Clase de Auditoría de Sistemas
Administración de Recursos

Índice General

Introducción de Auditoría de Sistemas....3
Auditoría de sistemas 3
El control Interno....4
Categoría de Controles 4
Tipos de Prueba 5
Áreas de la auditoría de sistemas de información 5
Pasos para la ejecución de una auditoría de sistemas de información....6
Planificación de la auditoría 6
Factores de afectan la complejidad de una auditoría de sistemas de información 7
Selección del área o aplicación a auditar....7
Carta de auditoría....8
Desarrollo del programa de auditoría 9
La evidencia en auditoría....10
Los informes de auditoría....10
Bibliografía utilizada....12

Apunte de Auditoría de Sistemas de Información

Introducción a la función de auditoría

Cabe mencionar que la auditoría de sistemas no se encuentra desligada de una auditoría general (que comprende también aspectos contables y operativos) de una empresa, por ello sus funciones integran el plan general de la misma.
Las auditorías pueden ser realizadas por gente de la misma empresa, o por auditores externos. De allí la división de auditorías externas e internas. El objetivo de la auditoría interna es ayudar a la gerencia a ejecutar sus funciones con efectividad, lo que implica las siguientes actividades:

- Revisión o evaluación de la adecuación, profundidad y aplicación de controles.
- Determinación del cumplimiento de las políticas, planes y procedimientos establecidos.
- Verificación de la adecuada registración de los activos de la empresa y su resguardo frente a pérdidas.
- Recomendaciones sobre el mejoramiento operativo.

Generalmente, las auditorías contables son de tipo externo, mientras que las operativas son de tipo interno.
La auditoría de sistemas tiene naturaleza operativa (Revisiones de controles de aplicaciones o de sistemas lógicos de seguridad, por ejemplo).

El auditor, deberá tener independencia de criterio a la hora de realizar una auditoría. Eso se logrará identificando una correcta estructura organizacional y a su objetividad. La organización deberá estar estructurada de manera tal que la función de la auditoría interna dependa de un funcionario que posea suficiente autoridad como para tomar acción sobre el personal, frente a recomendaciones o hallazgos que el auditor pueda mencionar. La objetividad del mismo, se manifiesta mediante la imposibilidad de que el auditor se involucre en el desarrollo e instalación de procedimientos que deban luego ser motivo de examen y revisión por el mismo implementador.

Auditoría de sistemas

La auditoría de sistemas se define como la revisión sistemática organizada de los sistemas en funcionamiento para ver si en ellos se verifican las propiedades de:

- VIGENCIA de los objetivos planeados como base del diseño original.
- CONCORDANCIA del sistema con los objetivos.
- PERMANENCIA del diseño por no haber sufrido alteraciones que lo degradan operativamente.
- EFICIENCIA del sistema

La auditoría de sistemas de información concentra sus esfuerzos en los aspectos relacionados con el control de sistemas. En consecuencia, la auditoria debe asegurar, con respecto a los sistemas, lo siguiente:

- La existencia de pistas de auditoría, de modo tal que las operaciones puedan ser rastreadas a través de todo el sistema.
- La existencia de controles adecuados con respecto a la entrada de datos y al mantenimiento de la integridad de los mismos, así como también de las

transacciones que se efectúan con ellos a través del segmento computarizado del sistema.
- El manejo adecuado de las excepciones y de los rechazos originados por los controles de entrada de datos, y el aseguramiento de su incorporación al sistema en los casos que corresponda.
- El aseguramiento de que las políticas corporativas y el cumplimiento de reglamentos gubernamentales hayan sido incorporados al sistema.
- La verificación de que los sistemas se comporten conforme fueron definidos.
- El control de que las modificaciones que se operen sobre los sistemas sean debidamente autorizadas por el nivel jerárquico que corresponda.
- La existencia de condiciones y procedimientos de seguridad que protejan los datos de la organización.
- El aseguramiento de la adecuada interconexión entre los diversos sistemas.

