

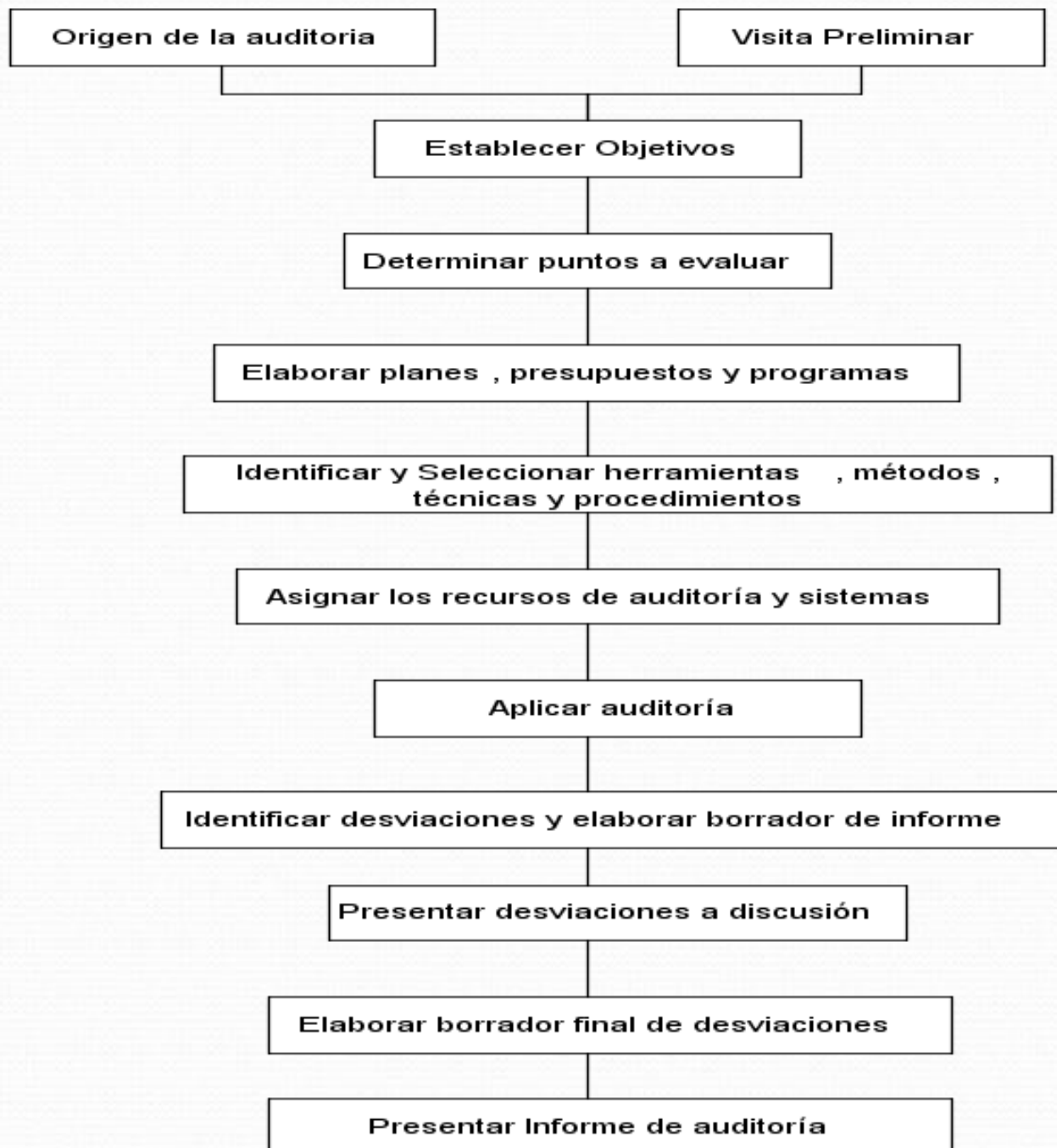
# **METODOLOGIA PARA REALIZAR AUDITORIA DE SISTEMAS COMPUTACIONALES**

# Introducción

Para llevar a cabo una auditoria de sistemas computacionales se requiere una serie ordenada de acciones y procedimientos específicos los cuales deberán ser diseñados previamente de manera secuencial, cronológica y ordenada de acuerdo a las etapas, eventos y actividades que requieran para su ejecución.

