desarrollo? Si es así, ¿cuáles son los sistemas de desarrollo afectados?
 - 5.1 Mencione las causas principales de dicha problemática.
 - 5.2 ¿Tiene algunas sugerencias que conviertan esa problemática en un conjunto de áreas de oportunidad? Si es así, ¿puede enunciarlas?
6. ¿Durante el desarrollo de sistemas se tiene alguna función que verifique y lleve a cabo el control en los puntos siguientes?
 - El uso formal, adecuado y oportuno de la metodología de CDISI. ¿Cómo?
 - El desempeño eficiente de los involucrados en el desarrollo de los sistemas. ¿Cómo?
 - Coordinación entre usuarios e informática. ¿Cómo?
 - Coordinación entre informática y los asesores externos durante el proyecto. ¿Cómo?
 - Programación de revisiones para asegurar la calidad en los productos terminados que se obtienen a lo largo del CDISI. ¿Cómo?

- Otros que orienten a desarrollo de sistemas de información eficientes y oportunos. ¿Cómo?

Nota: El auditor en informática debe comprobar que lo anterior se ejecute de manera formal y oportuna. Por otro lado, la auditoría en informática ha de establecer qué sistemas de información en desarrollo serán auditados, tomando como base el plan de auditoría en informática.

7. ¿Se tienen procedimientos formales para garantizar que los acuerdos o compromisos que se originen en las reuniones o juntas durante las fases de desarrollo sean ejecutados oportunamente?
 - 7.1 Si es así, especifique cuáles son esos procedimientos (pasos, responsables del seguimiento de los acuerdos, etcétera).
8. Cuando hay problemas, retrasos u otros hechos que obstaculicen el desempeño del desarrollo de sistemas, ¿se analizan los siguientes aspectos para determinar la solución a dichas limitantes?
 - Seguimiento de planes y estándares
 - Supervisión del proyecto
 - Experiencia y conocimiento técnico de los involucrados en el proyecto
 - Comunicación entre los integrantes del mismo
 - Involucramiento y comunicación con los departamentos usuarios
 - Cargas de trabajo
 - Entendimiento real de la metodología, técnicas y herramientas
 - Conocimiento y entendimiento real de los requerimientos del usuario
 - Documentación actual del proyecto (etapas, tareas, resultados, etc., en relación con lo planeado)
 - Asignación de responsabilidades
 - Administración del proyecto
 - Otros
9. ¿Con qué periodicidad se revisan los resultados del proyecto, quiénes lo realizan y cómo documentan los resultados?
10. ¿Existe una bitácora que muestre los cambios a los planes, tareas, responsabilidades, etc., con respecto a lo planeado originalmente?
11. ¿Quiénes autorizan dichos cambios?
12. ¿Hay documentación que muestre dichos cambios, motivos o causas de los mismos y sus respectivas autorizaciones (verificar si es la misma bitácora)?

Nota: Una vez autorizados los cambios, lo que se debe modificar es la planeación original, los diagramas de procesos y de datos, el diseño, programas fuente, etc. Tener

los datos en una bitácora no es lo más recomendable, ni es suficiente soporte para el auditor.

13. ¿En las especificaciones del sistema propuesto (solución sugerida en la etapa de análisis se indica qué información) qué procesos son básicos y confidenciales para los usuarios y el negocio en particular?
14. ¿Cómo se asegura que permanezca dicha confidenciabilidad a lo largo del proyecto de desarrollo y después se implante dicho sistema?
 - 14.1 ¿Existen procedimientos, como cartas o documentos, que comprometan a los usuarios a manejar esos datos de manera confidencial?
15. ¿La función de aseguramiento de calidad (o función similar) en el desarrollo del sistema contempla los siguientes aspectos en la etapa de análisis?
 - Puntos de revisión en el análisis:
 - Alcance confirmado del proyecto
 - Perfil y responsabilidades del equipo del proyecto de acuerdo con sus funciones y tareas
 - Diagramas de procesos (manuales y automatizados)
 - Modelos de datos
 - Requerimientos:
 - ♦ Seguridad
 - ♦ Procedimientos, controles, etc.
 - ♦ Tecnológicos
 - ♦ Otros
 - Evaluación del sistema actual
 - Alternativas (tecnológicas, de procesos, de datos, de organización, económicas, etcétera)
 - Sistema sugerido de información (solución propuesta)
 - ♦ Diagramas de procesos (manuales y automatizados)
 - ♦ Modelos de datos
 - ♦ Interfases (manuales y automatizadas; internas y con otros sistemas)
 - ♦ Estructuras de datos
 - ♦ Volúmenes de información
 - ♦ Seguridad
 - ♦ Procedimientos, controles, etc.
 - ♦ Tecnológicos
 - ♦ Conversión
 - ♦ Evaluación costo/beneficio del sistema propuesto
 - ♦ Otros
 - Aprobación de la solución del líder del proyecto por parte de las siguientes áreas del negocio:
 - ♦ Alta dirección (indispensable)

- ♦ Usuarios responsables del sistema de información (indispensable)
 - ♦ Auditoría (recomendable)
 - ♦ Auditoría en informática (recomendable)
 - Puntos de revisión en el diseño del sistema:
 - Compatibilidad y congruencia con el análisis
 - Elaboración, verificación y documentación de:
 - ♦ Diseño de base de datos
 - ♦ Diseño de reportes
 - ♦ Diseño de programas
 - ♦ Diseño de procedimientos y controles
 - ♦ Diseño de interfases (gráficas, narrativas, etc.)
 - ♦ Otros aspectos
 - Aprobación del diseño
 - Puntos de revisión en la construcción o programación del sistema:
 - Compatibilidad y congruencia con el diseño
 - Elaboración, verificación y documentación de:
 - ♦ Construcción o programación de base de datos
 - ♦ Construcción o programación de reportes
 - ♦ Construcción o programación de programas
 - ♦ Construcción o programación de procedimientos y controles
 - ♦ Construcción o programación de interfases (gráficas, narrativas, etc.)
 - ♦ Otros aspectos
 - Aprobación del diseño
 - Puntos de revisión en las pruebas del sistema (incluye pruebas en el ambiente real):
 - Planes de pruebas y de capacitación
 - Programas y procedimientos (unitarios)
 - Subsistemas
 - Del sistema
 - Documentación (manual técnico, usuario y de operación del sistema)
 - Aceptación formal del usuario y del líder del proyecto
 - Puntos de revisión en la producción o liberación del sistema:
 - Conversión de datos y liberación del sistema
 - Arranque y formalización del uso inicial del sistema de información
 - Mejoras o adaptaciones posteriores al sistema de información (justificadas)
16. Si el personal de desarrollo de recién ingreso participa en el desarrollo de algún sistema, ¿se le capacita en el uso de metodología, técnicas y herramientas?
17. ¿Existe un procedimiento formal que asegure el cumplimiento satisfactorio de los estándares, técnicas y herramientas de productividad de dicho personal?
18. Explique cuáles técnicas y herramientas de productividad se emplean en cada etapa del desarrollo de sistemas:

Etapa	Técnicas	Herramientas de productividad
Análisis		
Diseño		
Construcción		
Pruebas		
Producción		
Mantenimiento		
Tareas de complemento		

Nota: Verificar que las etapas, tareas, productos terminados y responsables correspondientes a la planeación y desarrollo de sistemas se usen y documenten formalmente conforme la metodología del CDISI.

Operación

Aspectos clave por evaluar:

1. ¿Cuáles sistemas de información requiere para el soporte de las funciones y actividades de su gerencia, área o departamento?
2. ¿Cuales están en operación o producción formal?
3. ¿El personal de su área se involucró de manera activa y permanente cuando se desarrollaron estos sistemas?
4. ¿Los usuarios están debidamente capacitados en el uso de los sistemas que operan en la actualidad?
5. ¿Manejan de manera formal y satisfactoria?:
 - Llenado de documentos
 - Captura de transacciones
 - Proceso de transacciones
 - Uso y distribución de reportes
 - Manejo de los manuales de usuario
 - Procedimientos y controles del sistema
6. Califique en un nivel de 1 a 10 los siguientes puntos:

Oportunidad	()
Calidad	()
Contenido	()
Veracidad de la información	()
Confiabilidad de la información	()
Adecuaciones o nuevos requerimientos	()
Otros (especifique)	()

7. ¿Qué procedimientos se siguen en la atención y solución de los nuevos requerimientos de su área?
8. ¿Cómo se definieron, autorizaron y difundieron estos procedimientos?
9. ¿Existe una función encargada de dar seguimiento oportuno a dichos procedimientos, ya sea de su área o de informática?
10. ¿Todos los usuarios que operan los sistemas conocen dichos procedimientos?
¿Por qué?
10.1. ¿Considera que los procedimientos mencionados son suficientes?
11. ¿Existen procedimientos para el manejo de errores o cambios en los sistemas actuales?
11.1 ¿Los cambios y adiciones a los nuevos sistemas son aprobados formalmente por los usuarios?
12. ¿Se tiene una documentación formal de los sistemas en operación?
12.1 Si la respuesta es afirmativa, verifique si existe al menos la siguiente documentación:
 - Manuales de usuarios
 - Manuales de operación
 - Manuales técnicos (éstos deben estar en el área de informática)
 - Procedimientos de contingencia y recuperación
 - Datos de referencia del personal de informática responsable de los sistemas de su área
 - Fechas en que los sistemas fueron formalmente liberados (cuando se trasladaron de pruebas a producción)
 - Responsables del área usuaria y del área de informática que autorizaron dicha liberación
 - Procedimientos para el manejo del equipo en el sitio donde operan los sistemas
 - Procedimientos de seguridad que garanticen la continuidad de la operación de los sistemas
 - Lista de usuarios responsables de cada sistema y sus principales funciones
 - Personal de informática responsable de cada sistema
 - Otros
13. ¿Existe un conocimiento real, por parte de los usuarios, de los alcances y limitaciones de cada sistema en operación? ¿Por qué?
14. ¿Se conocen de manera satisfactoria los siguientes puntos?
 - a) El procedimiento de llenado y captura de documentos fuente para alimentar datos a los sistemas. ¿Por qué?
 - b) El manejo de errores y realimentación de datos para asegurar que sean válidos y correctos. ¿Por qué?

- c) El uso de los reportes que generan los sistemas. ¿Por qué?
- d) La distribución (a quién) y periodos (cuándo) de dichos reportes. ¿Por qué?
- e) Procedimientos para el manejo de papelería (sobre todo papelería preimpresa como cheques), reportes rechazados, documentos fuente alimentados, etc. ¿Por qué?
- f) Los procedimientos para el acceso a la papelería y números de control (secuencia) de la misma. ¿Por qué?
- g) El Almacenamiento y destrucción de papelería no útil al negocio. ¿Por qué?
- h) Otros

¿Cómo se aseguran de que el conocimiento, ejecución y seguimiento de cada uno de los puntos anteriores sean oportunos y adecuados?

15. Indique si en la operación de los sistemas de información existen controles para:

- Verificar totales:
 - Documentos vs reportes
 - Cifras de control del computador vs totales alimentados
 - Otros (especifique)
- Comprobar que no se omitan movimientos
- Confirmar que las correcciones sean autorizadas, correctas y registradas en los archivos correspondientes oportunamente
- Verificar que la información confidencial no sea conocida por personal no autorizado
- Los procedimientos de verificación dentro de los sistemas en operación que eliminen:
 - Posibilidades de error en el manejo de la información
 - Tiempos de revisión y captura
 - Acceso a información confidencial por personal no autorizado (accidental o deliberado)
 - Información duplicada
 - Otros
- Registros de:
 - Usuarios que operaron los sistemas
 - Tiempo de operación
 - Accesos rechazados a módulos del sistema
 - Datos alimentados a los sistemas
 - Datos aceptados como válidos
 - Datos rechazados
 - Datos corregidos y realimentados
 - Otros

- Para asignación, borrado y cambio oportuno y formal de contraseñas o claves de acceso a los usuarios
 - Capacitación formal y oportuna de la operación de los sistemas
 - Uso adecuado y autorizado de utilerías de los sistemas (respaldos, reprocesos, etc.)
 - Uso y registro formal de bitácoras del empleo del equipo donde se alojan los sistemas
 - Acceso a la documentación de los sistemas por personal autorizado
 - Evitar el acceso a los operadores o usuarios a los programas fuente de los sistemas
 - Acceso exclusivo del personal autorizado a las áreas donde está el equipo de cómputo
 - Evitar accesos no autorizados a los archivos de datos de los sistemas
 - Detección y corrección de datos transmitidos de una localidad a otra
 - Comprobación de la congruencia de la documentación de los sistemas con lo que existe en los sistemas en operación (verificarlo a detalle)
 - Otros
16. ¿Existe la documentación de los sistemas en producción? Si es así, verifique que exista al menos:
- Manual de usuario
 - Nombre y objetivos del sistema
 - Módulos principales del sistema
 - Documentos fuente que serán alimentados al sistema
 - Procedimientos de llenado de documentos
 - Procedimiento para iniciar la operación del sistema
 - Procedimiento para trabajar cada módulo del sistema (altas, bajas, consultas, cambios, reportes, respaldos [si son válidos], entre otros)
 - Menús de ayuda en cada módulo del sistema
 - Procedimientos de manejo de errores
 - Descripción y uso de los reportes
 - Manual computacional o técnico del sistema
 - Nombre y objetivos del sistema
 - Módulos del sistema
 - Ligas entre los módulos principales
 - Ligas con otros sistemas (Interfases)
 - Descripción de cada programa
 - Diagrama de flujo de cada programa
 - Estructura y descripción de archivos
 - Procedimientos para actualización y documentación de programas

- Tabla de referencias cruzadas (programas-archivos; programas-reportes; reportes vs archivos, por señalar algunos)
- Otros
- Manual de operación
 - Nombre del sistema y objetivos
 - Descripción de procedimientos (*Job Description*)
 - Secuencia, flujo, tiempos y programación de procesos
 - Procedimientos de inicio y terminación de procesos
 - Procedimientos para el manejo de errores y mensajes por consola
 - Reprocesos, respaldos y procedimientos de inicialización y recuperación
 - Lista de distribución de documentos de entrada y salida con fechas de corte y periodos de retención de documentos
 - Procedimientos de entrada y consulta por terminal
 - Otros
- 16.1 ¿Estos manuales están donde les corresponde? (Hay que confirmarlo mediante observación directa en las áreas de los usuarios, de operación y de informática.)
- 16.2 ¿Se capacitó al personal en el uso de estos manuales? (Compruébese mediante entrevistas al personal.)
- 16.3 ¿Se actualiza la documentación cuando hay cambios? (Compruébese comparando el sistema actual con los manuales.)
- 16.4 ¿Existe algún sistema a punto de liberarse? (Comfirmense los controles existentes con base en las preguntas anteriores.)
- 17. ¿Alguna sugerencia para mejorar los sistemas en operación?

Soluciones de mercado

Aspectos clave por evaluar:

1. ¿Existen proyectos relativos a la evaluación, compra e instalación de soluciones de mercado (sistemas de información hechos fuera de la empresa) para el negocio?
 - 1.1 ¿Son proyectos emanados de la planeación de sistemas?
 - 1.2 Si no es así, ¿cómo se justifican?
2. ¿La ejecución y administración de este tipo de proyectos se basan en la metodología del CDISI?
 - 2.1 Si no es así, ¿cómo se definen, planean, evalúan, seleccionan, aprueban y compran las soluciones de mercado antes de instalarlas en el negocio?
 - 2.2 ¿Con qué procedimientos y controles de aseguramiento de calidad se cuenta para las actividades mencionadas en la pregunta 2.1?

3. Mencione los productos terminados, tareas y responsables de las etapas de este tipo de proyectos ejecutados en la empresa:

Etapas	Tareas	Productos	Responsables

- 3.1 Mencione las técnicas y herramientas de productividad que utiliza por cada etapa:

Etapas	Técnicas	Productos	Responsables

4. ¿Qué etapas y tareas adicionales (complementarias) realiza cuando compra una solución de mercado y tiene que agregarle o modificarle ciertos módulos o subsistemas para que el sistema de información satisfaga los requerimientos específicos de los usuarios?

