

# Auditoría de sistemas



Informe de auditoría

# INFORME FINAL

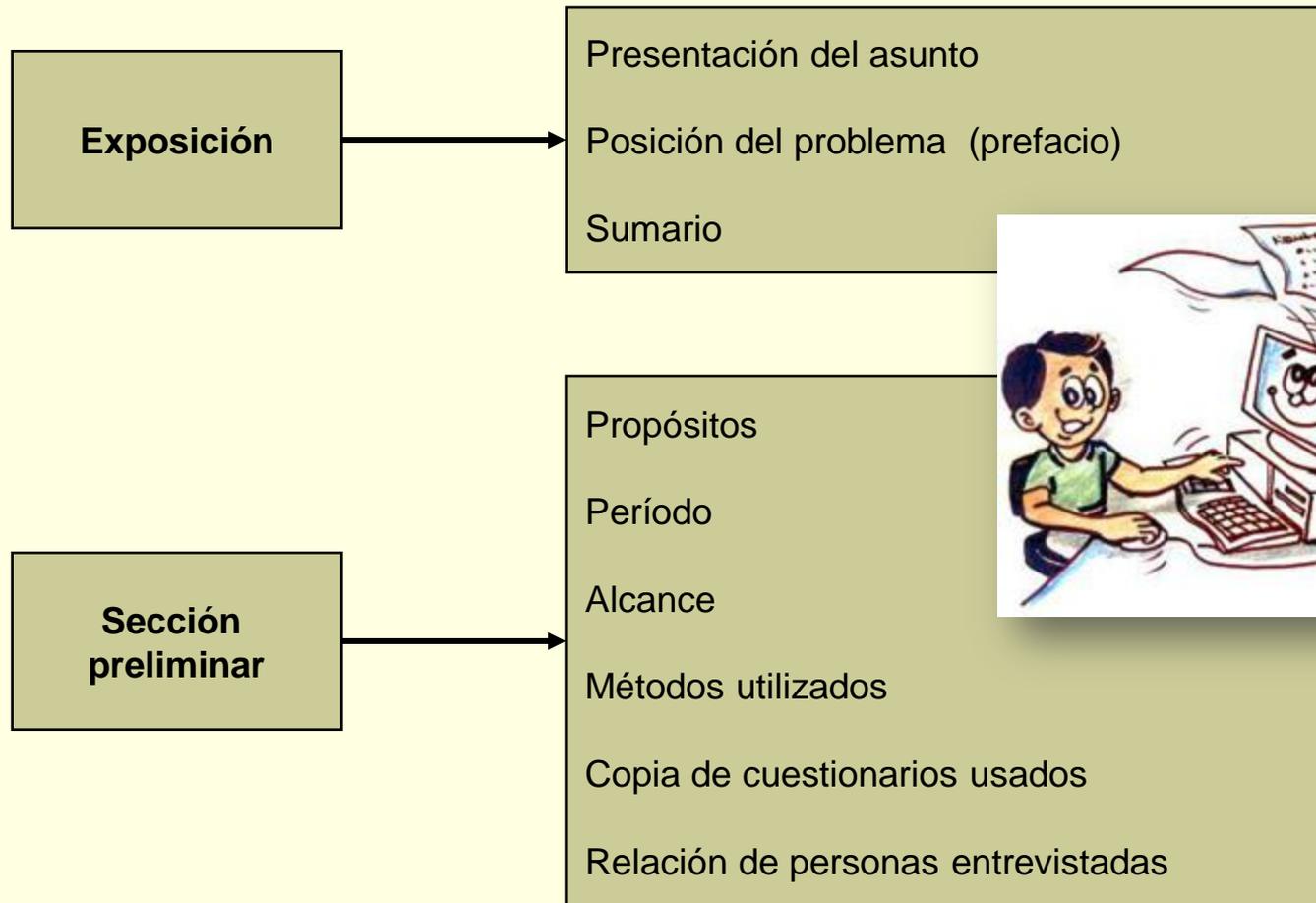
- La función auditora se materializa exclusivamente por escrito. El auditor avala personalmente su juicio de forma documental.
- Por tanto, la elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad.
- Resulta evidente la necesidad de redactar borradores e informes parciales y previos al citado informe final, ya que es el método más adecuado para equilibrar las técnicas analíticas utilizadas durante la auditoría, con las sintéticas que la confección del informe necesita.
- Los borradores e informes parciales son los elementos de contraste de opiniones entre auditor y auditado y pueden descubrir fallos de apreciación en el auditor.
- Nuevamente ha de resaltarse que la auditoría difiere sustancialmente de cualquier actuación coercitiva. El auditado no es un acusado sino un profesional informático. En todo caso, la ética auditora ha de facilitar la información aproximada, pero clara, de los resultados provisionales de aquél.