# Introducción

Con base a lo anterior podemos entender la necesidad de establecer una metodología específica de revisión, la cual nos servirá para diseñar correctamente los pasos a seguir en la evaluación de áreas de sistemas y actividades elegidas, a fin de que el seguimiento, desarrollo y aplicación de las etapas y eventos propuestos sean más sencillos.





# Etapas fundamentales en la Metodología.

- Planeación de la auditoria de sistemas computacionales
- Ejecución de la auditoria de sistemas computacionales
- Dictamen de la auditoria de sistemas computacionales

# Fases y Pasos para realizar auditorías de sistemas computacionales

- **Planeación de la auditoria de sistemas computacionales**
  - Identificar origen de la auditoria.
  - Realizar visita preliminar al área que será evaluada.
  - Establecer objetivos de auditoría.
  - Determinar puntos que serán evaluados.
  - Elaborar planes, programas y presupuestos para realizar auditoría.
  - Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos para la auditoría.
  - Asignar recursos y sistemas computacionales

# Fases y Pasos para realizar auditorías de sistemas computacionales

- **Ejecución de la auditoria de sistemas computacionales**
  - Realizar acciones programadas para auditoria.
  - Aplicar los instrumentos y herramientas para la auditoria.
  - Identificar y elaborar los documentos de desviaciones encontradas.
  - Elaborar el dictamen preliminar y presentarlo a discusión.
  - Integrar la documentación de trabajo de la auditoria.

# Fases y Pasos para realizar auditorías de sistemas computacionales

- **Dictamen de la auditoria de sistemas computacionales**
  - Analizar la información y elaborar un informe de situaciones detectadas.
  - Elaborar el dictamen final.
  - Presentar el informe de auditoría.



# PLANEACIÓN DE LA AUDITORIA DE SISTEMAS COMPUTACIONALES

- Para realizar una auditoría de sistemas computacionales se requiere la definición de las actividades necesarias para su ejecución y esto se logra con una adecuada planeación.
- Se deben identificar claramente las razones por las cuales se va realizar la auditoria y determinar los objetivos de la misma así como el diseño, métodos, técnicas y procedimientos para llevarla a cabo.

# PLANEACIÓN DE LA AUDITORIA DE SISTEMAS COMPUTACIONALES

- El responsable de la planeación de esta primera etapa de la metodología debe iniciar con el planteamiento de los siguientes interrogantes.
- *¿Por qué se realizara la auditoría?*
- *¿Se debe hacer una visita preliminar al área de sistemas?*
- *¿Cuál es el objetivo que se pretende alcanzar con esta auditoría?*

# Identificar el origen de la auditoria.

- El primer paso formal en la planeación de auditoría en el área de sistema es identificar el origen de la auditoria, lo primero es saber por qué surge la necesidad o inquietud de realizar una auditoría. Para esto se debe preguntar *¿de dónde?, ¿Por qué?, ¿quién?, o para qué* se requiere hacer la evaluación de algún aspecto.
- Para el responsable de realizar la auditoria es de suma importancia identificar el origen debido a que además de proporcionarle elementos necesarios para realizar una buena auditoria, también le ayuda definir los elementos de juicio que contribuirán a formar un criterio.

# Identificar el origen de la auditoria.

- También puede saber de antemano cuales serán los aspectos primordiales en la evaluación, es decir, cuales serán los asuntos más relevantes sobre los cuales deberá trabajar.



# Causas para realización de una auditoria

- Solicitud expresa de procedencia interna: se define como origen oficial sobre la necesidad de realizar una auditoría al área de sistemas de la empresa, debido a petición formal de algún funcionario de la misma.
- A petición de accionistas, socios y dueños: este es uno de los más comunes orígenes ya que esta solicitud es ordenada por los dueños de la empresa con el propósito de saber cómo se administra su patrimonio, como se utilizan los recursos y como es el rendimiento de su patrimonio.