Etapas	Técnicas	Productos	Responsables

5. ¿Qué actividades se efectúan para evaluar las diferentes alternativas que se ofrecen en el mercado en relación con aplicaciones o sistemas de información mientras no existen en el negocio proyectos de este tipo? ¿Quién las lleva a cabo?

MANTENIMIENTO

1. Hardware
2. Software
3. Sistemas de información
4. red de comunicaciones

Objetivos de esta revisión

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

- Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento correctivo
- Otros

Nota: Esta aplicación pertenece a los responsables de dar mantenimiento a los aspectos mencionados.

Principales actividades en la auditoría de esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla C.1)

1. Hardware

Aspectos clave por evaluar:

1. ¿Existe una lista del hardware existente en el negocio (departamento de informática y áreas usuarias)?
 - 1.1 ¿Cómo se levantó el inventario del hardware (inventarios físicos, por software, con base en compras, etc.)? (El auditor en informática debe validar esta información.)
2. ¿Está identificado el lugar físico del hardware y los responsables de su uso y custodia?
3. ¿Se cuenta con manuales o procedimientos para el manejo del equipo?
4. ¿Dichos manuales o procedimientos están actualizados?
5. ¿Existe un procedimiento formal para dar mantenimiento al hardware?
 - 5.1 ¿Dicho procedimiento contempla lo siguiente?
 - Formulación y difusión del plan de mantenimiento preventivo/correctivo
 - Difusión del plan de mantenimiento preventivo/correctivo
 - Medidas que garanticen la continuidad de las operaciones durante este proceso
 - Desarrollo de las actividades de mantenimiento preventivo/correctivo
 - Identificación del tipo de mantenimiento (preventivo o correctivo) y las causas o razones de su realización
 - Identificación de los recursos de hardware que recibirán mantenimiento
 - Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo/correctivo
 - Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática del negocio, usuarios, entre otros)
 - Elaboración y análisis de estadísticas para fortalecer el mantenimiento preventivo
 - 5.2 Señale si este procedimiento es válido para:
 - Microcomputadoras
 - Minicomputadoras
 - *Mainframes*
 - Equipo periférico
 - Otro equipo
6. ¿Existen acciones complementarias que apoyen el mantenimiento y que registren algunos datos relacionados con el mismo?

6.1 Indique si entre dichas acciones se cuentan las siguientes:

- Registro del hardware que reemplazará al equipo que recibirá mantenimiento
- Registro del costo originado por el mantenimiento preventivo y el causado por el mantenimiento correctivo para los siguientes elementos:
 - Microcomputadoras
 - Minicomputadoras
 - *Mainframes*
 - Equipo periférico
 - Otro equipo
- Todo mantenimiento deberá ser autorizado por el responsable del equipo
- Procedimientos de seguridad (egreso e ingreso del equipo)
- Elaborar estadísticas que ayuden a identificar las áreas del negocio y los componentes del equipo que “viven en mantenimiento correctivo”
- Otros

7. ¿Se actualiza la información de los manuales de alguno de los elementos del hardware cuando se libera una nueva versión?

7.1 ¿Se capacita a los usuarios cuando esto sucede?

8. ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los equipos de cómputo y periféricos?

8.1 Si es así, ¿cuáles son esos controles?

9. ¿Se implantan controles y procedimientos a los equipos y periféricos que reciben mantenimiento con objeto de garantizar que la integridad de la información que guardan sea íntegra y correcta antes, durante y después de dicho proceso?

9.1 Si es así, ¿qué controles y procedimientos se tienen contemplados?

9.2 ¿Quién es el responsable de dar seguimiento a dichos controles?

10. ¿Está consciente el personal de informática de que un buen equipo y los procedimientos de uso y cuidado del mismo deben evitar en gran medida los problemas típicos del mantenimiento tradicional?

- Altos costos
- Cargas de trabajo
- Caídas de los equipos
- Dificultad en el manejo del equipo
- Medidas de seguridad incompletas
- Insatisfacción del usuario
- Otros

10.1 ¿Está consciente el usuario de la importancia de seguir de manera formal y oportuna los procedimientos de uso y buen cuidado del equipo para evitar en gran medida los problemas mencionados en la pregunta 10? ¿Por qué?



11. ¿La actualización oportuna del hardware es originada por sugerencias del proveedor o usted la solicita?
 - 11.1 ¿Cuáles de las siguientes son las principales razones de la actualización del hardware?
 - El equipo tiene mal desempeño (velocidad de procesamiento, E/S, otros)
 - Capacidades de memoria y almacenamiento insatisfactorias
 - Leyó en el periódico las bondades y facilidades del nuevo modelo
 - Algún conocido le recomienda adquirir la nueva versión
 - El gerente o director de informática lo ha utilizado en las empresas donde ha trabajado y le ha funcionado de "maravilla"
 - La presión de los usuarios para instalar equipos modernos
 - Obedece a las nuevas estrategias del negocio
 - Se lo prestó un proveedor y prefirió comprarlo que volver a usar el equipo viejo
 - Otros de carácter técnico, estratégico o sentimentales
12. Señale si existe algún sistema computarizado que apoye la administración 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
 - Otros

2. Software

Aspectos clave por evaluar:

1. ¿Hay una lista del software existente en la organización (departamento de informática y áreas usuarias)?
 - 1.1 ¿Cómo se hizo el inventario del software (inventarios a los diferentes equipos por medio de algún software, con base en compras, etc.)? (El auditor en informática debe validar esta información.)
2. ¿Está identificado el equipo donde se encuentra el software y los responsables de su uso y custodia?
3. ¿Se cuenta con manuales o procedimientos para el manejo del software?
4. ¿Están actualizados?
5. ¿Existe un procedimiento formal para dar mantenimiento (actualización) al software?

5.1 Indique si dicho procedimiento contempla lo siguiente:

- Formulación y difusión del plan de mantenimiento (actualización) preventivo/correctivo
- Medidas que garanticen la continuidad de las operaciones durante este proceso
- Desarrollo de las actividades de mantenimiento (actualización) preventivo o correctivo
- Identificación del tipo de mantenimiento o actualización (preventivo o correctivo) y las causas o razones de su realización
- Identificación del software que recibirá mantenimiento o requiere actualización
- Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento (actualización) preventivo o correctivo
- Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática, usuarios, otros)
- Elaboración y análisis de estadísticas para fortalecer el mantenimiento (actualización) preventivo

5.2. ¿Este procedimiento es válido para?

- Paquetes de software (procesadores de palabras, hojas electrónicas, etc.)
- Lenguajes de programación (tercera, cuarta generación, CASE, etc.)
- Bases de datos
- Sistemas operativos, utilerías, software de comunicaciones
- Otro software

6. ¿Está identificado el software original y las copias?

7. ¿Existe un mismo procedimiento para dar mantenimiento (actualización) al software instalado en micros, minis y *mainframes*?

7.1 Si no es así, ¿existe el siguiente procedimiento?

- a) Definición de los responsables de dar mantenimiento o actualización del software
- b) Razones o causas que justifiquen el proceso de mantenimiento o actualización
- c) Identificación del tipo de mantenimiento o actualización (preventivo o correctivo)
- d) Calendario de programación (fechas, usuarios afectados, etc.)
- e) Identificar las partes del software que serán afectadas por dicho mantenimiento o actualización
- f) Registro del software que recibirá mantenimiento o será actualizado

- g) El software afectado por el mantenimiento debe ser alojado en el siguiente orden:
- Área de prueba
 - Área de instalación del producto
- h) Todo cambio ha de ser probado y autorizado por un responsable definido con anterioridad
- i) Seguridad (acceso para cambios y adaptaciones)
- j) Identificar productos del software que “viven en mantenimiento correctivo”
- k) Otros
8. ¿La información de los manuales del producto se actualiza cuando se coloca una nueva versión?
9. ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los productos del software que se está operando?
- 9.1 Si es así, ¿cuáles son esos controles?
10. ¿Se implantan controles y procedimientos inherentes a los productos de software que reciben mantenimiento con objeto de garantizar la integridad de la información que se relaciona con estos productos?
- 10.1 Si es así, ¿cuáles son esos controles y procedimientos?
11. ¿Está consciente el personal de informática de que un buen producto evita en gran medida los problemas típicos del mantenimiento tradicional?
- Cargas de trabajo
 - Eliminar módulos que no cumplen la totalidad de los requerimientos de informática
 - Dificultad en el manejo del software
 - Medidas de seguridad incompletas
 - Otros
12. ¿La actualización oportuna del software es originada por sugerencias del proveedor o usted la solicita porque?:
- No cumple los requisitos técnicos exigidos por informática
 - No satisface los requerimientos de los usuarios
 - Leyó en el periódico las bondades y facilidades del nuevo modelo
 - Algún conocido le recomienda adquirir la nueva versión
 - El gerente o director de informática lo ha utilizado en las empresas donde ha trabajado y le ha funcionado de “maravilla”
 - Los usuarios presionan para instalar equipos modernos

- Obedece a las nuevas estrategias del negocio
- Se lo prestó un proveedor y prefirió comprarlo que volver a usar el equipo viejo
- Otros de carácter técnico, estratégico o sentimental

13. Indique si cuenta con algún sistema computarizado que apoye el control del mantenimiento en aspectos como:

- Calendarización del mantenimiento o actualización preventivo
- Seguimiento del mantenimiento o actualización (correctivo o preventivo)
- Niveles de servicio
- Costos del mantenimiento
- Causas y soluciones del mantenimiento
- Tareas, fechas y responsables del mantenimiento
- Otros

3. Sistemas de información

Aspectos clave por evaluar:

1. ¿Existe una lista de los sistemas de información en operación?
 2. ¿Dichos sistemas fueron aprobados formalmente por los usuarios?
 3. ¿Se cuenta con manuales de usuarios, técnicos y de operación para cada uno de los sistemas de información en producción?
 4. ¿Dichos manuales están actualizados?
 5. ¿Hay un procedimiento formal para el mantenimiento de los sistemas de información?
- 5.1 ¿Dicho procedimiento contempla lo siguiente?

- Formulación y difusión del plan de mantenimiento (actualización) preventivo o correctivo
- Medidas que garanticen la continuidad de las operaciones durante este proceso
- Desarrollo de las actividades de mantenimiento (actualización) preventivo o correctivo
- Identificación del tipo de mantenimiento o actualización (preventivo o correctivo) y las causas o razones de su realización
- Identificación de los sistemas de información que recibirán mantenimiento o serán actualizados
- Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento o actualización

- Responsables de la ejecución, seguimiento y autorización del mantenimiento o actualización (personal externo, personal de informática, usuarios, etc.)
- Elaboración y análisis de estadísticas para fortalecer el mantenimiento o actualización preventivo

5.2 Indique si este procedimiento es válido para:

- Sistemas de información desarrollados con paquetes de software (procesadores de palabras, hojas electrónicas, otros)
- Sistemas de información desarrollados con lenguajes de programación (tercera, cuarta generación, bases de datos, CASE, etc.)
- Sistemas de información comprados a externos (soluciones de mercado)

Nota: Verificar qué sucede con el servicio de mantenimiento de los proveedores que vendieron estas aplicaciones.

6. ¿Están identificados los sistemas de información comprados a externos?
7. ¿Se cuenta con el mismo procedimiento formal para dar mantenimiento o actualizar los sistemas de información instalados en micros, minis o *mainframes*?

7.1 Si no es así, indique si existe el siguiente procedimiento:

- a) Definición de los responsables de dar mantenimiento o actualizar los sistemas de información
- b) Razones o causas que justifiquen el proceso de mantenimiento o actualización
- c) Identificación del tipo de mantenimiento o actualización (preventivo o correctivo)
- d) Calendario de programación (fechas, usuarios afectados, otros)
- e) Identificar los módulos o componentes de los sistemas de información afectados por dicho mantenimiento o actualización
- f) Registro de los sistemas de información que recibirán mantenimiento o serán actualizados
- g) Los sistemas de información afectados por el mantenimiento se deben alojar en el siguiente orden:

- Área de desarrollo (nuevos módulos) y prueba (durante la actualización)
 - Área de producción (instalación de cambios o adaptaciones aprobadas)
- h) Todo cambio ha de ser probado y autorizado por un responsable definido para este objetivo
 - i) Seguridad (acceso para cambios y adaptaciones)
 - j) Identificar los sistemas de información que “viven en mantenimiento correctivo”
 - k) Otros

- 7.2 ¿Se actualiza la información de los manuales de usuarios, técnicos y de operación cuando así corresponda? (Verificar los últimos cambios.)
8. Si el mantenimiento implica la inserción de un módulo, ¿se capacita a los usuarios?
9. ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los sistemas de información en operación?
- 9.1 Si es así, ¿cuáles son esos controles?
10. ¿Se implantan controles y procedimientos en los sistemas de información que reciben mantenimiento con objeto de garantizar la integridad de la información?
- 10.1 Si es así, con qué controles y procedimientos se cuenta?
11. ¿Está consciente el personal de informática de que un buen desarrollo elimina en gran medida los problemas típicos del mantenimiento tradicional?
- Cargas de trabajo
 - Eliminación de sistemas que no cumplen la totalidad de los requerimientos del usuario
 - Sistemas que no contemplan controles y procedimientos que garanticen confiabilidad, oportunidad y calidad
 - Medidas de seguridad incompletas
 - Insatisfacción de la alta dirección por los bajos resultados de los sistemas
 - Falta de estandarización en el uso de:
 - Metodología para el desarrollo
 - Técnicas (análisis, diseño, etc.)
 - Tareas
 - Productos terminados
 - Funciones y responsabilidades
 - Otros
 - Sistemas que no son flexibles (no se adaptan a los cambios del negocio)
 - Otros
12. Señale si hay algún sistema computarizado que apoye el control del mantenimiento en aspectos como:
- Calendarización del mantenimiento preventivo
 - Seguimiento al mantenimiento (correctivo y preventivo)
 - Niveles de servicio
 - Costos del mantenimiento
 - Causas y soluciones del mantenimiento
 - Tareas, fechas y responsables del mantenimiento
 - Otros

4. Red de telecomunicaciones

Aspectos clave por evaluar:

1. ¿Hay una lista de los componentes de la red existente en el negocio, así como una ilustración gráfica de la distribución y cantidad de los mismos?
 - 1.1 ¿Cómo se inventarió la red de telecomunicaciones (inventarios físicos, por software, con base en las compras, etc.)? (El auditor en informática debe validar esta información.)
2. ¿Está identificado el lugar físico de la red y los responsables de su uso y custodia?
3. ¿Existen manuales o procedimientos para el manejo de la red?
4. ¿Dichos manuales o procedimientos están actualizados?
5. ¿Existe un procedimiento formal para el mantenimiento de la red?
 - 5.1 ¿Este procedimiento contempla lo siguiente?
 - Formulación y difusión del plan de mantenimiento preventivo o correctivo
 - Medidas que garanticen la continuidad de las operaciones durante este proceso
 - Desarrollo de las actividades de mantenimiento preventivo o correctivo
 - Identificación del tipo de mantenimiento (preventivo o correctivo) y las causas o razones de su realización
 - Identificación de los recursos de la red que recibirán mantenimiento
 - Registro de las actividades realizadas, pendientes y problemas originados durante el mantenimiento preventivo o correctivo
 - Responsables de la ejecución, seguimiento y autorización del mantenimiento (personal externo, personal de informática, etc.)
 - Elaboración y análisis de estadísticas para fortalecer el mantenimiento preventivo
 - 5.2 ¿Este procedimiento es válido para?
 - Componentes de los enlaces por satélite
 - Componentes para los enlaces terrestres
 - Componentes para los enlaces internos en la(s) empresa(s)
 - Otro equipo
6. ¿Entre las acciones complementarias con que apoyan el proceso de mantenimiento y que registran algunos datos relacionados con el mismo tienen alguna(s) de las siguientes?
 - Registro de los componentes de la red de telecomunicaciones que reemplazarán al equipo que recibirá mantenimiento
 - Registro del costo originado por el mantenimiento preventivo o correctivo para los siguientes elementos:

- Componentes de los enlaces por satélite
 - Componentes para los enlaces terrestres
 - Componentes para los enlaces internos en la(s) empresa(s)
 - Otro equipo
 - Todo mantenimiento deberá ser autorizado por el responsable del equipo
 - Procedimientos de seguridad (egreso e ingreso del equipo)
 - Elaborar estadísticas que ayuden a identificar las áreas del negocio y los componentes de equipo que “viven en mantenimiento correctivo”
 - Otros
8. ¿Se actualiza la información de los manuales de alguno de los elementos de la red de telecomunicaciones cuando se libera una nueva versión tecnológica?
- 8.1 ¿Se capacita a los usuarios de la red de telecomunicaciones cuando sucede lo anterior?
9. ¿Existen controles para que únicamente personal autorizado dé mantenimiento a los equipos de cómputo y a sus periféricos?
- 9.1 Si es así, ¿cuáles son esos controles?
10. ¿Se implantan controles y procedimientos en los componentes de la red de telecomunicaciones que reciben mantenimiento con objeto de garantizar que la información alojada en estos componentes permanezca íntegra y correcta antes, durante y después de este proceso?
- 10.1 Si es así, ¿cuáles son esos controles y procedimientos?
- 10.2 ¿Quién es el responsable de dar seguimiento a dichos controles?
11. ¿Está consciente el personal de informática de que un buen equipo y la aplicación de las políticas y procedimientos de uso y cuidado del mismo evitan en gran medida los problemas típicos del mantenimiento tradicional?
- Altos costos
 - Cargas de trabajo y tiempos de respuesta bajos
 - Caídas de la línea e interrupción de comunicaciones
 - Dificultad en el manejo de la red
 - Medidas de seguridad incompletas
 - Insatisfacción del usuario/informática
 - Otros
- 11.1 ¿Está consciente el usuario de la importancia de seguir formal y oportunamente las políticas y procedimientos de uso y buen cuidado del equipo para evitar en gran medida los problemas mencionados en la pregunta 11? ¿Por qué?
12. ¿La actualización oportuna de la red es originada por sugerencias del proveedor o usted la solicita?