<u>El control Interno</u>

La evaluación del control interno es necesaria para determinar el alcance de las pruebas a las cuales deben restringirse los procedimientos de auditoría.
Los tipos de controles que constituyen los componentes de un sistema de control interno son los siguientes:

- Controles contables internos: conciernes a la salvaguardia de los activos y a la confiabilidad de los riesgos contables.
- Controles operativos: inherentes a las operaciones, funciones y actividades diarias. Garantizan que las operaciones satisfagan los objetivos del negocio.
- Controles administrativos: destinados a controlar la eficacia en un área funcional, en cumplimiento de las políticas gerenciales y su adhesión a las normas de la administración.

De las definiciones anteriores surgen los objetivos de control:

- Resguardo de activos
- Cumplimiento de políticas corporativas y exigencias legales.
- Verificación de la exactitud e integridad de las transacciones.
- Aseguramiento de la confiabilidad de los procesos.
- Control de la eficiencia y economía de las operaciones.

Todo sistema de control interno tiene limitaciones. Por eso puede brindar solo una seguridad “razonable” en el logro de sus objetivos. Estas limitaciones surgen de las siguientes circunstancias:

- El control se ejerce principalmente hacia las operaciones respectivas.
- Ejercer control implica un costo.
- Siempre estará latente la posibilidad de burlar en control que se apoya en la separación de funciones. (Violación del control por oposición de intereses)

<u>Categorías de controles</u>

Control Preventivos: Diseñados para evitar que se produzca un error, omisión o acto doloso.
Control Correctivo: Corrige errores, omisiones o actos maliciosos.
Control de Detección: Detectan que se ha producido un error, omisión o acto malicioso, e informan de su aparición.

Tipos de pruebas

En las auditorías se distinguen dos categorías de pruebas: Las de cumplimiento y las sustantivas.

Una prueba de cumplimiento tiene por objeto determinar si los controles se ajustan a las políticas y procedimientos de la organización, y si se aplican conforme a la descripción de la documentación de los programas de computación, mientras que las pruebas sustantivas intentan verificar la adecuación de los controles existentes para proteger a la organización de actividades fraudulentas.

Áreas de la auditoría de sistemas de información

- Revisión de controles generales: Son los que afectan a la estructura organizacional, a las políticas y procedimientos y al ambiente de control de los sistemas de información.
- Revisión de las operaciones de procesamiento de información: Se refiere a todas las operaciones que se realizan dentro del entorno informático.
- Revisión de seguridad: Abarca la revisión de la calidad de acceso lógico, acceso físico y de los controles del ambiente informático.
- Revisión del SW del SO: Se relaciona con la revisión de las políticas y procedimientos de desarrollo y adquisición mantenimiento del SW del SO.
- Revisión de la metodología para el desarrollo de sistemas de información: Abarca la revisión de la metodología empleada, las normas y los procedimientos para el desarrollo, la adquisición y mantenimiento del SW dentro del ciclo de vida del desarrollo de sistemas u otras estrategias que se adopten.
- Revisión de los controles del SW de aplicación: Comprende la revisión y evaluación de las fortalezas y debilidades de los puntos de control y procedimientos de control que deben permanecer insertos en los sistemas de aplicación de la organización.
- Plan de contingencias: Consiste en Verificar la existencia y aplicación de políticas y procedimientos referentes a recuperación de información y continuidad de operaciones en cas de presentación de desastres.