# Causas para realización de una auditoria

- Por orden de dirección general: esta revisión se realiza por orden directa por quien ejerce la autoridad máxima e la empresa, la cual puede abarcar varios motivos, como evaluación periódica, por desconfianza de dirigentes, para verificar el cumplimiento de actividades, para verificar el aprovechamiento de los sistemas computacionales.
- Por orden de gerencia o departamentos de nivel superior: esta petición se origina por mando superior de la empresa según su estructura organizacional y funciones.

# Causas para realización de una auditoria

- Solicitud externa: este es otro de los orígenes oficiales, debido a que surge de una petición formal de alguien ajeno a la empresa a quien por alguna causa le interesa que sean auditados los sistemas computacionales.
- Por mandato de autoridad judiciales: es uno de los más comunes por que deriva de autoridades judiciales las cuales por algún motivo imponen la realización de una auditoria la empresa por sospecha de piratería, carencia de licencia de software, presunción de mal uso de software, delitos informáticos.



# Causas para realización de una auditoria

- Por ordenamiento de autoridades fiscales: es uno de los orígenes más importantes de una auditoría externa y es cuando las autoridades fiscales imponen la realización de la misma con el propósito de verificar información sistematizada de la empresa, para verificar el funcionamiento del sistema en el ámbito contable, el correcto y oportuno calculo de impuestos o los resultados financieros y obligaciones, ocasionalmente para verificar licencias de usos de software y paquetería institucional con el fin de evitar piratería informática.



# Causas para realización de una auditoria

- Por solicitud de distribuidores y desarrolladores de software y hardware: es de origen especial donde la empresa puede dictaminar si accede o se niega a ello según sus intereses particulares, pero jamás este tipo de auditoría deberá ser de carácter impositivo.
- Como consecuencia de emergencias y condiciones especiales: este tipo de auditoría se realiza cuando se presenta situaciones de emergencia y condiciones extraordinarias en el área de sistemas las cuales están fuera de control, la auditoria se realiza casi de inmediato sin que medie la autorización de funcionarios.

# Causas para realización de una auditoria

- De incidencia interna: este tipo de auditoría se realiza cuando se presenta novedades en el área de sistemas la cual repercute en alguno de los recursos informáticos ya sea en el personal o usuarios, en el equipo de cómputo.
- De incidencia externa: este tipo de auditoría se presentan por contingencias, emergencia o incidencias de carácter externo que repercuten en el área de sistemas, tomo memos como ejemplo: ataques de virus, temblores, incendios lo cual lleva de inmediato a la evaluación de los daños sufridos en el área de sistemas.

# Causas para realización de una auditoria

- Por riesgos y contingencias informáticas: se presenta por solicitud de funcionarios, personal o usuarios del área de sistemas, cuando a ocurrido alguna contingencia que afecte el procesamiento de la información.
- Riesgos y contingencias del personal informático: esta solicitud se presenta por posibles riesgos derivados de la actuación del factor humano.



# Causas para realización de una auditoria

- Riesgos y contingencias físicas: esta solicitud se presenta por una contingencia o posible riesgo derivado de los bienes tangibles de la empresa en el área de sistemas.
- Riesgos y contingencias operativas: este tipo de solicitud se presenta por contingencias o riesgos que posiblemente afectaran el funcionamiento operativo(lógico) del sistema, cuando el comportamiento del software, así como niveles de seguridad, limitaciones de manejo de archivos , bases de datos influirán en el funcionamiento del sistema computacional.



# Causas para realización de una auditoria

- Riesgos y contingencias en las base de datos: esta solicitud se hace exclusivamente para evaluar el manejo de la información contemplada en la operación de bases de datos.
- Como resultados de planes de contingencia: esta solicitud se presenta por la implantación de planes de contingencia ya sea que carezca de estos o no el área de sistemas y se necesite evaluar su posible efecto o que ya estén establecidos y se quieran evaluar el grado de utilidad para dichos sistemas.