12.1 Indique cuáles son las principales razones de la actualización de la red de telecomunicaciones:

- El equipo tiene mal desempeño (velocidad de transmisión, por ejemplo)
- Capacidades de transmisión inadecuadas
- El gerente o director de informática lo ha utilizado en las empresas donde ha trabajado y le ha funcionado de “maravilla”
- Nuevas estrategias del negocio
- Otros de carácter técnico o estratégico

13. ¿Existe algún sistema computarizado que apoye la administración del mantenimiento en los siguientes aspectos?

- Calendarización del mantenimiento preventivo
- Seguimiento del mantenimiento correctivo y preventivo
- Niveles de servicio
- Costos del mantenimiento
- Causas y soluciones del mantenimiento
- Tareas, fechas y responsables del mantenimiento
- Otros

AUDITORÍA DE REDES LOCALES Y TELECOMUNICACIONES

1. Administración
2. Instalación
3. Operación y seguridad

Objetivos de esta revisión

- Asegurar que exista una 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 (véase el cuestionario sobre seguridad para mayor detalle)
 - El mantenimiento de las redes locales
- Detectar el grado de confianza, satisfacción y desempeño que brindan al negocio las redes locales existentes
- Confirmar que existan parámetros de medición del desempeño de las redes (bitácoras, gráficas, estadísticas, entre otros)
- Evaluar el grado de soporte que se brinda a los usuarios de la red en el uso de sistemas y software al que tienen acceso en la misma
- Determinar si existen los suficientes controles y procedimientos de seguridad para la(s) red(es) de la empresa
- Evaluar las acciones que se llevan a cabo para actualizar los diversos componentes de las redes locales
- Asegurar que sólo se encuentre instalado software legalizado en las redes locales
- Comprobar si se cuenta con algún software que apoye el monitoreo y la auditoría de los diferentes elementos que componen una red local

Principales actividades para auditar esta área

1. Comparar proyectos con la planeación de auditoría.
2. Concertar citas con el personal que se va a entrevistar.

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla C.1)

1. Administración

1. ¿La empresa cuenta con red(es) local(es)?
 - 1.1 Si es así, ¿cuántas micros hay en dicha red, incluyendo el servidor? (Mencione las características básicas de aquéllas y de los periféricos.)
 - 1.2 ¿Qué software (paquetes, lenguajes, sistemas de información, sistemas operativos, bases de datos, etc. hay instalados? ¿Cuáles son las versiones correspondientes?
 - 1.3 Si no tiene una red local, ¿con cuántas micros, periféricos, paquetes, etc. cuenta?
 - 1.4 ¿Existe una administración formal de la red?

- 1.5 En caso de no tener una administración formal de la(s) red(es) o de las microcomputadoras no conectadas en red de la empresa, ¿cómo se da seguimiento a los siguientes aspectos?
 - Planeación de nueva tecnología de información (hardware, software, etc.) para la red
 - Monitoreo de las actividades de la operación y mantenimiento de la red
 - Procedimientos de control y seguridad de la red
 - Aspectos legales del software instalado
 - Capacitación y soporte a usuarios
 - Otros
- 1.6 Si la empresa tiene una administración de la(s) red(es) local(es) o microcomputadoras no conectadas en red, ¿cuáles de las funciones listadas en la tabla E.1 realiza, con qué tareas efectúa cada función y cómo les dan seguimiento sus coordinadores o jefes inmediatos?
2. ¿Algún personal externo interviene en las funciones de administración mencionadas?
 - 2.1 Si es así, ¿en qué funciones participa y por qué?
3. ¿Existe la documentación formal que especifique qué hacer y cómo efectuar cada función administrativa de la red?

Tabla E.1 Administración de redes locales

Función	Tareas	Acciones de seguimiento
Planeación		
<ul style="list-style-type: none"> • Definir un plan formal que contemple: <ul style="list-style-type: none"> • Evaluación del hardware actual: <ul style="list-style-type: none"> - Análisis y evaluación de la red local actual (si existe) - Análisis y diagnóstico del número de microcomputadoras, características, usuarios, etc. - Análisis y diagnóstico de periféricos - Otros • Evaluación del software actual: <ul style="list-style-type: none"> - Análisis y diagnóstico del software instalado en la red o computadoras aisladas: <ul style="list-style-type: none"> graficadores, procesadores, hojas electrónicas, otros - Lenguajes de programación, sistemas operativos, etc. - Cantidad de licencias, copias pirata, versiones, número de usuarios - Software por legalizar - Otros 		

Tabla E.1 Administración de redes locales (continuación)

Función	Tareas	Acciones de seguimiento
<ul style="list-style-type: none"> • Estudio de justificación de instalación o reemplazo de la red local: <ul style="list-style-type: none"> - Hardware requerido: computadoras, periféricos, otros - Configuración de la red: distribución física, interfase, etc. - Software requerido: aspectos legales, paquetes de cómputo, lenguajes de programación, sistemas operativos, otros - Evaluación costo/beneficio - Procedimientos de capacitación, seguridad, operación, mantenimiento, monitoreo, etc. 		
Organización		
<ul style="list-style-type: none"> • Elaboración de políticas y procedimientos para: <ul style="list-style-type: none"> • La evaluación de hardware, software, etc. de la red • Adquisición o instalación de hardware o software • Asignación y baja de usuarios • Administración de la red • Nivel de servicios para usuarios de la red: <ul style="list-style-type: none"> - Desempeño <ul style="list-style-type: none"> ♦ Tiempos de respuesta ♦ Proceso ♦ Atención a fallas ♦ Otros - Capacitación, soporte, mantenimiento <ul style="list-style-type: none"> ♦ Hardware ♦ Software ♦ Aplicaciones • Operación de: <ul style="list-style-type: none"> - Equipo - Software - Aplicaciones • Seguridad: <ul style="list-style-type: none"> - Datos - Software - Hardware - Aplicaciones - Accesorios 		

3.1 Si es así, ¿las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación?

4. En caso de que no exista esta documentación, ¿cómo se indica al personal responsable y a los usuarios lo referente a los puntos mencionados en la pregunta 1?

5. ¿Existe un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios?
6. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre los usuarios y los responsables de la red?
7. ¿Qué garantiza que se está utilizando la tecnología de redes más adecuada para el negocio?
8. ¿Hay análisis costo/beneficio de las diferentes estrategias de redes implantadas?
¿Se han aprobado de manera formal?

2. Instalación

Aspectos clave por evaluar:

1. ¿Existen procedimientos que aseguren la oportuna y adecuada instalación de los diferentes componentes de la red conforme se hayan realizado los contratos y compras formales de los mismos?

Procedimientos	Responsables de ejecutarlos	Responsables de seguimiento

2. Mencione las actividades que se realizan durante el proceso de instalación de los componentes de la red local (hardware, software, procedimientos, etc.)

Actividades	Responsables de ejecutarlos	Responsables de seguimiento

3. ¿Las compras de los diferentes elementos de la red, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla?
4. En caso de que las compras e instalación de componentes de la red —sea hardware, software u otros— no se hayan planeado formalmente, ¿cómo se justifica esto ante los responsables de informática y de las áreas usuarias?
5. En cuanto a la instalación de software, ¿cómo se asegura la compra legal? ¿Cómo aseguran que no sea instalado en otros equipos de la empresa sin licencia de uso?
¿Qué hacen cuando detectan anomalías al respecto?
5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección del software?
6. Cuando son terceros (personal externo) los encargados de la instalación parcial o total de cualquiera de los elementos que componen la red, ¿cómo se asegura la

empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confiabilidad?

7. ¿Tiene alguna(s) sugerencia(s) que apoyen el proceso de instalación?

3. Operación y seguridad

1. ¿Se cuenta con manuales de operación de la red? ¿Contemplan aspectos de seguridad?

1.1 Si es así, ¿el personal responsable de administrarla y operarla fue capacitado y preparado para el manejo de la misma? ¿Le da seguimiento a la seguridad?

1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?

2. Indique si existen estándares relativos a la operación y administración de la red como:

- Estándares de desempeño:
 - Tiempos de respuesta
 - Tráfico (volumenes de información, velocidad)
 - Interrupciones
 - Tiempo de recuperación de la red
 - Equipos o terminales interconectados
 - Otros
- Estándares de mantenimiento:
 - Calendarios (fechas, horarios, etc.)
 - Responsables
 - Otros

2.1 Si existen, ¿son aplicados formalmente por los responsables de la red?

2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos?

2.3 Una vez que se aplican estos estándares, ¿qué datos se envían a otras áreas (usuarios, auditoría en informática)?

2.4 ¿Los costos por el uso de la red se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios?

2.5 ¿Existe otro procedimiento para establecer los costos derivados por el uso de la red? Si es así, ¿cuál?

2.6 ¿El usuario aprueba formalmente este procedimiento de pago?

3. ¿Se desarrolló o adquirió algún cuestionario estándar que permita saber el nivel de servicios que brinda la red?

3.1 ¿Si es así, ¿con que periodicidad se distribuye este cuestionario a los usuarios o encargados de la red?

- 3.2 ¿Qué indicadores o parámetros importantes salen de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática?
4. ¿Hay procedimientos que protejan los datos transmitidos de una red local a otra(s)?
 - 4.1 Si se tienen, ¿cuáles son?
 - 4.2 ¿Se cuenta con un responsable o un software de comunicaciones que vigile de manera permanente que los datos sean transmitidos con los estándares de oportunidad, totalidad, exactitud y autorización de una red a otra(s)?
 - 4.3 ¿Existen registros (*logs*) con información relevante para el administrador de la red o el auditor en informática?
 - 4.4 Si es así, señale si éstos contienen información relativa a:
 - Usuarios que accedieron a la red
 - Operaciones realizadas en la red (envío, recepción)
 - Tiempos de conexión
 - Interrupciones en el transcurso del uso de la red
 - Causas
 - Tiempo para reiniciar cada interrupción
 - Terminales o equipos conectados
 - Accesos invalidados a la red
 - Terminales donde se llevaron a cabo estos accesos no autorizados
 - Otros
 - 4.5 ¿Estos registros son generados por algún software de la red o por los responsables de la misma?
5. Señale si se tiene identificada formalmente la siguiente información:
 - Usuarios de la red
 - Registros y niveles de acceso
 - Terminales conectadas a la red
 - Responsables de la red
 - Procedimientos de contingencia
 - Software
 - Periféricos conectados
 - Software original y pirata instalado
 - Software de las micros conectadas a la red (duplicidad o carencia de software en la red)
 - Tipos de unidades centrales de procesamiento (CPU)
 - Capacidad de discos o espacio libre por servidor y micros
 - Otros

- 5.1 ¿Estos registros son generados por algún software de la red o los elaboran por separado los responsables de la misma?
6. ¿Hay una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios de la red?
7. ¿Existe un procedimiento formal para dar un servicio oportuno y eficiente a los requerimientos de los usuarios?
 - 7.1 ¿Lo conocen los usuarios?
8. ¿La red tiene controles de acceso a personas no autorizadas (acceso a equipo, datos y software)?
 - 8.1 En caso de contar con esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado?
 - 8.2 Si es así, ¿cuáles son estos controles y quiénes le dan seguimiento?
 - 8.3 Verificar que los controles contemplen al menos:
 - Protección de archivos
 - Protección a programas fuente de las aplicaciones en red
 - Protección a otro software alojado en la red
 - Métodos para prevenir el monitoreo no autorizado de la red
 - Detección inmediata y automatizada de accesos no autorizados
 - Contraseñas que autoricen el acceso a la red, sin permitir la entrada a archivos no autorizados
 - Otros
9. ¿Existen controles relativos a la seguridad física de los diversos componentes de la red (tarjetas, terminales, manuales, software, documentación, etc.)?
 - 9.1 En caso de contar con esos controles, ¿cómo se aseguran los responsables de darles seguimiento?
 - 9.2 Verificar que estos controles cuenten con:
 - Protección adecuada de los componentes de la red (cables, tarjetas, terminales, servidores, etc.)
 - Guardias o personal que vigile el acceso al centro de telecomunicaciones
 - Bitácoras de acceso a las áreas conectadas a la red
 - Métodos de control de acceso como pases, tarjetas de identificación, puertas con candados, monitores, etc.
 - Listado de personal autorizado con acceso a las terminales y controladores de la red
 - Otros
10. ¿Se tiene un seguro que proteja el software y el equipo de la red?
11. ¿Se cuenta con alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en la(s) red(es)?
12. ¿Estos convenios están formalizados?

13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la(s) red(es) local(es) del negocio como las siguientes?

- Evaluación periódica de la red: hardware, software, grado de satisfacción, grado de utilización, etc.
- Acceso a la red de nuevos usuarios, niveles de acceso por perfil de usuario, asignaciones de software o datos para utilizar, consultar, modificar, borrar, etc.
- Aspectos administrativos: administrador u operadores (tareas, sueldos, capacitación, vacaciones, reemplazos, otros)
- Capacitación, planeación, ejecución y actualización
- Crecimiento de la red: periféricos, memoria, usuarios, software, aplicaciones
- Respaldo: datos, equipo, periféricos, software, aplicaciones, etc.
- Seguridad: controles, procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc.
- Otros que se consideren pertinentes

Telecomunicaciones

Administración
Instalación
Operación/seguridad

Objetivos de esta revisión

- Asegurar que exista una función formal de administración de la red de comunicaciones (RC)
- Asegurar la existencia de procedimientos y controles que orienten a la satisfacción de:
 - La administración de la RC
 - La instalación de la RC
 - La operación y seguridad de la RC (véase cuestionario de Seguridad para mayor detalle)
 - El mantenimiento de la RC
- Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio la RC existente
- Verificar que existan parámetros de medición del desempeño de la RC (bitácoras, gráficas, estadísticas, entre otros)
- Evaluar el grado de soporte que se brinda a los usuarios de la RC en el uso de sistemas y software al que tienen acceso en la misma
- Determinar si existen los suficientes controles y procedimientos de seguridad para la RC de la empresa

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

Nota: Esta evaluación se aplica a los responsables de la red de telecomunicaciones y, de ser necesario, a los usuarios de la misma.