# Estructura del informe completo

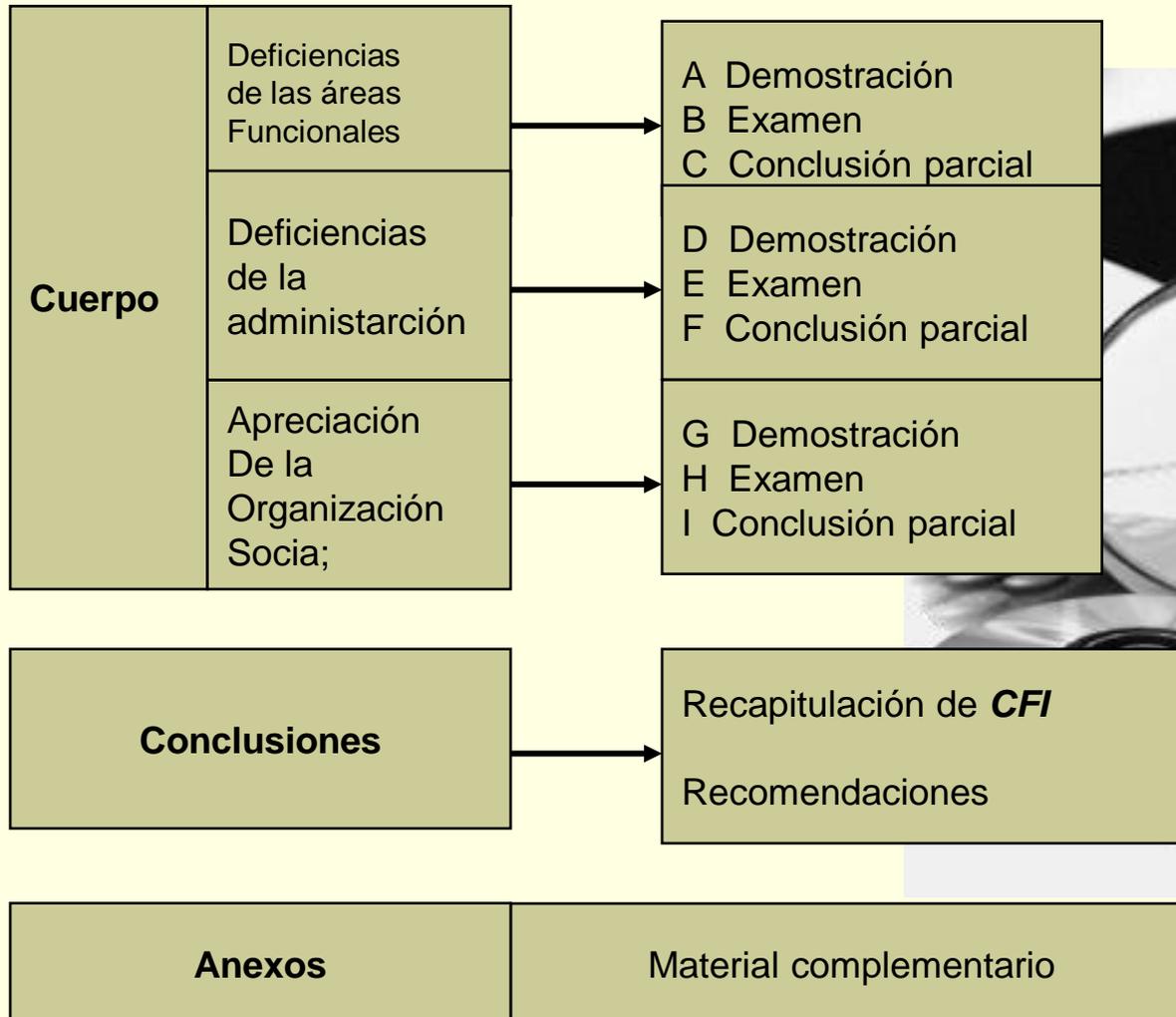
- Exposición
- Sección preliminar
- Cuerpo
  - ↖ Deficiencias de las áreas funcionales
  - ↖ Deficiencias de la administración
  - ↖ Apreciación de la organización social
- Conclusiones
- Anexos