# Causas para realización de una auditoria

- Como parte de un programa integral de auditoría: también es frecuente que existan programas concretos de auditoría integral o global los cuales se aplica en la empresa para evaluar la correcta administración y comportamiento de todas sus áreas.

# Realizar visita preliminar al área que será evaluada

Es imprescindible que el auditor realice una visita preliminar después de conocer el origen de la petición de la auditoria y antes de iniciarla formalmente, con el propósito de tener un contacto inicial con el personal, para que verifique el área que será evaluada, observe a distribución de los sistemas y el número de equipos y en sí que conozca la problemática ala cual se enfrentara.



# Aspectos de la Visita preliminar

- Visita preliminar de arranque: esta visita la realiza el auditor con la finalidad de advertir de antemano las siguientes cuestiones:
  - *¿Cómo se encuentran distribuidos los sistemas del área?*
  - *¿Cuántos, cuales como y de qué tipo son los equipos ?*
  - *¿Cuáles son, a simple vista, las principales características físicas de los sistemas?*
  - *¿Cómo reacciona el personal ante la visita?*
  - *¿Cuáles son las medidas de seguridad visible?*
  - *¿Cómo actúan los usuarios?*
  - *¿Qué limitaciones se observan para realización de la auditoria?*



# Aspectos de la Visita preliminar

- Contacto inicial con funcionarios y empleados del área: en esta visita el auditor aprovecha para hacer contacto con los funcionarios, empleados y usuarios del área de sistemas, con el propósito de conocer cuáles son sus expectativas y ver cuáles son sus reacciones ante la realización de la auditoría, esto le permitirá conocer las limitaciones que tendrá en cuanto cooperación ya que la visita del auditor en la empresa casi siempre no es bien recibida lo que le generará problemas en el proceso de evaluación.

# Aspectos de la Visita preliminar

- Identificación preliminar de la problemática de sistemas: el auditor puede y debe aprovechar para saber cuál es la problemática a la que se enfrentará el área de sistemas su personal y usuarios, procesamiento y administración de bases de datos aunque sea de carácter obligatorio.
- Prever los objetivos iniciales de la auditoría: otro aspecto que se puede obtener de la visita al área que será auditada se puede anticipar cuáles objetivos se van a satisfacer y por lo menos tratar de entender cuáles son las metas que se quieren alcanzar.

# Aspectos de la Visita preliminar

- Calcular recursos y personas necesarias para la auditoria: otro beneficio de la visita es poder calcular el tipo, la cantidad de recursos que serán necesarios para llevar a cabo la evaluación, contemplando los recursos de carácter humano, informático, material técnico y económico.

# Establecer los objetivos de la auditoria

Después de haber realizado las dos fases anteriores lo que sigue es definir de forma clara los objetivos de la auditoria, ajustándolos a las necesidades de la evaluación, el propósito es establecer claramente lo que busca.



# Aspectos a analizar

- Objetivo general: es el fin global que se pretende alcanzar con el desarrollo de la auditoria de sistemas en el cual se plantean los aspectos que se pretenden evaluar.
- Objetivos particulares: son los fines individuales que se pretende alcanzar con el desarrollo de la auditoria ya sea de un área específica de un sistema en especial o de alguna función en particular.

# Aspectos a analizar

- Objetivos específicos de la auditoria de sistemas computacionales: es la determinación, en forma detallada, de los fines que se pretenden alcanzar con la auditoria de sistemas, señalando concretamente las áreas a evaluar y, específicamente, lo sistemas, componentes o elementos concretos que deben ser evaluados.

# Determinar los puntos que serán evaluados en la auditoria

- Después de haber realizado las tres faces anteriores lo que sigue es determinar los puntos concretos que serán evaluados.
- Es de suma importancia destacar la definición y establecimiento de los puntos que se debe evaluar es el elemento fundamental de apoyo del auditor, debido a que esto es producto de un análisis previo, tanto del origen de la auditoria y de la visita previa como de los objetivos que se pretenden satisfacer con esta auditoría.