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla E.2)

Tabla E-2

Métodos, técnicas y herramientas requeridas	Comunicaciones	Hardware	Software	Seguridad
Metodología de desarrollo e implantación de sistemas	No	No	Sí	Sí
Metodología de planeación	Sí	Sí	Sí	Sí
Cuestionarios	Sí	Sí	Sí	Sí
Entrevistas	Sí	Sí	Sí	Sí
Observación / monitoreo	Sí	Sí	Sí	Sí
Análisis / diseño	Sí	Sí	Sí	Sí
Trabajo en equipo	Sí	Sí	Sí	Sí
Análisis costo / beneficio	Sí	Sí	Sí	Sí
Documentación	Sí	Sí	Sí	Sí
Pruebas de auditoría	Sí	Sí	Sí	Sí
Control de proyectos	Sí	Sí	Sí	Sí
Índices de producción (benchmarking)	Sí	Sí	Sí	Sí

Administración

1. ¿La empresa cuenta con una RC?
 - 1.1 Si es así, ¿qué tipo de enlaces tiene (satelitales, terrestres)?
 - 1.2 ¿Qué software de comunicaciones utiliza para el manejo de la RC? ¿Cuáles son las versiones correspondientes?
 - 1.3 Si no tiene una RC, ¿piensa integrar una a la empresa? ¿Cuándo?
 - 1.4 ¿Existe una administración formal de la RC?
 - 1.5 En caso de no tener una administración formal de la RC, indique cómo se da seguimiento a los siguientes aspectos:
 - Planeación de nueva tecnología de información (hardware, software, etc.) para la RC
 - Monitoreo de las actividades de la operación y mantenimiento de la RC
 - Procedimientos de control y seguridad
 - Aspectos legales del software instalado
 - Capacitación y soporte a usuarios, operadores y técnicos de la RC
 - Otros
 - 1.6 Si la empresa tiene administración de la RC, ¿cuáles de las funciones mencionadas en la tabla E.3 realiza; con qué tareas efectúa cada función y cómo les dan seguimiento sus coordinadores o jefes inmediatos?
2. ¿Algún personal externo interviene en la administración de la RC mencionada?
 - 2.1 Si es así, mencione cuál y por qué.
3. ¿Hay documentación formal que especifique qué hacer y cómo realizar cada una de las funciones de administración de la RC?
 - 3.1 Si es así, ¿las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación?
4. En caso de que no exista esta documentación, ¿cómo se indica al personal responsable de la RC y a los usuarios lo referente a los puntos mencionados en la pregunta 1?
5. ¿Se cuenta con un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios?
6. ¿Cómo se canalizan dudas, sugerencias y compromisos entre los usuarios y los responsables de la RC?
7. ¿Qué garantiza que se está utilizando la tecnología de RC más adecuada para el negocio?
8. ¿Existen análisis costo/beneficio de las diferentes estrategias de la RC implantada? ¿Son aprobados de manera formal?

Tabla E.3 Administración de telecomunicaciones

Función	Tareas	Acciones de seguimiento
Planeación:		
<ul style="list-style-type: none">• Definir un plan formal que contemple:• Evaluación de la red de comunicaciones (si existe)		
<ul style="list-style-type: none">- Análisis y evaluación de la red de comunicaciones: diseño, uso, costo/beneficio- Análisis y diagnóstico de módems, controladores, cables, medios de transmisión, etc.- Otros		
<ul style="list-style-type: none">• Evaluación del software actual de la red de comunicaciones:		
<ul style="list-style-type: none">- Análisis y diagnóstico del software instalado para el uso de la red de comunicaciones- Software de monitoreo- Cantidad de licencias, copias pirata, versiones, número de usuarios- Software por legalizar- Otros		
<ul style="list-style-type: none">• Estudio de justificación de instalación o reemplazo de la red de comunicaciones local:		
<ul style="list-style-type: none">- Hardware requerido: módems, multiplexores, antenas, etc.- Configuración de la red de comunicaciones: distribución física, interfases, etc.- Software requerido: operación, seguridad, monitoreo, etc.- Evaluación costo/beneficio- Procedimientos de capacitación, seguridad, operación, mantenimiento, monitoreo, etc.		

Tabla E.3 Administración de telecomunicaciones (continuación)

Función	Tareas	Acciones de seguimiento
Organización		
<ul style="list-style-type: none"> • Elaboración de políticas y procedimientos para: <ul style="list-style-type: none"> • La evaluación de hardware, software, etc., de la red de comunicaciones • Adquisición o instalación de hardware o software de la red de comunicaciones • Asignación y baja de usuarios en la red de comunicaciones • Administración de la red de comunicaciones • Nivel de servicios para usuarios de la red de comunicaciones: <ul style="list-style-type: none"> - Desempeño en tiempos de respuesta, proceso, atención a fallas, otros - Capacitación, soporte y mantenimiento del hardware, software y aplicaciones • Operación de equipo, software y aplicaciones • Seguridad de datos, software, hardware, aplicaciones y accesorios 		

Instalación

Aspectos clave por evaluar:

1. ¿Hay procedimientos que aseguren la oportuna y adecuada instalación de los diferentes componentes de la RC conforme se realizan los contratos y compras formales de los mismos?

Procedimientos	Responsables de ejecutarlos	Responsables de seguimiento



2. Mencione las actividades que se realizan durante el proceso de instalación de los componentes de la RC (hardware, software, procedimientos, etc.):

Actividades	Responsables de ejecutarlos	Responsables de seguimiento
-------------	-----------------------------	-----------------------------

3. ¿Las compras de los diferentes elementos de la RC, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla?
4. ¿En caso de que las compras e instalación de componentes de la RC, sea hardware, software, etc., no hayan sido planeados formalmente, ¿cómo se justifican ante los responsables de informática y de las áreas usuarias involucradas en el uso de dicha RC?
5. En cuanto a la instalación del software, ¿cómo se aseguran que éste haya sido comprado legalmente? ¿Cómo se aseguran de que no sea instalado en otros equipos de la empresa sin licencia de uso? ¿Qué hacen cuando detectan algunas anomalías al respecto?
 - 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección de dicho software?
6. Cuando el encargado de la instalación parcial o total de cualquiera de los elementos que componen la RC es externo, ¿cómo se asegura la empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confiabilidad?
7. ¿Tiene alguna(s) sugerencia(s) que apoyen el proceso de instalación?

Operación y seguridad

1. ¿Se cuenta con manuales de operación de la RC? ¿Contemplan aspectos de seguridad?
 - 1.1 Si es así, ¿el personal responsable de administrar y operar la RC fue capacitado y preparado para el manejo de la misma? ¿Le da seguimiento a la seguridad?
 - 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?
2. ¿Existen estándares relativos a la operación y administración?, por ejemplo:
 - Estándares de desempeño:
 - Tiempos de respuesta
 - Tráfico (volumenes de información, velocidad)

- Interrupciones
 - Tiempo de recuperación de la RC
 - Equipos o terminales interconectados
 - Otros
 - Estándares de mantenimiento:
 - Calendarios (fechas, horarios, etc.)
 - Responsables
 - Otros
- 2.1 Si existen, ¿los responsables de la RC los aplican de manera formal?
 - 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos?
 - 2.3 Una vez que se aplican estos estándares, ¿qué datos se envían a otras áreas (usuarios, auditoría en informática)?
 - 2.4 ¿Los costos por el uso de la RC se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios?
 - 2.5 ¿Existe otro procedimiento para establecer los costos derivados por el uso de la RC? Si es así, ¿cuál es?
 - 2.6 ¿El usuario aprueba formalmente este procedimiento de pago?
3. ¿Se desarrolló o adquirió algún cuestionario estándar que permita saber el nivel de servicios que brinda la RC?
 - 3.1 Si es así, ¿con qué periodicidad se distribuye este cuestionario entre los usuarios o encargados de la RC?
 - 3.2 ¿Qué indicadores o parámetros importantes resultan de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática?
 4. ¿Se tienen procedimientos que protejan los datos transmitidos de una RC propia a otra(s)?
 - 4.1 Si se tienen, ¿cuáles son?
 - 4.2 ¿Existe un responsable o un software de comunicaciones que revise de manera permanente que los datos sean transmitidos con los estándares de oportunidad, totalidad, exactitud y autorización de una RC a otra(s)?
 - 4.3 ¿Existen registros con información relevante para el administrador de la RC o el auditor en informática?
 - 4.4 Si es así, señale si contienen la siguiente información:
 - Usuarios que accedieron la RC
 - Operaciones realizadas en la RC (envío, recepción)
 - Tiempos de conexión
 - Interrupciones durante el uso de la RC
 - Causas
 - Tiempo para reinicializar cada interrupción

- Terminales o equipos conectados
 - Accesos invalidados a la RC
 - Terminales donde se llevaron a cabo estos accesos no autorizados
 - Otros
- 4.5 ¿Estos registros son generados por algún software de RC o los elaboran de manera independiente los responsables de la administración de la misma?
5. Indique si se tiene identificada formalmente la siguiente información:
- Usuarios de la RC
 - Registros y niveles de acceso
 - Terminales conectadas
 - Responsables
 - Procedimientos de contingencia
 - Software
 - Periféricos conectados
 - Componentes
 - Otros
- 5.1 ¿Estos registros son generados por algún software de la RC o por los responsables de su administración?
6. ¿Existe una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios de la RC?
7. ¿Hay un procedimiento formal para dar un servicio oportuno y eficiente a los requerimientos de los usuarios?
- 7.1 ¿Lo conocen éstos?
8. ¿La RC cuenta con controles de acceso para personas no autorizadas (equipo, datos y software)?
- 8.1 En caso de tener esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado a la RC?
- 8.2 Si es así, ¿cuáles son esos controles y quiénes son los responsables de darles seguimiento?
- 8.3 ¿Verificar que los controles contemplen al menos:
- Protección a datos transmitidos a través de la RC
 - Protección a los componentes de la RC
 - Métodos para prevenir el monitoreo no autorizado de la RC
 - Detección inmediata y automatizada de accesos no autorizados a la RC
 - Contraseñas que autoricen el acceso a la RC y eviten la entrada en archivos no autorizados
 - Otros

9. ¿Existen controles relativos a la seguridad física de los diversos componentes de la RC (tarjetas, terminales, manuales, software, documentación, etc.)?
 - 9.1 En caso de contar con esos controles, ¿cómo se aseguran los responsables de darles seguimiento?
 - 9.2 Verificar que los controles cuenten con:
 - Protección adecuada de los componentes de la RC (cables, tarjetas, terminales, servidores, etc.)
 - Guardias o personal que vigile el acceso al centro de telecomunicaciones
 - Bitácoras de acceso en las áreas conectadas a la RC
 - Métodos de control de acceso como pases, tarjetas de identificación, puertas con candados, monitores, entre otros
 - Listado de personal con acceso autorizado a las terminales y controladores de la RC
 - Otros
10. ¿Se tiene un seguro que proteja el software y el equipo de la RC?
11. ¿Hay alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en la RC?
12. ¿Estos convenios están formalizados?
13. ¿Se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo de la RC del negocio como las siguientes?
 - Evaluación periódica de la RC: hardware, software, grado de satisfacción, grado de utilización, etc.
 - Acceso a la RC: nuevos usuarios, niveles de acceso por perfil de usuario, asignaciones de software o datos para utilizar, consultar, modificar, borrar, etc.
 - Aspectos administrativos: administrador u operadores (tareas, sueldos, capacitación, vacaciones, reemplazos, entre otros)
 - Capacitación: planeación, ejecución y actualización
 - Crecimiento de la RC: multiplexores, enlaces, usuarios, módems y medios de transmisión
 - Respaldo: datos, equipo, medios de transmisión, software, por mencionar algunos
 - Seguridad: controles, procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc.
 - Otros que se consideren pertinentes

AUDITORÍA DEL HARDWARE

1. Administración
2. Instalación
3. Operación y seguridad

Objetivos de esta revisión

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

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

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla E.2)

1. Administración

1. ¿La empresa cuenta con microcomputadoras, minicomputadoras o *mainframes*?
 - 1.1 Si es así, ¿cuántos tipos de equipo tiene? (Mencione sus características básicas, periféricos y atributos básicos de éstos.)
 - 1.2 ¿Qué software (paquetes, lenguajes, sistemas de información, sistemas operativos, bases de datos, etc. hay instalados? ¿Cuáles son las versiones correspondientes?
 - 1.3 ¿Existe una administración formal del equipo?

- 1.4 En caso de no tener una administración formal del equipo de cómputo, ¿con qué cuenta la empresa, esto es, cómo se da seguimiento a los siguientes aspectos?
 - Planeación de nueva tecnología de información (hardware, software, etc.)
 - Monitoreo de la operación y mantenimiento del equipo
 - Procedimientos de control y seguridad del equipo
 - Aspectos legales del software instalado en los equipos
 - Capacitación y soporte a usuarios
 - Otros
- 1.5 Si no se cuenta con administración del hardware, ¿cuáles de las funciones mencionadas en la tabla F.1 realiza; con qué tareas efectúa cada función y cómo les dan seguimiento sus coordinadores o jefes inmediatos?
2. ¿Algún personal externo interviene en la administración del equipo?
 - 2.1 Si es así, ¿quién y por qué?
3. ¿Existe la documentación que especifique qué hacer y cómo hacer cada una de las funciones de administración del equipo?
 - 3.1 Si es así, ¿las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación?
4. En caso de que no exista esta documentación, ¿cómo se indica al personal responsable del equipo y a los usuarios lo referente a los puntos mencionados en la pregunta 1?
5. ¿Existe un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios?
6. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre usuarios y responsables del equipo?
7. ¿Qué garantiza que se está utilizando la tecnología de hardware más adecuada para el negocio?
8. ¿Existen análisis costo/beneficio de las diferentes estrategias de hardware implantadas? ¿Son aprobados de manera formal?

2. Instalación

Aspectos clave por evaluar:

1. ¿Existen procedimientos que aseguren la oportuna y adecuada instalación de los diferentes componentes del equipo conforme se realicen los contratos y compras formales de los mismos?

Procedimientos	Responsables de ejecutarlos	Responsables del seguimiento

Tabla F.1 Administración del Hardware

Función	Tareas	Acciones de seguimiento
Planeación:		
<ul style="list-style-type: none">• Definir un plan formal que contemple:<ul style="list-style-type: none">• Evaluación del hardware actual:<ul style="list-style-type: none">- Análisis y evaluación del equipo- Análisis y diagnóstico del número de equipos (por tipo), características, usuarios, etc.- Análisis y diagnóstico de periféricos- Otros• Evaluación del software actual:<ul style="list-style-type: none">- Análisis y diagnóstico del software instalado en los equipos de cómputo como graficadores, procesadores, etc.- Bases de datos- Lenguajes de programación, sistemas operativos, etc.- Cantidad de licencias, copias pirata, versiones, número de usuarios- Software por legalizar- Otros• Estudio de justificación de instalación/reemplazo del equipo de cómputo:<ul style="list-style-type: none">- Hardware requerido: micro, periféricos, etc.- Configuración del equipo: distribución física, interfases, etc.- Software requerido: aspectos legales, paquetes de cómputo, lenguajes de programación, sistemas operativos, etc.- Evaluación costo/beneficio- Procedimientos de capacitación, seguridad, operación, mantenimiento, monitoreo, etc.		

Tabla F.1 Administración del Hardware (continuación)

Función	Tareas	Acciones de seguimiento
Organización:		
<ul style="list-style-type: none"> • Elaboración de políticas y procedimientos para: <ul style="list-style-type: none"> • La evaluación de hardware, software, etc. del equipo • Adquisición o instalación de hardware o software • Asignación y baja de usuarios del hardware • Administración del equipo • Nivel de servicios para usuarios del equipo <ul style="list-style-type: none"> - Desempeño en tiempos de respuesta, proceso, atención a falla y otros - Capacitación, soporte y mantenimiento del hardware, software y aplicaciones • Operación de equipo, software y aplicaciones • Seguridad de datos, software, hardware, aplicaciones y accesorios 		

2. Mencione las actividades que se efectúan durante el proceso de instalación de los componentes de la tecnología adquirida (hardware, software, procedimientos, etc.):

Actividades	Responsables de ejecutarlos	Responsables del seguimiento

3. ¿Las compras de los diferentes elementos del equipo, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla?