Pasos para la ejecución de una auditoría de sistemas de información

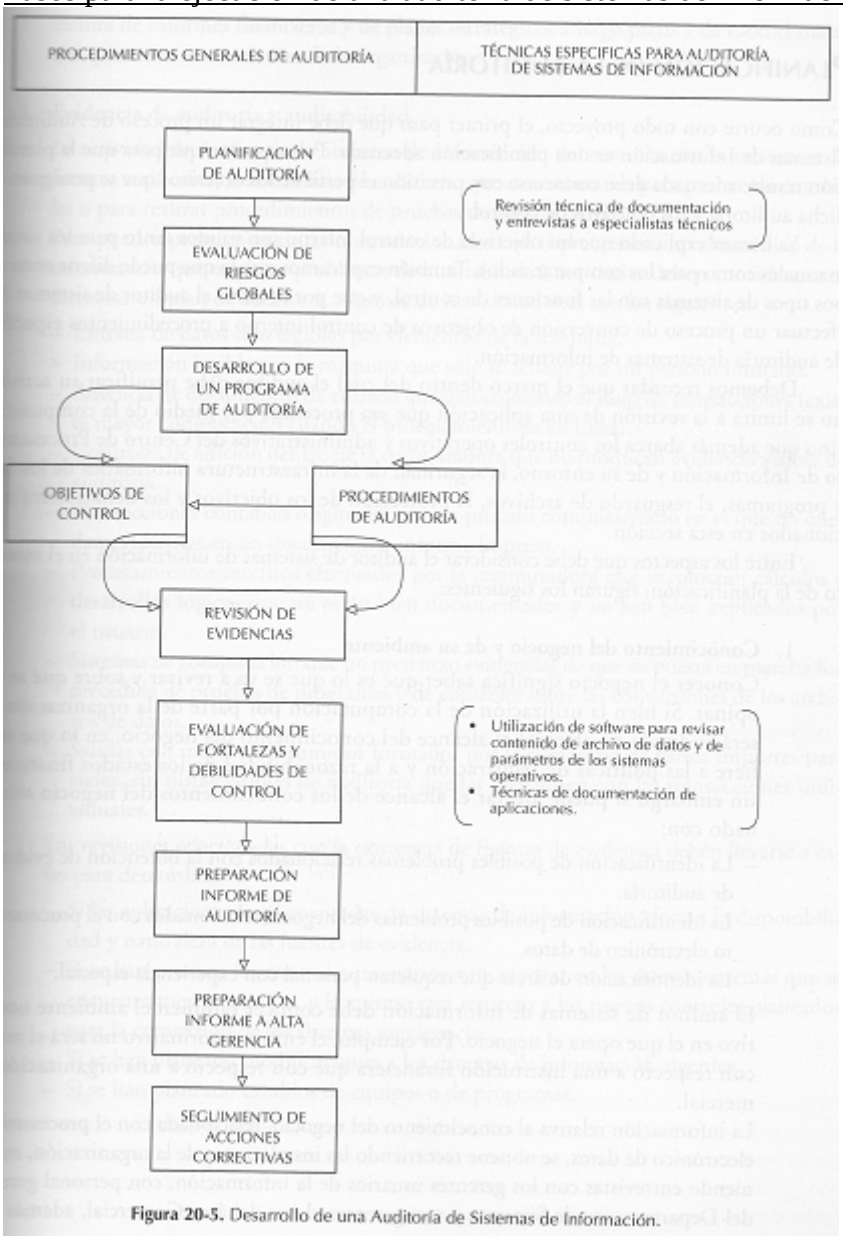


Figura 20-5. Desarrollo de una Auditoría de Sistemas de Información.

Planificación de la auditoría

En la misma deberá conocerse el perfil de los objetivo que se persiguen con dicha auditoría y cuáles son los objetivos de control. Cabe recordar que el marco dentro del cual el auditor debe planificar su actividad no se limita simplemente a la revisión de una aplicación, sino que además abarcará todos los controles operativos y administrativos, la seguridad y la infraestructura informática de los datos y programas, el resguardo de archivos, la protección de los objetivos, etc. Por ello, los aspectos más destacados que se deberán considerar al momento de la planificación son:

1) Conocimiento del negocio y de su ambiente
    a. Saber qué se va a revisar y sobre que se va a opinar. Para ello deberá contar con:
        i. La identificación de posibles problemas relacionándolos con la obtención de evidencias de auditorías.
        ii. La identificación de posibles problemas del negocio relacionados con el procesamiento electrónico de datos.

iii. La identificación de áreas que requieran personal con experiencia especial.