# Determinar los puntos que serán evaluados en la auditoria

- La selección de tales puntos, los cuales, por su propia diversidad, pueden y deben ser establecidos de acuerdo a las necesidades de evaluación de la empresa, del equipo y del sistema operativo, así como la forma de procesamiento de información que se tiene establecida en la empresa.
- Cabe aclarar que este criterio de selección es de carácter general y solo se presenta al nivel de sugerencia y el responsable de la auditoria deberá determinar su aplicación real, de acuerdo con las necesidades de la evaluación. Los puntos a evaluar se pueden agrupar de la siguiente forma:



# Determinar los puntos que serán evaluados en la auditoría

*Evaluación de las funciones y actividades del personal del área de sistemas*

*Evaluación de las áreas y unidades administrativas del centro de cómputo*

*Evaluación de la seguridad de los sistemas de información*

*Evaluación de la información, documentación y registros de los sistemas*

*Evaluación de los sistemas, equipos, instalaciones y componentes*

*Evaluación de los recursos humanos del área de sistemas*

*Evaluación del hardware*

*Evaluación del software*

*Evaluación de la información y bases de datos*

*Evaluación de otros recursos informáticos*

*Evaluación de equipos, instalaciones y demás componentes*

*Elegir los tipos de auditoría que serán utilizados*

*Determinar los recursos que serán utilizados en la auditoría*

*Personal de auditoría de sistemas*

*Personal del área que será evaluada*

*Apoyo de los sistemas y equipos técnicos e informáticos*

*Apoyos materiales y administrativos*

*Otros apoyos*

*Recursos económicos*

# Personal de la auditoria

- Es el personal especializado que aplica sus conocimientos, habilidades y experiencias en las diferentes disciplinas de la auditoría, utilizando para ello técnicas, procedimientos , métodos de evaluación, herramientas e instrumentos de revisión especializados y tradicionales para la evaluación del sistema.

# Personal del área que será evaluado

- Este personal no estará a disposición del auditor y tampoco tiene ningún tipo de autoridad sobre el ni injerencia en su trabajo.



# Apoyo de los sistemas y equipos técnicos e informáticos.

- Estos recursos incluyen hardware, software (sistemas operativos, Aplicaciones especializadas, librerías, base de datos, entre otros), instalaciones, el personal especializado en las operaciones del sistema y la información al área a auditada.



# Apoyos materiales y administrativos

- Estos recursos son imprescindibles para el buen desempeño de los auditores, tales como:
  - Oficina principal privada.
  - Lugares de trabajo exclusivas.
  - Apoyo logístico y secretarial para realizar evaluaciones.
  - Apoyo logístico y administrativo del área de sistemas.

# Otros apoyos

- Dependiendo de las necesidades específicas de la evaluación del sistema, para la revisión de ciertos aspectos del área de sistemas que se tengan que auditar de manera particular.

# Recursos económicos

- El auditor debe comprobar los gastos efectuados durante la evaluación o pueden ser libres de comprobación. Estos gastos se representan en los siguientes rubros:
  - Viáticos.
  - Pasajes.
  - Otros gastos.

# Elaborar planes, programas y prepuestos

- Se deben elaborar los documentos que contemplen los planes formales para el desarrollo de la auditoria, los programas en donde se delimiten las etapas, eventos, actividades y los tiempos de ejecución para cumplir los objetivos.



# Elaboración del documento formal de los planes


- Es conocido como Plan de Auditoría de Sistemas, el cual contiene todos los aspectos relacionados con la realización de la auditoría. A continuación algunos aspectos :
  - Las actividades: Responsables, recursos y tiempo.
  - Los eventos: guías de acción.
  - Estimaciones: Recursos.
  - Los tiempos: duración de actividades y la auditoria.
  - Los auditores: responsabilidades.

# Plan de auditoría

- **La portada:** es la primera hoja del documento, en la cual se establece los siguientes puntos:
  - Nombre y logotipo de la empresa responsable de la auditoría.
  - Indicación del nombre del documento.
  - Nombre de la empresa (área) auditada.
  - Nombre del responsable de elaborar el plan de auditoría.
  - Fecha de vigencia del plan.

# Portada de identificación del Plan de auditoría

Nombre de la empresa (área) auditada

 AUDITORÍA EN SISTEMAS A.C.