4. En caso de que las compras e instalación de componentes del equipo (sean microcomputadoras, minicomputadoras, software, etc.) no hayan sido planeados formalmente, ¿cómo se justifican ante los responsables de informática y de las áreas usuarias involucradas en el uso de dicha tecnología?
5. En cuanto a la instalación de software, ¿cómo se aseguran que haya sido comprado legalmente? ¿Cómo se aseguran de que no sea instalado en otros equipos de la empresa sin tener licencia de uso? ¿Qué hacen cuando detectan algunas anomalías al respecto?
 - 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección de dicho software?
6. Cuando la instalación parcial o total de cualquiera de los elementos que componen el equipo de cómputo es realizada por personal externo, ¿cómo se asegura la empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confiabilidad?
7. ¿Tiene alguna(s) sugerencia(s) que apoyen el proceso de instalación?

3. Operación y seguridad

1. ¿Se cuenta con manuales de operación del equipo? ¿Contemplan aspectos de seguridad?
 - 1.1 Si es así, ¿el personal responsable de administrar y operar el equipo fue capacitado y preparado para el manejo del mismo? ¿Da seguimiento a la seguridad?
 - 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?
2. Indique si existen estándares relativos a la operación y administración como:
 - Estándares de desempeño:
 - Tiempos de respuesta
 - Tráfico (volumenes de información, velocidad)
 - Interrupciones
 - Tiempo de recuperación del equipo
 - Equipos o terminales interconectados
 - Otros
 - Estándares de mantenimiento:
 - Calendarios (fechas, horarios, etc.)
 - Responsables
 - Otros
- 2.1 Si existen, ¿son aplicados formalmente por los responsables del equipo?
- 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos?

- 2.3 Una vez que se aplican estos estándares, ¿qué datos se envían a otras áreas (usuarios, auditoría de informática)?
- 2.4 ¿Los costos por el uso del equipo se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios?
- 2.5 ¿Existe otro procedimiento para definir los costos derivados por el uso del equipo? Si es así, ¿cuál es?
- 2.6 ¿El usuario aprueba formalmente este procedimiento de pago?
3. ¿Se desarrolló o adquirió algún cuestionario estándar que permita establecer el nivel de servicios que brindan las microcomputadoras, minicomputadoras o *mainframes*?
 - 3.1 Si es así, ¿con qué periodicidad se distribuye este cuestionario a los usuarios o encargados del equipo?
 - 3.2 ¿Qué indicadores o parámetros importantes resultan de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática?
4. ¿Se tienen procedimientos que protejan los datos transmitidos de un equipo de cómputo a otro(s)?
 - 4.1 Si se tienen, ¿cuáles son?
 - 4.2 ¿Hay un responsable o un software de comunicaciones revisando que los datos sean transmitidos conforme los estándares de oportunidad, totalidad, exactitud y autorización de un equipo a otro(s)?
 - 4.3 ¿Se tienen registros con información relevante para el administrador del equipo o el auditor en informática?
 - 4.4 Si es así, ¿contienen información relativa a los puntos siguientes?
 - Usuarios que accedieron los diferentes equipos de cómputo
 - Operaciones realizadas en el equipo (envío, recepción)
 - Tiempos de conexión
 - Interrupciones durante el uso del equipo
 - Causas
 - Tiempo para reinicializar cada interrupción
 - Terminales o equipos conectados
 - Accesos invalidados a los diferentes equipos
 - Terminales donde se intentaron estos accesos no autorizados
 - Otros
 - 4.5 ¿Estos registros son generados por algún software o los producen de manera independiente los responsables de la administración de la misma?
5. ¿Se tiene identificada formalmente la siguiente información?
 - Usuarios del equipo
 - Registros y niveles de acceso

- Terminales conectadas en los diferentes equipos
 - Responsables del equipo
 - Procedimientos de contingencia
 - Software del equipo
 - Periféricos conectados a los equipos
 - Software original y pirata instalado en los equipos
 - Software duplicado de las micros
 - Tipos de CPU
 - Capacidad de discos y espacio libre por servidor y micros
 - Otros
- 5.1 ¿Estos registros son generados por algún software o por los responsables de la administración de la misma?
6. ¿Existe una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios del equipo?
7. ¿Se tiene un procedimiento formal para dar un servicio oportuno y eficiente a los requerimientos de los usuarios del equipo?
- 7.1 ¿Lo conocen los usuarios?
8. ¿Los equipos poseen controles de acceso a personas no autorizadas (equipo, datos y software)?
- 8.1 En caso de contar con esos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado a los equipos?
- 8.2 Si es así, ¿cuáles son esos controles y quiénes son los responsables de darles seguimiento?
- 8.3 Verificar que los controles contemplen al menos:
- Protección a archivos
 - Protección a programas fuente de las aplicaciones que están en los equipos
 - Protección a otro software alojado en los equipos
 - Métodos para prevenir el monitoreo no autorizado del equipo
 - Detección inmediata y automatizada de accesos no autorizados a los equipos
 - Contraseñas que autoricen el acceso a los equipos, sin permitir la entrada en archivos no autorizados
 - Otros
9. ¿Existen controles relativos a la seguridad física de los diversos componentes del equipo (tarjetas, terminales, manuales, software, documentación, entre otros)?
- 9.1 En caso de contar con esos controles, ¿cómo se aseguran los responsables de darles seguimiento?
- 9.2 Verificar que estos controles cuenten con:
- Protección adecuada de los componentes del equipo (cables, tarjetas, terminales, servidores, etc.)

- Guardias o personal que vigile el acceso al centro de telecomunicaciones
 - Bitácoras de acceso a las áreas conectadas al equipo
 - Métodos de control de acceso como pases, tarjetas de identificación, puertas con candados, monitores, etc.
 - Listado de personal con acceso autorizado a las terminales y controladores del equipo
 - Otros
10. ¿Se cuenta con un seguro que proteja el software y el equipo?
 11. ¿Se tienen alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en algunos de los equipos? ¿Tienen convenios con otras empresas?
 12. ¿Estos convenios están formalizados?
 13. Indique si se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo del hardware instalado en el negocio, como las siguientes:
 - Evaluación periódica del equipo: hardware, software, grado de satisfacción, grado de utilización, etc.
 - Acceso a los equipos de los nuevos usuarios, niveles de acceso por perfil de usuario, asignaciones de software o datos para utilizar, consultar, modificar, borrar, etc.
 - Aspectos administrativos: administrador u operadores, tareas, sueldos, capacitación, vacaciones, reemplazos, entre otros
 - Capacitación: planeación, ejecución y actualización
 - Crecimiento del equipo: periféricos, memoria, usuarios, software y aplicaciones
 - Respaldo: datos, equipo, periféricos, software, aplicaciones, entre otros
 - Seguridad: controles, procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc.
 - Otros que se consideren pertinentes



AUDITORÍA DEL SOFTWARE

1. Administración
2. Legalización e instalación
3. Operación y seguridad

Objetivos de esta revisión

- Asegurar que exista una función formal de administración del software
- Asegurar la presencia de procedimientos y controles que orienten a la satisfacción de:
 - La administración del software
 - La instalación del software
 - La operación y seguridad del software (véase cuestionario de Seguridad para mayor detalle)
 - La actualización del software
- Detectar el grado de confianza, satisfacción y desempeño que brinda al negocio el software existente
- Investigar si hay políticas que aseguren un proceso formal de:
 - Evaluación y selección del software por comprar
 - Contratos que aseguren la legalización, instalación, capacitación y actualización oportuna del software adquirido por la empresa
 - Seguimiento a las normas de utilización del software legal, no de copias
 - Evaluación permanente del software existente en el mercado
 - Evaluación permanente de nuevos requerimientos de software en el negocio
- Evaluar el grado de soporte que se brinda a los usuarios en el uso del software al que tienen acceso en los equipos de la empresa
- Determinar si existen los suficientes controles y procedimientos de seguridad para el software de la empresa
- Evaluar las acciones que se llevan a cabo para la actualización del software
- Asegurar que sólo se encuentre instalado software legalizado en todas las microcomputadoras o redes locales de la organización
- Analizar si se cuenta con algún sistema o paquete computacional que apoye el monitoreo y la auditoría del software instalado en los equipos del negocio

- Evaluar el grado de integración entre los diferentes tipos de software instalado en las computadoras del negocio

Nota: Esta revisión se aplica a los administradores de software y a los usuarios del mismo.

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla E.2)

1. Administración

1. ¿La empresa cuenta con microcomputadoras, minicomputadoras o *mainframes*?
 - 1.1 ¿Existe un documento que muestre la distribución del equipo y sus usuarios?
 - 1.2 ¿Qué software (paquetes, lenguajes, sistemas de información, sistemas operativos, bases de datos, etc.) hay instalado? ¿Cuáles son las versiones correspondientes?
 - 1.3 ¿Existe una administración formal del software? ¿Quién es el responsable?
 - 1.4 En caso de no tener esa administración formal, indique cómo se da seguimiento a los siguientes aspectos:
 - Planeación de nueva tecnología de información (hardware, software, etc.)
 - Monitoreo de las actividades de manejo y actualización del software
 - Procedimientos de control y seguridad
 - Aspectos legales del software instalado
 - Capacitación y soporte a usuarios
 - Otros
 - 1.5 Si se tiene tal administración, ¿cuáles de las funciones mencionadas en la tabla G.1 realiza; con qué tareas efectúa cada función y cómo les dan seguimiento sus coordinadores o jefes inmediatos?
2. ¿Hay personal externo que intervenga en las funciones de administración mencionadas?
 - 2.1 Si es así, mencione su especialización y por qué participa.
3. ¿Existe la documentación formal que especifique qué hacer y cómo llevar a cabo cada una de las funciones de administración del software?
 - 3.1 Si es así, ¿las funciones desarrolladas en la realidad concuerdan con las especificadas en la documentación?
4. En caso de que no exista esta documentación, ¿cómo se indica al personal responsable del equipo y a los usuarios lo referente a la pregunta 1?
5. ¿Existe un plan vacacional y de reemplazo de personal que asegure el servicio continuo a los usuarios?
6. ¿Cómo se canalizan las dudas, sugerencias y compromisos entre los usuarios y los responsables de la administración del software?
7. ¿Qué les garantiza que se está utilizando el software idóneo?
8. ¿Existen análisis costo/beneficio de las diferentes estrategias de software implantadas? ¿Se han aprobado formalmente?

Tabla G.1 Administración del software

Función	Tareas	Acciones de seguimiento
Planeación		
<ul style="list-style-type: none"> • Definir un plan formal que contemple: <ul style="list-style-type: none"> • Evaluación del software actual <ul style="list-style-type: none"> - Análisis y diagnóstico del software instalado en los equipos de cómputo (graficadores, procesadores, etc.) - Bases de datos - Lenguajes de programación, sistemas operativos, etc. - Cantidad de licencias, copias pirata, versiones, número de usuarios - Grado de satisfacción de los usuarios - Requerimientos no satisfechos - Costo/beneficio del software actual - Software por legalizar - Otros aspectos • Evaluación del hardware actual: <ul style="list-style-type: none"> - Distribución y ubicación del equipo donde está instalado el software (microcomputadoras, red, minis, mainframes) - Características (memoria, RAM, etc.)* • Estudio de justificación de instalación, actualización o reemplazo del software: <ul style="list-style-type: none"> - Software requerido: (aspectos legales, paquetes de cómputo, lenguajes de programación, sistemas operativos, etc.) - Hardware requerido: (micros, periféricos, etc.) - Evaluación costo/beneficio - Procedimientos de: capacitación, seguridad, operación, actualización, monitoreo, etc. 		
Organización		
<ul style="list-style-type: none"> • Elaboración de políticas y procedimientos para: <ul style="list-style-type: none"> • La evaluación del software • Adquisición o instalación • Autorización de su uso • Administración del software • Soporte a usuarios: capacitación, soporte y actualización • Manejo de software • Seguridad: acceso al software, modificación o destrucción 		

*Nota: véase cuestionario del hardware

2. Legalización e instalación

Aspectos clave por evaluar:

1. ¿Existen procedimientos que aseguren la oportuna y adecuada instalación del software conforme se hayan realizado los contratos y compras formales del mismo?

Procedimientos	Responsables de ejecutarlos	Responsables del seguimiento

2. Mencione las actividades que se realizan durante la instalación de la tecnología adquirida (software, hardware, procedimientos, entre otros):

Actividades	Responsables de ejecutarlos	Responsables del seguimiento

3. ¿Las compras del software, así como su instalación, se derivan de un proceso de planeación y evaluación formal? ¿Cómo se aseguran de que esto se cumpla?
4. En caso de que las compras e instalación del software no hayan sido planeadas formalmente, ¿cómo se justifica esto ante los responsables de informática y de las áreas usuarias?
5. En cuanto a la instalación del software, ¿cómo se aseguran de que éste haya sido comprado legalmente? ¿Cómo previenen que no sea instalado en otros equipos de la empresa sin licencia de uso? ¿Qué hacen cuando detectan algunas anomalías al respecto?
 - 5.1 ¿Quién es el responsable de las actividades de seguridad y control para garantizar el uso adecuado y la protección de dicho software?
6. Cuando son terceros (personal externo) los encargados de la instalación del software, ¿cómo se asegura la empresa de que esto se haga conforme a sus políticas y lineamientos de servicio, oportunidad y confiabilidad?
7. ¿Tiene alguna(s) sugerencia(s) que apoyen el proceso de instalación?

3. Operación y seguridad

1. ¿Se cuenta con manuales de operación? ¿Contemplan aspectos de seguridad?

- 1.1 Si es así, ¿el personal responsable de administrar o manejar el software fue capacitado y preparado para el manejo del mismo? ¿Se da seguimiento a la seguridad?
- 1.2 ¿Qué sucede cuando algunos de estos responsables salen de vacaciones, se incapacitan o dejan de laborar en la empresa?
2. Indique si existen estándares relativos a la operación y administración como:
 - Programas de capacitación:
 - Calendario de cursos
 - Costo de los cursos
 - Material empleado en los cursos
 - Lugares donde se impartirán los cursos
 - Evaluación de los cursos
 - Otros
 - Estándares de actualización:
 - Software por actualizar o reemplazar
 - Calendarios (fechas, horarios, etc.)
 - Responsables
 - Otros
- 2.1 Si existen estos estándares, ¿son aplicados formalmente por los responsables del software?
- 2.2 ¿Cómo se da seguimiento al cumplimiento de los mismos?
- 2.3 Una vez que se aplican estos estándares, ¿qué datos relativos a los resultados de los mismos se envían a otras áreas (usuarios, auditoría en informática, entre otros)?
- 2.4 ¿Los costos por el uso del software se determinan con estos parámetros o son costos uniformes y fijos que se distribuyen en sumas idénticas entre todos los usuarios?
- 2.5 ¿Existe otro procedimiento para establecer los costos derivados por el uso del software? Si es así, ¿cuál es?
- 2.6 ¿El usuario aprueba formalmente este procedimiento de pago?
3. ¿Se desarrolló o adquirió algún cuestionario estándar que permita saber el grado de utilización o satisfacción relativos al software?
 - 3.1 Si es así, ¿con qué periodicidad se distribuye entre los usuarios o encargados del software?
 - 3.2 ¿Qué indicadores o parámetros importantes resultan de estos cuestionarios que sean utilizados por los responsables de la gerencia o dirección de informática?
4. ¿Se tienen procedimientos que protejan los datos transmitidos de un equipo de cómputo a otro(s) generados por el uso del software?

- 4.1 Si se tienen, ¿cuáles son?
- 4.2 ¿Hay un responsable o un software de comunicaciones que revise permanentemente que los datos sean transmitidos con los estándares de oportunidad, totalidad, exactitud y autorización de un equipo a otro(s)?
- 4.3 ¿Existen registros con información relevante para el administrador del equipo o el auditor en informática?
- 4.4 Si es así, señale si contienen información relativa a:
 - Usuarios que accedieron los diferentes tipos del software (usuarios, programadores, otros)
 - Operaciones realizadas en el equipo (envío, recepción)
 - Interrupciones en el uso del equipo donde está instalado el software
 - Causas
 - Tiempo para reinicializar cada interrupción
 - Accesos invalidados a los diferentes tipos de software
 - Terminales donde se llevaron a cabo estos accesos no autorizados
 - Usuarios que intentaron estos accesos
 - Otros
- 4.5 ¿Estos registros son generados por algún software o por los responsables de la administración del mismo?
5. Indique si se tiene identificada formalmente la siguiente información:
 - Usuarios
 - Registros y niveles de acceso
 - Equipos donde se encuentra instalado cada tipo de software
 - Periféricos conectados a dichos equipos
 - Software original y pirata instalados en los equipos
 - Otros
- 5.1 ¿Estos registros son generados por algún software o por los responsables del mismo?
6. ¿Se cuenta con una línea telefónica disponible las veinticuatro horas del día para atención de quejas y dudas de los usuarios?
7. ¿Existe un procedimiento formal para dar un servicio oportuno y eficiente a los requerimientos de los usuarios?
 - 7.1 ¿Lo conocen los usuarios?
8. ¿Los equipos tienen controles de acceso a personas no autorizadas (equipo, datos y software)?
 - 8.1 En caso de contar con estos controles, ¿están diseñados para prevenir, detectar o corregir el acceso no autorizado a los diferentes tipos de software?
 - 8.2 Si es así, ¿cuáles son y quiénes son los responsables de darles seguimiento?