# Estructura del informe completo



# Estructura del informe completo



# *Modelo conceptual de exposición del informe final*

- El Informe debe incluir solamente hechos importantes.- La inclusión de hechos poco relevantes o accesorios desvía la atención del que lo lee y desvirtúa el informe en su conjunto.
- El Informe debe consolidar los hechos que se describen en el mismo.- En auditoría, el término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados.

La consolidación de los hechos debe satisfacer, al menos, los siguientes criterios básicos:

1. El hecho que se incluya debe poder ser sometido a cambio.
2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
3. No deben existir alternativas viables que superen, por más beneficiosos y por mejor razón prestación/costo, al cambio propuesto.
4. La recomendación del auditor sobre el hecho en cuestión ha de mantener o mejorar las Normas y estándares existentes en la instalación.

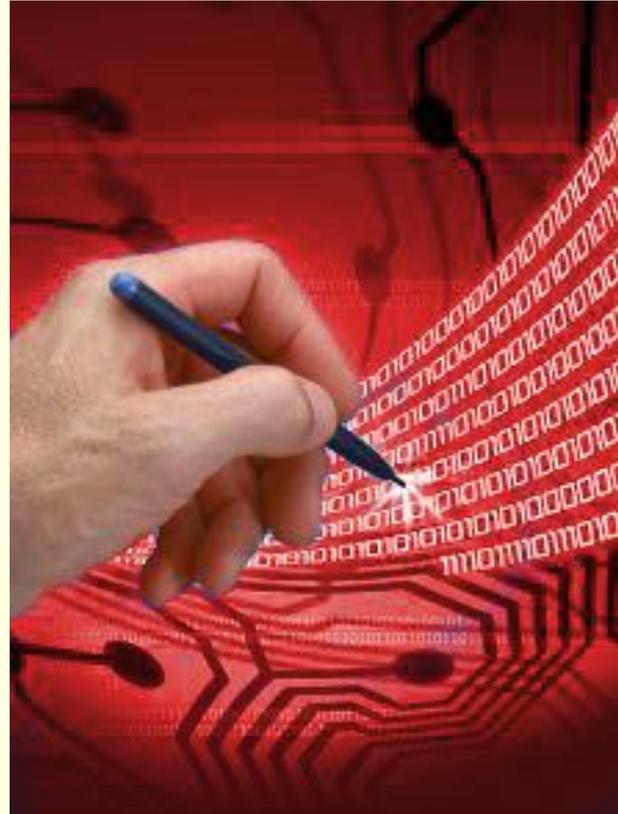
- Cumplidos los dos principios y los criterios de consolidación expuestos, el hecho pasa al Informe.
- La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.
- Veamos el modelo de flujo del hecho o debilidad, y el orden, desde su aparición hasta la recomendación del auditor para eliminarla

# 1. *Hecho encontrado*

- Ha de ser relevante para el auditor y para el cliente.
  - Ha de ser exacto, y además convincente.
  - No deben existir hechos repetidos. Deben procurarse evitar incluso las referencias y alusiones a otros hechos.
  - En lo posible contar con las evidencias necesarias
-

## 2. *Consecuencias del hecho*

- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.



### *3. Repercusión del hecho*

- Se redactará, si existe, las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa auditada.
-

## 4. *Conclusión del hecho*

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa y compleja.



## *5. Recomendación del auditor de sistemas*

- Siempre se explicitará la palabra "Recomendación", y ninguna otra.
  - Deberá entenderse por sí sola, por su simple lectura.
  - Deberá estar suficientemente soportada en el propio texto.
-

## *5. Recomendación del auditor de sistemas*

- Deberá ser concreta y exacta en el tiempo, para que pueda ser seguida y verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.