EMPRESA: Instituto Nacional de Migración

AUDITOR: Ma. Araceli Arceo Gálvez

Nombre del responsable de elaborar el plan de auditoría

Fecha de vigencia del plan

FECHA			HOJA
DD	MM	AA	
26	3	96	26 de 29

PERÍODO: 01 al 16 de marzo de 1996

ÁREA AUDITADA: Dirección de Informática y Estadística

PLAN DE AUDITORÍA DE SISTEMA

Indicación del nombre del documento



# Plan de auditoría

- **Índice:** tiene como objetivo ayudar a una rápida consulta del documento.
- **Definición de objetivos:** son los objetivos que se pretenden alcanzar con la auditoria.
- **Delimitación de estrategias de el desarrollo:** es bueno contemplar las estrategias para diferentes partes de la auditoria.



# Plan de auditoría

- **Planes de auditoría:** aquí se detalla cada una de las acciones para la evaluación.
- **Definición de normas, políticas y lineamientos:** es importante que las actividades que van a realizar los auditores estén bien detalladas en el proyecto, para evitar traumas en el funcionamiento de la empresa auditada.

# Plan de auditoría

- **Contenido de los planes para realizar la auditoría:** es la elaboración de todos los planes formales de la auditoría, el cual debe contener de manera específica las fases, etapas, actividades recursos y tiempos de ejecución.

# Plan de auditoría

- Definir los objetivos finales: estos objetivos se deben redactar de manera sencilla , objetiva y concreta.
- Establecer las estrategias para la auditoria: se redactan de forma precisa con el fin de que loa auditores las entiendan rápida y perfectamente.



# Plan de auditoría

- **Calcular la duración de las tareas y eventos:** se debe planear la duración de acuerdo con la importancia, necesidad concreta y la forma de satisfacer el objetivo de una tarea o evento.
- **Distribuir los recursos que serán utilizados en las diferentes etapas y actividades:** en esta parte se establece la asignación de los recursos que serán utilizados, documentando detallada mente su utilizacio.

# Plan de auditoría

- Confeccionar los planes concretos: se establecen de manera escrita y grafica las etapas, eventos, tareas y actividades, incluyendo la duración de cada uno de estos aspectos.
- Elaborar el documento formal de auditoría: se cologa en forma grafica, los eventos, actividades

# Plan de auditoría

- Elaborar el documento formal de auditoría: se coloca en forma grafica, los eventos, actividades que se realizaran, con su duración de cada una de las partes en que se dividió el trabajo de valuación.
- Este documento debe ser unido al anterior, ya que es parte integral de él y solo se complementa con los siguientes:



# Plan de auditoría

- Elaborar el documento formal de auditoría
  - Grafica del programa de actividades.
  - Definición de las etapas y eventos que se llevaran acabo.
  - Definición de las actividades y tareas.

# Plan de auditoría

- Elaborar el documento formal de auditoría



**AUDITORÍA EN SISTEMAS  
COMPUTACIONALES**

**VIGENCIA**

DEL	DD	MM	AA
	28	3	98
AL	31	4	98

**EMPRESA:** Instituto Nacional de Computación

**PERÍODO:** 01 al 16 de marzo de 1996

**AUDITOR:** Ma. Araceli Arceo Gálvez

**ÁREA AUDITADA:** Dirección de Informática y Estadística

**PLAN DE AUDITORÍA DE SISTEMA**

ACTIVIDAD			SEMANAS							
No.	Nombre	responsable	1	2	3	4	5	6	7	8
1	Elaborar plan de auditoría	J. Dpto. asignado								
2	Aprobar plan de auditoría	Director								
3	Prepara instrumentos de remisión	Resp. Auditor								
4	Iniciar preparativos	Aud. Senior								
5	Cobrar viáticos y pasajes	Aud. Asignados								
6	Iniciar viaje	Aud. Asignados								
7	Iniciar auditoría	Aud. Asignados								
8	Auditar gestión informática	Aud. Sr. 1								
9	Auditar Bases de datos	Aud. Sr. 2								
10	Auditar Sistemas de cómputo	Aud. Sr. 3								
11	Auditar personal informático	Aud. Sr. 4								
12	Auditar la seguridad de los sistemas	Aud. Sr. 5								
13	Presentar borrador de informe	Resp. Auditor								

# Plan de auditoría

- **Elaborar los programas de actividades para realizar la auditoria:** se redacta en forma escrita y grafica, especificando los tiempos en que se lleva acabo cada una de loas etapas, eventos y actividades, para cada periodo de duración de cada una de las partes en que se dividió e trabajo de evaluación.