8.3 Verificar que tales controles contemplen al menos:

- Protección de archivos
- Protección a programas fuente de las aplicaciones que están en los equipos
- Protección a otro software alojado en los equipos
- Métodos para prevenir el monitoreo no autorizado del equipo
- Detección inmediata y automatizada de accesos no autorizados a los equipos
- Contraseñas que autoricen acceso a los equipos y eviten el acceso a archivos no autorizados
- Otros

8.4 Verificar que estos controles cuenten con:

- Bitácoras de acceso a las áreas donde se encuentre el equipo y el software
- Métodos de control de acceso como pases, tarjetas de identificación, puertas con candados, monitores, etc.
- Listado de personal con acceso autorizado a las terminales y controladores del equipo
- Otros

9. ¿Se tiene un seguro que proteja el software y el equipo?
10. ¿Se tienen alternativas que apoyen a la empresa en caso de una falla generalizada y prolongada en algunos de los equipos? ¿Cuenta con convenios con otras empresas?
11. ¿Estos convenios están formalizados?
12. Indique si se han tomado en cuenta algunas consideraciones complementarias que ayuden al mejoramiento continuo del software instalado en la empresa como las siguientes:
 - Evaluación periódica del software y el equipo donde está instalado: hardware, software, grado de satisfacción, grado de utilización, etc.
 - Acceso a los equipos: nuevos usuarios, niveles de acceso por perfil de usuario, asignaciones de software o datos por utilizar, consultar, modificar, borrar, entre otros
 - Aspectos administrativos: administrador u operadores (tareas, sueldos, capacitación, vacaciones, reemplazos, otros)
 - Capacitación: planeación, ejecución y actualización
 - Crecimiento del equipo: periféricos, memoria, usuarios, software y aplicaciones
 - Respaldo: datos, equipo, periféricos, software, aplicaciones, entre otros
 - Seguridad: controles, procedimientos, software de auditoría, niveles de acceso, planes de contingencia, plan de reinicialización y recuperación, etc.
 - Otros que se consideren pertinentes



AUDITORÍA DE SEGURIDAD

1. Hardware
2. Aplicaciones del software
3. Plan de contingencias y de recuperación

Objetivos de esta revisión

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

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

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla E.2)

1. Hardware

Aspectos por evaluar:

1. ¿Hay políticas y procedimientos relativos al uso y protección del hardware de la organización?

1.1 Si existen, indique si están formalmente identificados los siguientes aspectos de seguridad:

- Administración del hardware
- Micros, minis y supercomputadoras (*mainframes*)
 - Tecnología de comunicaciones, redes, etc.
 - Cuantificación del hardware
 - Descripción del hardware (características básicas)
 - Distribución del hardware (ubicación física)
 - Áreas de informática: departamentos usuarios y áreas locales y remotas
 - Registro del hardware instalado, dado de baja, en proceso de adquisición, etc.
 - Uso del hardware: desarrollo, operación, mantenimiento, monitoreo y toma de decisiones
 - Funciones responsables del control del hardware
 - Otros
- Procedimientos y controles de seguridad para la evaluación, selección y adquisición de hardware
- Políticas enfocadas a comprobar que el software adquirido cubra los siguientes puntos:
 - Módulos de seguridad: acceso al hardware (llaves de seguridad, por ejemplo); uso del hardware (facilidades de monitorear la operación) y bitácoras de uso del hardware (quién, cuándo, para qué, entre otros puntos)
- La actualización del hardware:
- Políticas orientadas a confirmar que el hardware actualizado cubra los siguientes puntos:
 - Autorización del hardware por medio de la justificación de la actualización
 - Impacto de la implantación del hardware en el medio de informática: aplicaciones, software y costos
 - Implicaciones de control en la implantación y uso del hardware actualizado
- Reemplazo del hardware
- Políticas para verificar que el hardware reemplazado cubra los siguientes puntos:
 - Autorización por medio de la justificación del reemplazo
 - Impacto de la implantación en el medio de informática: aplicaciones, hardware y costos
 - Implicaciones de control en la implantación y uso del hardware nuevo

2. En cuanto al equipo de soporte, se han de tener los siguientes datos:

- Localización física de:
 - Aire acondicionado
 - Equipo *No-Break*

- Equipos contra Incendios
- Otros

3. ¿La ubicación física del equipo de cómputo en el edificio es la más adecuada pensando en los diversos desastres o contingencias que se pueden presentar (manifestaciones o huelgas, inundaciones, incendios, otros)?

Nota: Verificar si el edificio cuenta con instalaciones de escape en casos de emergencia.

4. ¿Hay procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de desastres o contingencias?

4.1 Si es así, ¿están documentados y difundidos formalmente?

5. Indique si se cuenta con controles y procedimientos para:

- Clasificación y justificación del personal con acceso a los centros de cómputo del negocio y a las oficinas donde se encuentra papelería o accesorios relacionados con informática
- Restringir el acceso a los centros de cómputo sólo al personal autorizado
- Definición y difusión de las horas de acceso al centro de cómputo
- Uso y control de bitácoras de acceso a los centros de cómputo
- Definir la aceptación de la entrada a visitantes
- Manejo de bitácoras especiales para los visitantes a los centros de cómputo

Nota: Comprobar el cumplimiento de estos controles y procedimientos.

6. ¿Existe personal de seguridad encargado de la salvaguarda de los equipos de cómputo de la empresa?

6.1 ¿Fue capacitado el personal para este trabajo o simplemente sigue las normas de seguridad que se aplican en bancos o industrias?

6.2 Si no se cuenta con tal personal, ¿a qué área o función pertenecen los responsables de proteger físicamente el equipo?

Nota: Analizar el grado de confianza que brinda dicho personal a la protección de estos activos de la empresa.

7. Mencione si existen políticas relacionadas con el ingreso y salida del hardware que aseguren al menos lo siguiente:

- Que la entrada y salida del hardware sea:
 - Revisada (contenido, cantidad, destino)
 - Justificada (compra, pruebas, reemplazo, devolución, dado de baja, otros)
 - Aprobada por el responsable de informática que va a recibirlo
 - Registrada (responsables, hora, motivo, etc.)
 - Devuelta (comparar con la fecha estimada de salida)

- Devuelta en las mismas condiciones de entrada
 - Devolución autorizada por medio de un responsable de informática
8. ¿Existe alguna función de investigación, auditoría o seguridad que se dedique a la evaluación permanente de software, métodos, procedimientos, etc., sugeridos en el mercado (como conferencias, publicaciones, asesores, investigaciones) para la implantación de nuevas acciones relativas a la seguridad que brinden continuidad en la operación y cuidado de los recursos relacionados con informática?
- 8.1 Si es así, ¿cuáles son las actividades principales que se asignan a esta tarea?
- 8.2 En caso de que lo anterior no ocurra, ¿qué acciones garantizan la adecuación de los controles y procedimientos de seguridad en el momento de implantar nuevas tecnologías?

2. Aplicaciones del software

Aspectos clave por evaluar:

1. ¿Se tienen políticas y procedimientos relativos al uso y protección del software existente?
 - 1.1 Si las hay, indique si los siguientes aspectos de seguridad están formalmente identificados:
 - Administración del software
 - Sistemas operativos, utilerías, paquetes, etc.
 - Cuantificación del software (original y copias)
 - Descripción (por original)
 - Distribución (en qué equipos o dispositivos de almacenamiento secundarios se encuentra, en qué lugar físico se localizan: áreas del negocio, bancos, etc.)
 - Registro del software instalado, dado de baja, en proceso de adquisición, etc.)
 - Uso del software (tipo de uso, responsables de su uso, entre otros puntos)
 - Procedimientos y controles de seguridad para la evaluación, selección y adquisición de software
 - Políticas para verificar que el software adquirido cubra los siguientes puntos:
 - Módulos de seguridad para acceso al software, uso y bitácoras de uso (quién, cuándo, qué, etc.)
 - La actualización del software
 - Políticas para confirmar que el software actualizado cubra los siguientes puntos:
 - Autorización del mismo por medio de la justificación de la actualización
 - Impacto de la implantación en el medio de informática, aplicaciones, hardware y costos

- Implicaciones de control en la implantación y uso del software actualizado
 - Reemplazo del software actual por otro
 - Políticas para asegurar que el software reemplazado cubra los siguientes puntos:
 - Autorización por medio de la justificación del reemplazo
 - Impacto de la implantación en el medio de informática: aplicaciones, hardware y costos
 - Implicaciones de control en la implantación y uso del software nuevo
2. Diga si poseen políticas relacionadas con el ingreso y salida del software que aseguren al menos lo siguiente:
- Que el software que salga de la empresa sea:
 - Revisado (contenido, cantidad, destino)
 - Esté registrado formalmente en la empresa
 - Justificado
 - Aprobado por el responsable de informática
 - Registrado (quién y a qué hora lo sacó)
 - Devuelto (comparar con fecha estimada de devolución)
 - Devuelto en las mismas condiciones en que salió
 - El personal esté comprometido formalmente a no hacer un mal uso del mismo (copiarlo, dañarlo, modificarlo, etc.)
 - Que el software que ingrese a la empresa sea:
 - Revisado (contenido, cantidad, destino)
 - Justificado (evaluación, prueba o respaldo de las aplicaciones del negocio)
 - Aprobado por el responsable de informática
 - Registrado (quién y a qué hora lo metió)
 - Devuelto (Comparar con la fecha estimada de devolución)
 - Devuelto en las mismas condiciones que tenía en la salida
 - El personal esté comprometido formalmente a no hacer un mal uso del mismo (copiarlo, dañarlo, etc.)
3. En cuanto a las aplicaciones (sistemas de información) que se desarrollan en la empresa, ¿se tienen los controles y procedimientos necesarios para garantizar la seguridad mínima requerida?
- 3.1 En caso de que existan, ¿al menos contemplan lo siguiente?
- Procedimientos de llenado de documentos fuente
 - Procedimientos de uso de la computadora
 - Encendido e inicialización del equipo
 - Reinicialización del equipo en caso de fallas
 - Manejo de bitácoras de uso de la computadora
 - Monitoreo de uso de la computadora

- Niveles de acceso (perfil de usuarios) a los módulos de:
 - Captura
 - Actualización
 - Consulta
 - Generación de reportes
 - RespalDOS
 - Otros
 - Procedimientos de uso de los módulos de:
 - Captura
 - Actualización
 - Consulta
 - Generación de reportes
 - RespalDOS
 - Otros
4. ¿Existen procedimientos que verifiquen que la construcción (programación), prueba e implantación de los controles y procedimientos de seguridad sean formalmente aprobados antes de que se utilice el sistema?
 5. ¿Participan funciones de control o evaluación de sistemas, como auditores o consultores, en la aprobación de los controles de seguridad de los sistemas antes de que sean formalmente aprobados por los usuarios?
 - 5.1 Si es así, ¿en qué etapas del desarrollo participan?
 - 5.2 ¿Se involucran en todos los proyectos de desarrollo?
 6. Mencione si los controles aseguran que el sistema contemple los procedimientos necesarios para que la información manejada en el mismo sea total, exacta, autorizada, mantenida y actualizada
 - 6.1 ¿Existen procedimientos para comprobar que los totales de los reportes de validación del usuario concuerden con los totales de validación del sistema computarizado?
 - 6.2 ¿Los documentos fuente por capturar llevan preimpresos sus números consecutivos o se los asigna el usuario? Si ocurre lo último, ¿hay alguno de los controles mencionados a continuación dentro del sistema que valide la no repetición o exclusión de algún número consecutivo?
 - Control de disquetes, cintas, papelería, etc.
 - Control de todos los movimientos o transacciones rechazados por el sistema (comprobar que los datos erróneos para el sistema sean registrados, corregidos, alimentados correctamente y actualizados)
 - Entendimiento y buen uso de los mensajes del sistema, como manejo de errores
 - Uso de bitácoras por parte de usuarios y personal de informática como pistas para auditoría

Nota: Revisar todos los posibles controles que debe asumir el sistema y que corresponden también al usuario.

- 6.3 ¿Cómo se aseguran que durante la operación del sistema se den los controles mencionados en el punto 6?

Nota: Comprobar que existan cifras de control manuales o automatizadas antes, durante y después de la operación de los sistemas que aseguren exactitud, totalidad, etc., de los datos.

- 6.4 ¿Cómo se aseguran que al estar el sistema en operación se cumplan formal y oportunamente los procedimientos de seguridad contemplados en el desarrollo del mismo?

- a) Con una auditoría de sistemas
- b) Con revisiones de consultores externos
- c) Con revisiones del personal de informática

Nota: Analizar si las revisiones son planeadas o surgen de la administración por crisis.

- 6.5 ¿Cómo se aseguran de que los manuales de usuario, técnicos y de operación cumplan con los estándares de la metodología de CVDS y de que sean completos?

- 6.6 ¿Cómo se aseguran de que el personal que va a utilizar estos manuales se encuentre capacitado en el uso de los mismos?

- 6.7 ¿Se documentan todas las debilidades derivadas de la revisión del cumplimiento de controles y procedimientos de seguridad durante la operación de los sistemas?

- 6.8 Si es así, indique si los clasifican en:

- Debilidades en los procedimientos de entrada, proceso o salida
- Entendimiento o manejo del equipo donde se encuentran los sistemas
- Dificultades en la comunicación usuarios-informática para el manejo de nuevos requerimientos o cambios a los sistemas
- Otros

7. En cuanto al mantenimiento de sistemas señale si se cuenta con un procedimiento formal para asegurar que los cambios efectuados en los sistemas sean:

- Justificados (apoyo a los requerimientos de usuarios)
- Descritos (objetivos, función, etc.)
- Probados en el área de desarrollo antes de ser trasladados al área de producción
- Revisados por funciones de control (auditoría de sistemas, consultores, entre otros)

- Aprobados por los responsables correspondientes antes de ser puestos en operación
- Registrados en bitácoras de cambios
- Actualizados en la documentación correspondiente como manuales de usuario, técnicos y de operación
- Implantados los controles de seguridad de dichos cambios
- Otros

8. ¿Hay un procedimiento formal para asegurar que los requerimientos de los departamentos usuarios sean registrados, justificados, programados, probados e implantados de acuerdo con los estándares de la metodología del CVDS?

Nota: Conviene asegurarse de que este punto esté relacionado estrechamente con el séptimo punto.

9. ¿Cómo se da seguimiento a los cambios de los sistemas sugeridos por la función de informática?

Nota: Asegúrese de que si estos cambios van a ser implantados en los sistemas, sigan la pauta del séptimo punto.

10. ¿Existen procedimientos que permitan identificar con claridad las responsabilidades en cuanto al uso del sistema y equipo de cómputo donde será implantado y operado?
11. ¿Qué procedimiento se utiliza para liberar formalmente el sistema?
 - 11.1 Indique si se registran todos los sistemas liberados y aprobados formalmente por los usuarios, auditores, función de informática, consultores, etc.
12. Una vez que el sistema está en operación, ¿qué funciones verifican que los controles y procedimientos relativos a la seguridad se cumplan de manera satisfactoria?
13. ¿Los responsables de modificar los programas fuente del sistema en operación están bien definidos?
 - 13.1 Si es así, ¿cómo se aseguran de que sólo ellos tengan acceso a dichos programas?
 - 13.2 ¿Cómo se aseguran que sólo se modifiquen programas autorizados en términos formales y que se documenten en los manuales correspondientes?
 - 13.3 ¿Cómo se aseguran los responsables de estos cambios de incluir los controles de seguridad?
14. ¿Hay un registro de los archivos existentes en cada sistema en operación (maestros y de movimientos)?
 - 14.1 Si es así, ¿existe un procedimiento que asegure que sólo sean accesados por personal autorizado?