2) Evidencia de auditorías y auditabilidad
   a. La actividad de Auditoría de Sistemas de información debe contar con la existencia de fuentes verificables de evidencia de auditoría, que son necesarias para probar los controles o para realizar procedimientos de pruebas de sustanciación.

Factores de afectan la complejidad de una auditoría de sistemas de información

FACTORES QUE AFECTAN LA COMPLEJIDAD DE UNA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

FACTORES	CONDICIONES QUE IMPLICAN UN AUMENTO DE COMPLEJIDAD
Objetivos de la auditoría de sistemas de información	Situaciones en que las expectativas respecto de los resultados de la autoridad exceden los requerimientos para detectar errores relevantes, tales como un análisis de la eficiencia del procedimiento de la información.
Evidencia de auditoría	La ausencia de salidas impresas con detalle de las transacciones o la falta de homogeneidad y frecuencia en la aplicación de controles.
Características de las aplicaciones de computación	Lógica de procesamiento compleja, incluso de fórmulas o cálculos no explicados con claridad, generación interna de datos que ingresan automáticamente sin evidencias a otra fase del proceso, datos que provienen de otras fases sin una clara determinación de su lógica de generación.
Confiabilidad en los controles	Ausencia o debilidad de los controles requeridos por los sistemas en cuanto a responsabilidad del usuario como a los que deberían estar incorporados a los sistemas.
Estabilidad de los sistemas de información	La ejecución frecuente de modificaciones a los sistemas en vigencia o introducción de nuevos.
Grado de complejidad de los recursos informáticos	Utilización de tecnología sofisticada (hardware y software)
Descentralización extendida	Transferencia de datos entre múltiples puntos. Falta de normalización de los procedimientos.
Técnicas de auditoría	Necesidad de aplicar técnicas de auditoría que incluyan el uso de la computadora.

Selección del área o aplicación a auditar

El auditor no podrá auditar todos los sistemas al mismo tiempo. Para ello deberá establecer criterios que faciliten el ordenamiento y la selección de la muestra a auditar. Estos son:

1) Nivel de los activos controlados por el sistema
2) Dimensión de la aplicación
3) Impacto sobre las decisiones
4) Expectativa de vida de la aplicación