# Plan de auditoría

- **Definir de manera precisa las etapas:** se debe definir de manera precisa las posibles etapas en las que se dividirá la misma, buscando se congruente y coherente en la en la división de las actividades, en cuanto al volumen de trabajo, importancia del aspecto que será evaluado y el peso que tendría la etapa para toda la auditoria.



# Plan de auditoría

- **Identificación concretamente de los eventos que se deben llevar a cabo en cada etapa:** tomando el evento como un suceso esperado, al cual se debe llegar después de una serie de actividades.
- **Delimitar las actividades, tareas y acciones para cada evento:** el auditor será el responsable de establecer estas actividades, tareas y acciones, para que se cumplan las metas de la auditoría.

# Plan de auditoría

- **Distribuir los recursos que serán utilizados en las diferentes etapas, eventos, actividades y tareas:** se determina los recursos humanos como los recursos adicionales que serán utilizados en cada una de esas etapas.
- **Calcular la duración de las etapas ,actividades y tareas:** dicha estimación se debe hacer de acuerdo a la disponibilidad de los recursos, a la prioridad de cada etapa a la habilidad del responsable.

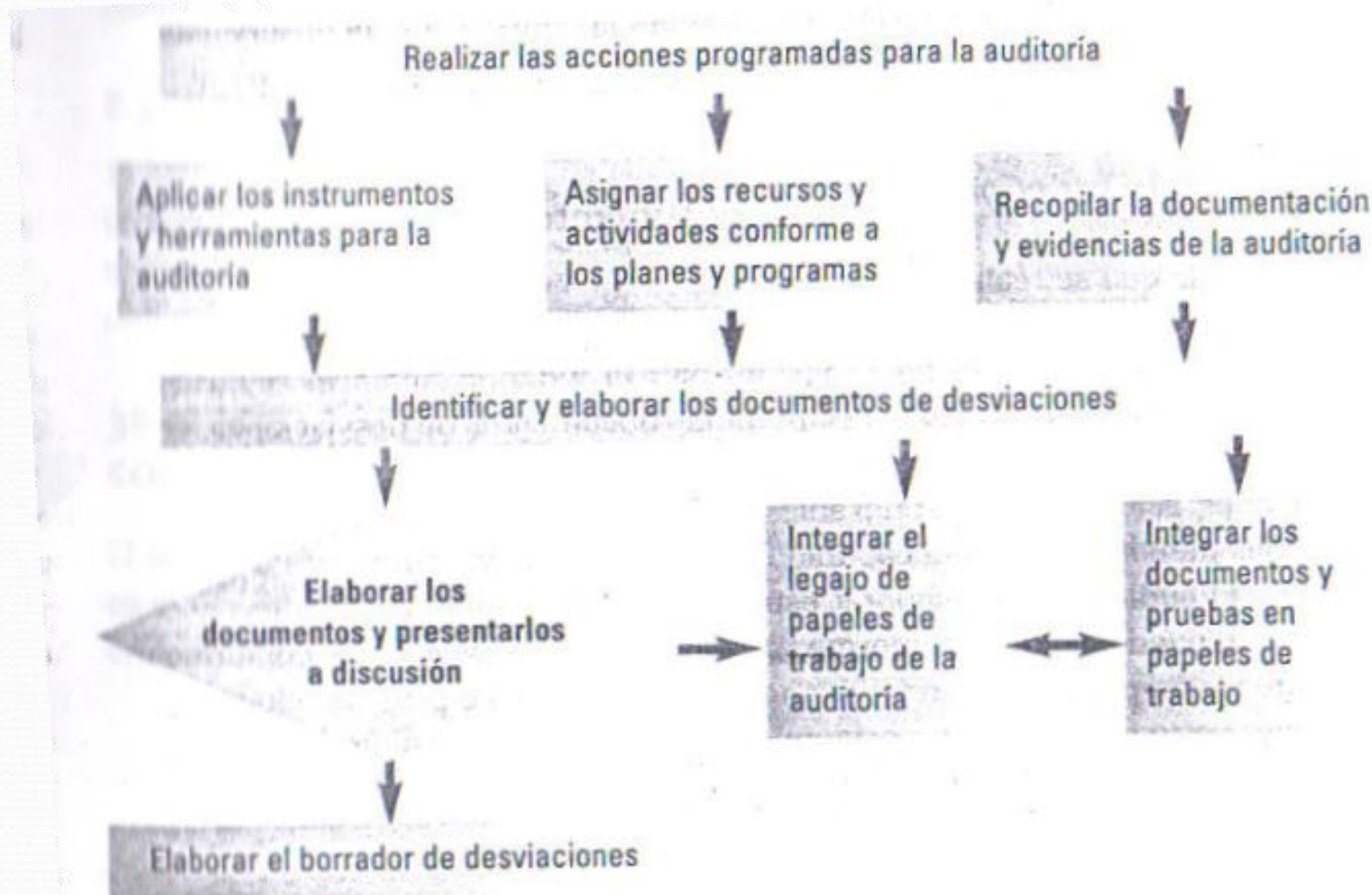
## 2 Etapa: Ejecución de la auditoria

- Después de planeación de la auditoria, se debe proceder a la ejecución, la cual estará determinada por las características concretas, los puntos y los requerimientos que se estimaron en la etapa de planeación.



## 2 Etapa: Ejecución de la auditoría

- Los principales puntos son los siguientes:





## 2 Etapa: Ejecución de la auditoria

- Concretamente, los siguientes aspectos:
  - Realizar las acciones Programadas para la auditoria.
  - Aplicar los instrumentos y herramientas para la auditoria.
  - Identificar y elaborar los documentos de la desviación.
  - Elaborar el dictamen preliminar y presentarlo a discusión.