## *5. Recomendación del auditor de sistemas*

- Deberán evitarse las recomendaciones demasiado generales.
  - No deberán redactarse expresiones como "... se den las órdenes oportunas para que...".
  - Se deberá decir:  
"... se elabore un programa para que en 60 días...".
-

# Profesión, actividades y conocimientos deseables en un auditor de sistemas

- Sin ánimo exhaustivo, y de modo sinóptico en el siguiente cuadro, se han relacionado los perfiles profesionales de lo que podría ser un equipo auditor informático para abordar una revisión general de la Informática en una organización.



PROFESION	ACTIVIDADES Y CONOCIMIENTOS DESEABLES
Informático en general	<i>Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.</i>
Experto en Desarrollo de Proyectos	<i>Amplia experiencia como responsable de Proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.</i>
Técnico de Sistemas	<i>Experto en Sistemas Operativos y Software Básico. Conocedor de los Productos equivalentes en el mercado. Amplios conocimientos de Explotación.</i>
Experto en Base de datos y administración de las mismas	<i>Con experiencia en mantenimiento de BD. Conocimiento de Productos compatibles y equivalentes. Buenos conocimientos de Explotación.</i>
Experto en Software de Comunicaciones	<i>Alta especialización dentro de la Técnica de Sistemas. Conocimientos profundos de Redes. Muy experto en Subsistemas de Teleproceso.</i>
Experto en Explotación y Gestión de Centro de Proceso de Datos	<i>Responsable de algún Centro de Cómputo. Amplia experiencia en Automatización de Trabajos. Experto en relaciones humanas. Buenos conocimientos de los Sistemas.</i>
Técnico de Organización	<i>Experto organizador y coordinador. Especialista en el análisis de flujos de información.</i>
Técnico de evaluación de Costos	<i>Economista con conocimientos de informática. Gestión de Costos.</i>

# Índice recomendable

<b>Tema</b>	<b>pág</b>
■ Introducción	1
■ Objetivos particulares de la auditoría	3
■ Seguridad física	4
■ Objetivo general	4
■ Objetivo específico	4
■ Alcance	4
■ Definición	5
■ Situación actual	5
■ Tendencias	6
■ Puntos débiles y amenazas	6
■ Recomendaciones y plan de acción	7
■ Seguridad del personal	
■ Objetivo general	7
■ Objetivo específico	7
■ Alcance	8
■ Definición	8
■ Situación actual	9
■ Tendencias	9
■ Puntos débiles y amenazas	9
■ Recomendaciones y plan de acción	10



# Índice recomendable (continua)

■	Seguridad del software	
■	Objetivo general	10
■	Objetivo específico	10
■	Alcance	11
■	Definición	11
■	Situación actual	12
■	Tendencias	12
■	Puntos débiles y amenazas	12
■	Recomendaciones y plan de acción	13
■	Seguridad de los datos	
■	Objetivo general	13
■	Objetivo específico	13
■	Alcance	14
■	Definición	14
■	Situación actual	15
■	Tendencias	15
■	Puntos débiles y amenazas	15
■	Recomendaciones y plan de acción	16

# Índice recomendable (continua)

■ Seguridad en las redes y telecomunicaciones	
■ Objetivo general	16
■ Objetivo específico	16
■ Alcance	17
■ Definición	17
■ Situación actual	17
■ Tendencias	18
■ Puntos débiles y amenazas	18
■ Recomendaciones y plan de acción	19
■ Seguridad en el área de operaciones	
■ Objetivo general	19
■ Objetivo específico	19
■ Alcance	20
■ Definición	20
■ Situación actual	20
■ Tendencias	21
■ Puntos débiles y amenazas	21
■ Recomendaciones y plan de acción	22



# Índice recomendable (continua)

■ Seguridad en mini y micro computadoras	
■     Objetivo general	22
■     Objetivo específico	22
■     Alcance	23
■     Definición	23
■     Situación actual	23
■     Tendencias	24
■     Puntos débiles y amenazas	24
■     Recomendaciones y plan de acción	25
■ Conclusiones	26
■ Anexos	28