- 14.2 ¿Se tiene algún procedimiento para especificar cuáles funciones se actualizarán, consultarán o eliminarán información de los archivos de los sistemas en operación?
- 14.3 ¿Están clasificados los procedimientos para actualizar archivos en línea o en lote?
15. ¿Se cuenta con procedimientos de respaldo de los programas fuente, de la documentación y de los archivos en operación?
16. ¿El respaldo de la información se encuentra en el mismo edificio?
17. ¿Sucede lo mismo con el equipo de cómputo?
18. ¿Se tienen controles para que sólo personal autorizado tenga acceso a dichos respaldos?

3. Plan de contingencias y de recuperación

Aspectos clave por evaluar:

1. ¿Considera que tanto la alta dirección, usuarios como el personal de informática están conscientes de que todos los recursos relacionados con la informática son activos del negocio y deben protegerse de una manera formal y permanente? ¿Por qué?
- 1.1 ¿Cuáles de los siguientes recursos vinculados con informática son más importantes para la organización y cuáles tienen más y mejores métodos de protección para seguir operando y apoyando los objetivos del negocio en condiciones optimas?

Recursos	Grado de importancia (B/I/N/M/NS)	Métodos formales para su protección
Humanos		
Materiales		
Financieros		
Tecnológicos		
De información		

* B = básico I = importante N = necesario M = mínimo NS = no se sabe

Nota: Comprobar que los recursos considerados básicos, importantes o necesarios tengan los métodos de seguridad para prevenir y enfrentar contingencias; en caso de que no existan, se podrá observar que dichas consideraciones son más teóricas que prácticas. En cuanto a los recursos de importancia mínima o desconocida, se preguntará el por qué de tales afirmaciones.

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

- 1.3 Indique si dichos planes contemplan los siguientes aspectos:
- Red de comunicaciones (RC)
 - Hardware
 - Software, aplicaciones, datos
 - Recursos humanos
 - Lugares físicos donde se localizan los recursos anteriores
 - Otros
- 1.4 Si es así, ¿fueron difundidos formalmente en toda la organización?
- 1.5 ¿Fueron elaborados por terceros, personal de informática, usuarios o se trató de un proyecto donde intervinieron varias áreas del negocio?
2. En el proceso de planeación de contingencias y recuperación y de su implantación en la empresa, indique cuáles fueron las tareas realizadas, cuáles están pendientes, cuáles en desarrollo y quiénes son sus responsables:

Tarea	Situación (D/T/NI)	Productos terminados
1. Definición de metas y objetivos del plan		
2. Evaluación e identificación de riesgos		
3. Elaboración de acciones, políticas y procedimientos por tipo de riesgo		
4. Documentación del plan		
5. Aprobación y difusión del plan		
6. Simulación del plan		
7. Actualización del plan		

* D = en desarrollo T = terminada NI = no iniciada

- 2.1 ¿Se han presentado contingencias que hayan sido enfrentadas con el plan de contingencias y de recuperación diseñado para la empresa? ¿Con qué resultados?
- 2.2 Si no tienen este plan, ¿qué acciones han tomado para enfrentar tales eventualidades y quiénes han sido los responsable de ejecutarlas?
3. Señale si poseen una función responsable de seguridad que verifique y de seguimiento a los siguientes puntos:
- Actualización formal de los planes
 - Capacitación a los usuarios y personal de informática en cuanto a la aplicación de los procedimientos contemplados en los planes

- Supervisión y orientación en la ejecución de simulacros
 - Asignación de los reponsables de la ejecución de las actividades contempladas en los planes para:
 - Prevención de contingencias
 - Apoyo a la empresa en casos de desastres o de contingencias con el fin de reducir en lo posible las pérdidas humanas, equipos, datos, etc.
 - Reinicio inmediato o en el tiempo mínimo posible de las operaciones de la empresa
 - Otros
4. ¿Las funciones involucradas en dichos planes los han probado?
 5. ¿Contemplan todas las contingencias o desastres probables en la(s) localidad(es) donde tiene instalaciones la organización (huelgas, diluvios, robos, incendios, otros)?
 6. ¿Los planes cubren los procedimientos necesarios para prevenir los elementos causales o restaurar los primordiales?
 7. ¿Se clasificó el orden en que reiniciará la operación de cada aplicación de acuerdo con las prioridades y estrategias del negocio?
 8. ¿Existen acuerdos con empresas o proveedores que tengan la misma tecnología (o que sea la más compatible)?
 9. Mencione si se cuenta con contratos legales que aseguren los siguientes elementos de la función de informática y de los departamentos usuarios:
 - Personal (de informática y usuarios), equipos de cómputo, software, aplicaciones, telecomunicaciones, edificios o instalaciones, entre otros
 10. ¿Existe algún procedimiento formal para efectuar todo el proceso de evaluación, selección y contratación de los seguros? ¿Cuáles son dichos procedimientos?
 - 10.1 ¿Quiénes llevaron o están llevando a cabo la negociación de los seguros?
 - 10.2 ¿En este proceso intervienen expertos en evaluación de riesgos (administrador, responsables de seguridad, auditores en informática, especialistas o expertos financieros)?
 - 10.3 ¿Qué plazos de cobertura marcan estos seguros?
 - 10.4 ¿Se tienen previstas acciones legales para prevenir posibles incumplimientos por parte de las compañías aseguradoras?
 11. ¿Existe una clasificación de los elementos prioritarios para que la operación de los sistemas básicos no se interrumpa por un desastre o contingencia?
 - 11.1 Indique si la clasificación contempla los siguientes elementos: equipo de cómputo, archivos, programas fuentes, lenguajes de desarrollo, sistemas operativos, documentación, personal, entre otros

Nota: Hay que comprobar si existe un programa de capacitación formal para que el personal usuario y de informática tome conciencia de la importancia que tiene

el concepto de seguridad y la oportuna y correcta aplicación de los controles y procedimientos relativos a dicho concepto.

Planeación de informática

Metodología
Técnicas
Herramientas
Capacitación y actualización

Objetivos de la revisión

- Detectar la existencia, formalización y conocimiento de la planeación de informática en las áreas clave del negocio
- Verificar que la planeación de informática haya sido evaluada y aprobada por la alta dirección
- Comprobar que la planeación de informática se enfoque en el soporte de los objetivos, planes, políticas y estrategias de la empresa
- Evaluar el grado de compromiso por parte de la alta dirección con informática para determinar si el apoyo que brinda a la planeación de informática es el adecuado
- Confirmar la existencia de una metodología en informática
- Investigar si existen técnicas y herramientas de productividad para el desarrollo del plan
- Comprobar que exista un proceso formal de capacitación para el entendimiento y manejo satisfactorio de la metodología de planeación en informática
- Evaluar el grado de cumplimiento de la metodología, técnicas y herramientas en el proceso de planeación de informática
- Comprobar si la alta dirección, los responsables de las áreas usuarias y los responsables de informática se han involucrado en el proceso de planeación de informática
- Verificar si se da cumplimiento a los proyectos surgidos del plan de informática
- Evaluar el grado de dominio que tiene el personal de informática sobre la metodología, técnicas y herramientas de productividad que utilizan para el desarrollo del plan de informática
- Valorar el nivel de estandarización que tiene la metodología de planeación de informática con respecto a las aceptadas comúnmente en el mercado (fases, tareas, actividades, productos terminados, funciones y responsabilidades, revisiones, aseguramiento de calidad, entre otros puntos)

Nota: En caso de que personal externo realice la planeación de informática, asegurar que se cumplan al menos las consideraciones mencionadas; además, obtener eviden-

cia de la seriedad y confiabilidad de dichos asesores, por el tipo de información que se maneja en este proceso.

Principales actividades para auditar esta área

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla H.1)

Metodología

Aspectos clave por evaluar:

1. ¿Existe en su área una metodología para la planeación de informática?



Tabla H-1

Métodos, técnicas y herramientas requeridas	Planeación de informática	Otros de interés para el auditor en informática
Metodología de desarrollo e implantación de sistemas	Sí	
Metodología de planeación	Sí	
Cuestionarios	Sí	
Entrevistas	Sí	
Observación / monitoreo	Sí	
Análisis / diseño	Sí	
Trabajo en equipo	Sí	
Análisis costo / beneficio	Sí	
Documentación	Sí	
Pruebas de auditoría	Sí	
Control de proyectos	Sí	
Índices de producción (benchmarking)	Sí	

- 1.1 ¿Esta metodología contempla qué hacer, quién debe hacerlo y cuándo debe hacerse durante los proyectos de planeación de informática?
- 1.2 Si es así, indique si también abarca los pasos y lineamientos requeridos para la siguiente clasificación de proyectos:
 - Planeación de sistemas de información por desarrollar e implantar (corto, mediano y largo plazos)
 - Desarrollo e implantación de sistemas de las diferentes áreas del negocio
 - Compra e implantación de aplicaciones de mercado
 - Adaptación de aplicaciones adquiridas a externos (aplicaciones de mercado)
 - Proyectos de telecomunicaciones
 - Proyectos de investigación tecnológica (hardware, software, telecomunicaciones, entre otros)
 - Proyectos de evaluación y selección de proveedores de productos y servicios
 - Proyectos de desarrollo e implantación de sistemas estratégicos de información para toma de decisiones
 - Proyectos de auditoría y evaluación de informática
 - Proyectos de desarrollo e implantación de planes de contingencia y recuperación
 - Proyectos de capacitación o actualización ejecutiva, técnica y de usuarios
 - Rediseño de sistemas existentes
 - Desarrollo e implantación de sistemas integrales en el negocio
 - Aseguramiento de calidad
 - Otros relacionados con la función de informática
- 1.3 ¿Esta documentada formalmente dicha metodología?
- 1.4 Si es así, indique si cubre cada uno de los siguientes puntos: *
 - Un panorama general de la metodología
 - Equipos de trabajo sugeridos según el tipo de proyecto
 - Etapas de la metodología
 - Tareas de cada etapa
 - Secuencia de las etapas y tareas
 - Responsables e involucrados en cada etapa y tarea
 - Productos terminados por cada etapa o tarea
 - Requerimientos técnicos y administrativos para el cumplimiento de cada tarea
 - Revisiones formales e informales sugeridas para cada etapa
 - Duraciones estimadas de cada etapa del proyecto
 - Consideraciones para proyectos especiales

* El auditor en informática debe verificar que la documentación de la metodología contemple los diferentes proyectos mencionados en la pregunta 1.3.

2. ¿Cómo se aseguran un compromiso formal, un desarrollo y seguimiento eficientes, así como la aprobación final de los proyectos si no se cuenta con una metodología que contenga lo mencionado en las preguntas 1.3, 1.4 y 1.5?
3. En caso de contar con una metodología de planeación de informática, ¿ésta fue desarrollada por personal de informática de la empresa, se compró o se renta cuando se requiere?
 - 3.1 ¿Se capacitó al personal de desarrollo en el entendimiento y uso práctico de la misma?
 - 3.2 Indique si la capacitación fue impartida de manera formal por grupos de trabajo o individualmente y con casos prácticos o proyectos piloto.
 - 3.3 ¿Se evaluó el grado de asimilación de la metodología? ¿Cómo?
 - 3.4 Si no se capacitó al personal en el uso de la metodología, ¿cómo se asegura su entendimiento y uso eficiente durante los proyectos?
 - 3.5 ¿Desde cuándo están usando dicha metodología?
 - 3.6 ¿Se capacita al personal de desarrollo de reciente ingreso a la empresa en el entendimiento y uso de la metodología? ¿Se contemplan los puntos mencionados en la pregunta 3.2?
 - 3.7 ¿Se actualiza la metodología cuando es necesario?
 - 3.8 ¿Qué actividades de investigación o consulta se realizan para formular cambios o adaptaciones en la metodología?
 - 3.9 ¿Se documentan formalmente estos cambios?
 - 3.10 ¿Quién aprueba los cambios a la metodología?
 - 3.11 ¿Capacitan formalmente al personal en lo referente a la actualización de la metodología?
4. ¿Existe una congruencia de la metodología de planeación de informática con las metodologías recomendadas como estándares en el mercado?
5. ¿Cómo se aseguran de que las metodologías de planeación de informática compradas o rentadas a externos satisfagan los requerimientos del negocio?
6. Mencione cuáles son las etapas, tareas, productos y los responsables del proceso de planeación de informática que se lleva en la empresa (verificar la congruencia con los estándares metodológicos más aceptados).

Etapas	Tareas	Productos	Responsable

6.1 Las etapas mencionadas deben cubrir al menos los siguientes aspectos:

- Estudio de la situación actual y tendencias de los aspectos culturales, tecnológicos y económicos, entre otros
- Análisis de la competencia: fortalezas, debilidades, imagen, aspectos financieros, etc.
- Expectativas y grado de satisfacción de los clientes: productos, servicios, expectativas, oportunidades
- Evaluación de la situación actual del negocio: aspectos culturales, tecnológicos y económicos, sistemas de información, fortalezas y debilidades
- Análisis de los planes del negocio: metas, objetivos, planes tácticos y estratégicos, etc.
- Evaluación de cada una de las áreas del negocio en aspectos relativos a sistemas de información, tecnología, proyectos estratégicos, entre otros
- Análisis y formulación de las áreas de oportunidad para apoyo a la alta dirección: factores básicos de éxito, proyectos estratégicos, inversiones, expectativas, apoyo requerido de informática, etc.
- Elaboración y formulación del plan de informática
- Proyectos tácticos y estratégicos que cubran los siguientes puntos:
 - Sistemas de información, administración de la función, equipos de cómputo, telecomunicaciones, auditoría en informática, investigación de la tecnología de informática, evaluación y adquisición de productos y servicios, proyectos conjuntos alta dirección —informática, proyectos conjuntos entre usuarios e informática, etc.

Técnicas

Aspectos clave por evaluar:

1. ¿El personal de informática sabe cuáles son las técnicas requeridas para el desarrollo, seguimiento y documentación de las etapas de planeación de informática?
 - 1.2 ¿Existen dichas técnicas para la planeación de informática en la empresa?
 - 1.3 ¿Se capacita formalmente al personal de desarrollo de sistemas en el uso y aplicación de estas técnicas?
 - 1.4 ¿Se capacita al personal recién contratado en el manejo de las mismas?
 - 1.5 ¿Qué procedimiento se utiliza para la capacitación del personal de desarrollo en el uso de metodologías y técnicas?
2. Explique cuáles de las técnicas siguientes son usadas en el desarrollo de sistemas por su empresa:

Técnica	Sí	No	Etapas donde se aplica
Listas de verificación			
Entrevistas			
Listas de verificación de aseguramiento de calidad			
Control de proyectos			
Análisis organizacional (sistemas de negocio)			
Análisis costo/beneficio			
Documentación			
Diagramación			
Modelación de datos y procesos			
Investigación			
Manejo de equipos de trabajo			
Otros (especifique)			

3. ¿Quiénes y cómo determinaron cuáles eran las técnicas requeridas para el desarrollo e implantación de sistemas de información del negocio?

3.1 ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique?

Herramientas

Aspectos clave por evaluar:

1. ¿Existe una clasificación de las herramientas de productividad utilizadas por su empresa en la planeación de informática? (Entiéndase por herramientas de productividad los medios computarizados —hardware o software— y manuales —instrumentos de medición, diagramación, etc.— que utiliza el personal de informática en la planeación.)

1.2 Si es así, ¿podría indicar cuáles de los siguientes utilizan en su empresa?

Concepto	Hardware	Software	Herramientas manuales
Procesadores de palabras			
Hojas electrónicas			
Graficadores			
Diagramadores			
Presentadores			
Generadores de aplicaciones			
Generadores de bases de datos			
Ingeniería de software			
Índices de productividad (benchmarks)			
Otros (especifique)			

- 1.3 ¿Su uso está generalizado en la empresa? ¿Cómo se aseguran de que se aplique?