  - Integrar los documentos de la auditoria.

# 3 Etapa: Dictamen de la auditoria

- El ultimo paso de la metodología que hemos estudiado en emitir el dictamen, el cual es el resultado final de la auditoria. Se debe tener en cuenta los siguientes puntos:
  - Analizar la información y elaborar un informe de situaciones detectadas.
  - Elaborar el dictamen final
  - Presentar el informe de la auditoria.

# 3 Etapa: Dictamen de la auditoria

- **Analizar la información y elaborar un informe de situaciones detectadas** : es el análisis de los papeles de trabajo y la elaboración de en borrador de las llamadas situaciones encontradas, el propósito es que el auditor elabore su borrador y comente las desviaciones con los auditados. En este punto se elaboran las siguientes actividades:
  - Analizar los papeles de trabajo.
  - Señalar las situaciones encontradas.
  - Comentar las situaciones encontradas con el personal auditado.
  - Realizar las modificaciones necesarias.
  - Elaborar el documento de las situaciones relevantes.

# 3 Etapa: Dictamen de la auditoria

- Elaborar el dictamen final: se debe terminar el informe de la auditoria y complementarlo con el dictamen final (opinión del auditor), para ello se elaboran las siguientes actividades:
  - Analizar la información y elaborar un documento de desviaciones detectadas.
  - Elaborar el informe y el dictamen formales.
  - Comentar el informe y el dictamen con los directivos del área.
  - Realizar las modificaciones necesarias.



# 3 Etapa: Dictamen de la auditoria

- **Presentar el informe de la auditoria:** esta presentación se debe hacer con toda la formalidad del caso, con la elaboración del dictamen de la auditoria, y en medio de una reunión directiva. El informe de auditoria debe llevar los siguientes puntos:
  - La carta de presentación.
  - El dictamen de la auditoria.
  - El informe de situaciones relevantes.
  - Anexos y cuadros adicionales.