Capacitación/actualización

Aspectos clave por evaluar:

1. Mencione si existen procedimientos formales para capacitar al personal de planeación de informática (o puestos equivalentes) en:

- Entendimiento y aplicación de
- metodología de planeación de informática
- Técnicas para efectuar las etapas de la planeación de informática
- Herramientas de productividad requeridas en la planeación de informática

- 1.2 ¿Se documentan dichos procedimientos?

- 1.3 ¿Hay un responsable directo de elaborar, actualizar, documentar y definir estos procedimientos de capacitación?

- 1.4 ¿Cómo se asegura el cumplimiento oportuno de tales procedimientos?

- 1.5 Si existen, ¿al menos contemplan lo siguiente?

- Calendarios de los cursos
- Responsables de impartir los cursos (personal externo o interno)
- Puestos o funciones que requieren dichos cursos
- Costos estimados de los cursos
- Beneficios esperados de cada curso
- Parámetros de medición para asistentes y expositores
- Material requerido para cada curso
- Responsables de la organización de los cursos

2. Si no se tiene un proceso formal de capacitación, ¿cómo se da seguimiento al entendimiento, uso y actualización oportuna de la metodología, técnicas y herramientas de productividad requeridas por parte del personal durante la planeación de informática?
3. ¿El responsable de informática está consciente de la importancia que tiene la actualización y mejoramiento continuos del personal de desarrollo de sistemas de información para la implantación de soluciones del negocio?
4. Cuando intervienen terceros (personal externo) en proyectos de planeación de información, ¿cómo se aseguran de que la metodología, técnicas y herramientas de productividad que usan cubran por lo menos los estándares (o normas) mínimos de la empresa? ¿Qué se hace si la organización no tiene dichos estándares definidos?

Aspectos complementarios

El auditor en informática ha de recomendar al menos los siguientes puntos:

a) Documentar formalmente los siguientes aspectos relevantes del negocio:

- Misión
- Objetivos
- Estrategias
- Oportunidades
- Fortalezas
- Debilidades
- Amenazas
- Planes a corto, mediano y largo plazos
- Políticas
- Funciones primordiales
- Información básica para dichas funciones
- Requerimientos
- Otros

b) Dirigir el plan de informática a las estrategias y objetivos del negocio orientados a planes de corto, mediano y largo plazos.

c) Que sea aprobada formalmente por la alta dirección.

d) Participación de los usuarios en la definición, formalización y aprobación del plan.

e) Darle seguimiento formal a dicha planeación elaborando y revisando reportes específicos.

f) Utilizar siempre una metodología formal de planeación de informática.

g) La metodología debe cubrir los aspectos más relevantes de las metodologías habituales.

h) La función de informática ha de desarrollar los proyectos con base en el plan maestro de informática.

i) Debe existir una función de administración de los proyectos de informática para el seguimiento del plan de informática, actualización del plan, etc.

j) Todos los proyectos de informática tendrán un análisis costo/beneficio.

k) Realizar estudios de manera periodica para tener:

- Una evaluación de la eficiencia en el uso de la tecnología informática
- Una evaluación de la infraestructura tecnológica actual
- Una evaluación de los sistemas de información
- Una evaluación de los datos de los sistemas
- Una evaluación de la función de informática (aspectos administrativos)

Con base en los puntos mencionados, resolver el siguiente cuestionario:

1. ¿Se tienen estrategias claras y documentadas para la implantación de los proyectos de la planeación?
2. ¿Están bien definidas las funciones y responsabilidades de los recursos involucrados en cada proyecto?
3. ¿Están conscientes la alta dirección e informática del compromiso que se deriva de la planeación?
4. ¿Está consciente la alta dirección del apoyo que requiere la función de informática para el logro satisfactorio de cada proyecto de la planeación?
5. ¿Se tiene contemplada la participación de asesores externos en el desarrollo de ciertos proyectos?
6. ¿Se utilizó algún procedimiento formal para la selección del mejor asesor?
7. Indique si se cuenta con políticas y procedimientos formales para proyectos de:
 - Evaluación y adquisición del hardware y software
 - Desarrollo de sistemas de información
 - Telecomunicaciones
 - Intercambio electrónico de datos
 - Automatización de oficinas
 - Automatización de procesos de producción
 - Otros



INVESTIGACIÓN TECNOLÓGICA

Objetivos de esta revisión

- Verificar si existe una función formal de investigación tecnológica (o puestos similares) dentro del área de informática
- Detectar el grado de confianza, satisfacción y respaldo que brinda al negocio la función de investigación tecnológica
- Verificar que exista una clasificación y entendimiento de los servicios y productos que proporciona al negocio la función de investigación tecnológica
- Determinar las acciones emprendidas por la función de investigación tecnológica para que la tecnología de informática (hardware, software, comunicaciones, etc.) se encuentre al alcance de las diferentes áreas de la empresa que así lo requieran
- Comprobar que exista un análisis costo/beneficio de los proyectos propuestos por la función de investigación tecnológica que justifiquen su aprobación antes de ser implantados
- Constatar que los proyectos de investigación tecnológica sean resultado del plan de informática (véanse los cuestionarios de Planeación de informática para mayor detalle)
- Evaluar el grado de compromiso de la alta dirección con los proyectos de investigación que informática considera estratégicos para el negocio

Nota: Esta evaluación se efectúa con los responsables directos de la investigación tecnológica, el responsable de la función de informática y, de ser necesario, con algunos usuarios y la alta dirección. Por otro lado, el auditor en informática podrá evaluar o hacer todas las consideraciones necesarias para asegurar el enfoque productivo, objetivo y práctico de los productos y servicios de investigación con el fin de orientar los esfuerzos de esta área hacia beneficios tangibles para el negocio.

Métodos, técnicas y herramientas requeridas por área de revisión

El auditor en informática es visto en las organizaciones como una persona profesional, experimentada en su trabajo y con un grado de especialización aceptable, ya que él desarrolla actividades como la evaluación y el control de las áreas relacionadas con informática.

La importancia de que conozca las funciones, actividades, estándares, políticas y procedimientos de las áreas específicas que auditará radica en que podrá ejercer la auditoría con conocimiento de causa; así, la implantación de las soluciones tendrá una certeza profesional y ética. Esto —evidentemente— brinda confianza y beneficios tangibles al negocio.

Otro aspecto importante que debe abarcar un proyecto de auditoría en informática es el conocimiento y aplicación formal de los métodos, técnicas y herramientas requeridos en cada área o función de informática para el desempeño ordenado y eficiente de su trabajo.

Si el auditor en informática busca evaluar el grado de uso que se da a las metodologías, técnicas y herramientas de trabajo, es recomendable que las haya utilizado formalmente en algún momento de su vida profesional (experiencia) o al menos las conozca a nivel teórico (conceptualización).

Tanto el personal de informática y usuarios, como los mismos auditores en informática deben estar conscientes de que no sólo las habilidades personales y la experiencia aseguran el éxito de los negocios; es necesario el apoyo metodológico complementado con técnicas y herramientas de productividad de uso generalizado (estándares o normas) y no personalizado (exclusividad) que permitan a todos trabajar con esquemas similares y que, aunados a la creatividad y responsabilidad profesional de cada individuo, brinden frutos a la empresa y no soluciones excelentes, pero aisladas.

Las actividades y funciones de las áreas recomendadas en la matriz de riesgos se pueden apoyar en la práctica con metodologías, técnicas y herramientas, que el auditor en informática está en condiciones de evaluar. En las tablas 13.1 y 13.2 se recomiendan algunas de las más importantes. (Sin embargo, el auditor en informática puede agregar o eliminar las que considere conveniente en función del proyecto, sin perder de vista el aseguramiento de los objetivos buscados al inicio del mismo.)

Principales actividades para auditar esta área

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

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

Requerimientos para el éxito de la revisión

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

Técnicas para obtener y evaluar la información (véase tabla H.1)

1. Consideraciones generales

Aspectos clave por evaluar:

1. ¿Existe una clasificación de los principales productos y servicios proporcionados por el área de investigación tecnológica?
 - 1.1 Si es así, ¿cuáles son?

Productos	Servicios	Orientados a

- 1.2 Si no tienen esta clasificación, ¿cómo justifican su función ante el responsable de informática y la alta dirección?
- 1.3 ¿Cómo estiman los proyectos futuros en:
 - Tipo de proyectos, tareas, tiempos
 - Recursos
 - Responsables

2. ¿Existe una descripción formal de la función de investigación tecnológica?
 - 2.1 Si es así, ¿dicha descripción contempla tareas, actividades, responsabilidades, entre otros?
 - 2.2 Si no se tiene esta descripción, ¿cómo se administra la función? ¿Cómo le dan seguimiento los encargados de esta área?
3. ¿Existe un proceso metodológico para desempeñar la función de investigación? ¿Cuál es?
 - 3.1 ¿Está dicho método de trabajo documentado formalmente? ¿Todos los involucrados lo conocen? ¿El personal de nuevo ingreso es capacitado para usarlo formalmente?
 - 3.2 Si no existe un método específico de trabajo, ¿cómo se desarrolla esta función? ¿Cómo se aseguran de alcanzar el nivel de productividad y calidad deseados por la empresa y el responsable de informática?
4. ¿Existen políticas y procedimientos específicos para las tareas y actividades de investigación? ¿Se cuenta con técnicas y herramientas para el desarrollo de las mismas? ¿Cuáles son? ¿Cómo preveen que se entiendan y usen en forma adecuada?
5. Indique si los proyectos de investigación están contemplados en el plan de informática. Si no es así, ¿cómo los justifican?

INFORME DE AUDITORÍA EN INFORMÁTICA

Informe final: un producto terminado de la función de auditoría en informática

Una vez que el proyecto de auditoría en informática ha terminado se procede a la elaboración de un documento final que refleje todas las observaciones, debilidades, áreas de oportunidad, acciones de mejoramiento, plazos sugeridos para su realización, responsables y personas involucradas.

Es importante aclarar que el orden y forma de este informe puede variar de acuerdo con la creatividad y estilo de los auditores en informática o de los estándares establecidos por el responsable de la función; sin embargo, hay que tomar en cuenta la información propuesta en el párrafo anterior y las consideraciones mencionadas a continuación.

El auditor en informática elabora formalmente este documento con el apoyo y asesoramiento del gerente o director de la función.

El informe se define como “el documento” que refleja los objetivos, alcances, observaciones, recomendaciones y conclusiones del proceso de evaluación relacionados con las áreas de informática.

1. ¿A quiénes va dirigido?

Se entrega a las siguientes funciones:

- Director del negocio o gerente general
- Director o gerente de las áreas usuarias auditadas
- Director o gerente de informática
- Director o gerente de auditoría en informática
- Director o gerente de auditoría (si así lo establecen las políticas de la empresa)

2. ¿Quiénes revisan y aprueban el documento final?

- Director o gerente de las áreas usuarias auditadas
- Director o gerente de informática
- Director o gerente de auditoría (en caso que así lo señalen las políticas de la empresa)

3. Requisitos del informe de auditoría en informática:

- a) Ser veraz: toda la información reflejada en el informe de auditoría en informática, sea ésta una observación (debilidad), recomendación, gráficas, etc., debe ser verídica, de manera que se tomen consideraciones y conclusiones con la certeza de que los datos son reales y de buena fuente.
- b) Estar documentado formalmente: todo el proceso de auditoría, incluso desde su planeación y justificación. El informe final es el resultado de los datos registrados desde el inicio hasta el final del proyecto:
 - Planes
 - Matriz de riesgos
 - Entrevistas aplicadas
 - Visitas y comentarios
 - Cuestionarios aplicados
 - Observaciones (debilidades)
 - Áreas de oportunidad
 - Recomendaciones
 - Revisiones formales e informales
 - Sugerencias y comentarios relevantes de los involucrados en el proyecto
 - Informe preliminar
 - Otros
- c) Mostrar las observaciones (debilidades) encontradas: cada una de las debilidades detectadas a lo largo del proceso de auditoría en informática deben ser documentadas en este informe; asimismo, se clasificarán por orden de importancia o impacto negativo que pueden tener en el negocio si no se atienden oportunamente. Además, han de tener un significado relevante en los aspectos financieros, materiales, políticos, de control, procedimientos, seguridad, etc.

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

Aquí es muy importante señalar que todas esas observaciones o debilidades se identificaron a lo largo del proyecto y que, de alguna manera, se comentaron con los responsables de las áreas o funciones que las originaron, excepto situaciones muy delicadas como fraudes o delitos graves contra la empresa.
- d) Tener recomendaciones y soluciones para cada observación: todas las debilidades mencionadas en el informe han de tener una solución clara y contundente que comprenda la siguiente información:
 - Observaciones (debilidades)
 - Áreas de oportunidad

- Acciones de mejoramiento
- Productos terminados (resultados)
- Plazos de implantación:
 - Inmediatos
 - A corto plazo
 - A mediano plazo
 - A largo plazo
- Responsables de cada acción
 - Involucrados:
 - Usuarios
 - Alta dirección
 - Informática (desarrollo, investigación, comunicaciones, planeación, etc.)
 - Auditoría
 - Auditoría en informática
 - Asesores externos
 - Otros

Nota: Tanto las debilidades como las recomendaciones descritas en el informe pueden apoyarse en tablas estadísticas, gráficas, diagramas, etc., con el fin de hacer más específica y entendible la información.

- e) Reflejar las áreas de oportunidad y cursos de acción: es muy factible que en el transcurso del proyecto el auditor en informática detecte áreas de oportunidad que no se relacionan con las debilidades encontradas en el proceso de evaluación y revisión; por ello, esas áreas de oportunidad deben orientarse a mejorar la productividad y calidad de las funciones o departamentos auditados, con lo cual se proporciona un valor agregado a las expectativas generadas por el proyecto. Algunos ejemplos pueden ser:

- Capacitación y actualización
- Formalización del proceso de planeación en informática
- Automatización de oficinas (integrar herramientas de productividad)
- Multimedia
- Desarrollo de sistemas estratégicos
- Otros aspectos

Seguimiento del informe

1. La empresa debe decidir con cuál de las siguientes alternativas se asegurará, que se dé cumplimiento oportuno a los compromisos y tareas que resulten del informe de auditoría en informática:

- a) Auditores internos

- b) Auditores externos
 - c) Ambas alternativas
2. La importancia de que se dé seguimiento formal estriba en que los gastos y tiempos incurridos en el proyecto de auditoría sólo serán reflejados en beneficios tangibles una vez ejecutadas al pie de la letra, las medidas seguidas por el auditor de informática a través de políticas y procedimientos acordes a las necesidades del negocio.
 3. Es recomendable realizar un informe posterior a la implantación que brinde la garantía de que todo fue satisfactorio, en caso contrario indique las medidas correctivas pertinentes.

BIBLIOGRAFÍA SUGERIDA

Bibliografía Libro/Fuente	Autor	Editorial
Análisis y diseño de sistemas de información	James A. Senn	McGraw-Hill
Auditoría I	Expositores de la Asociación Mexicana de Auditores de Informática	Asociación Mexicana de Informática
Auditoría II	Expositores de la Asociación Mexicana de Auditores de Informática	Asociación Mexicana de Informática
Auditoría en Informática	José Antonio Echenique	McGraw-Hill
Control Objectives	The EDP Auditors Foundation, Inc.	The EDP Auditors Foundation Inc.
EDP Auditing and Controls	MIS Training Institute	MIS Training Institute
INTEREX HP Computer Users Conference	INTEREX The International Association of Hewlett Packard Computers Users	INTEREX
Normas y procedimientos de Auditoría	IMCP	IMCP
Sistemas de Información	Burch John G.	LIMUSA
Systems Auditability and Control	The Institute of Internal Auditors Research Foundation	The Institute of Internal Auditors Research Foundation
EDP Audit	Weber, Ron	McGraw-Hill
Más allá de la reingeniería	Jablonsky	CECSA
Ventaja Competitiva	Porter, Michael	CECSA

Esta obra se terminó de imprimir en octubre de 1996
en los talleres de Impresos Naucalpan S.A. de C.V.
Calle San Andrés Atoto No. 12, C.P. 53550
Naucalpan, Edo. de México

La edición consta de 2,000 ejemplares más
sobrantes para reposición.