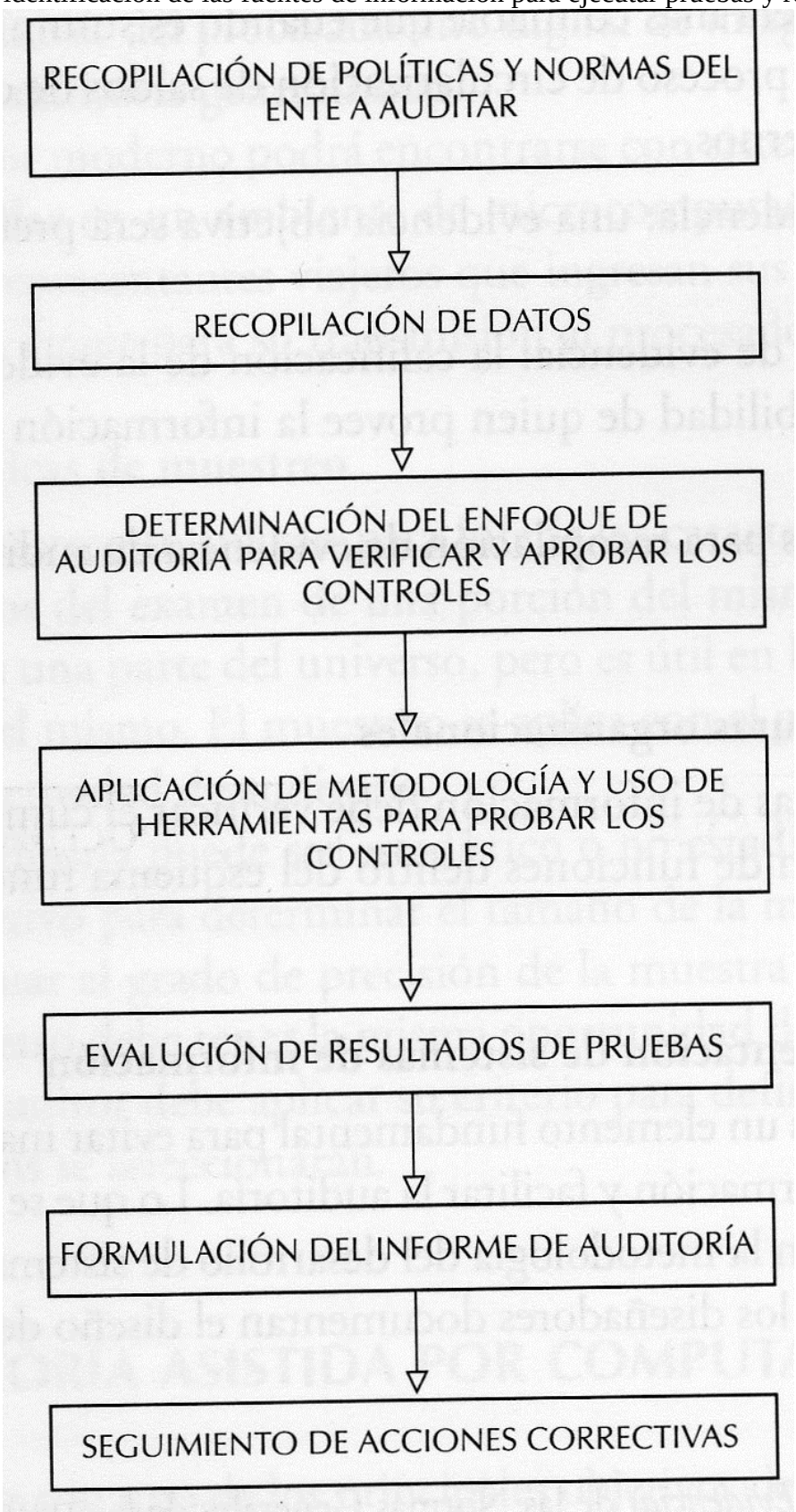
5) Sensitividad de la información

Carta de Auditoría

El trabajo de auditoría exige el apoyo de los niveles jerárquicos más altos dentro de la organización. Para poder reportar a los mismos se utilizan dos tipos de documentos; LA CARTA FUNDAMENTAL y la CARTA FUNDAMENTAL DEL PROYECTO. La primera define el grado de autoridad, el alcance y responsabilidad de la función de auditoría, la segunda, sin embargo determinará los objetivos de la misma para cada área o aplicación a auditar. La misma incluye el cronograma de actividades, los recursos y áreas que abarca el trabajo e informes a formular.

Desarrollo del programa de auditoría

Una vez finalizada la planificación, quedará definido el tema y área que se va a auditar, el objetivo de la auditoría, su alcance, las habilidades técnicas y recursos necesarios y la identificación de las fuentes de información para ejecutar pruebas y revisiones.



La evidencia en auditoría

El concepto de "Evidencia" es definido como el conjunto de información que ha reunido y que dispone el auditor para determinar si el ente, o los datos auditados han cumplido con los criterios u objetivos de la auditoría en cuestión. Las fuentes de la evidencia pueden ser los resultados de las pruebas de auditoría efectuadas o de las entrevistas con responsables de área, la documentación examinada u observaciones propias del auditor.

La evidencia debe reunir condiciones de calidad y cantidad. Dicha evidencia deberá ser entonces, competente y suficiente. Además la evidencia deberá ser confiable, y para ello se definen algunos parámetros a tener en cuenta. A saberse:

1) Evidencia de fuente externas.
2) Objetividad de la evidencia.
3) Calidad de la fuente de la evidencia.

Para reunirse de evidencias potables, el auditor cuenta con diversas técnicas de recopilación de evidencia. Las mismas son detalladas a continuación:

a) Revisión de estructuras organizacionales: El auditor deberá verificar el cumplimiento de los criterios referidos a segregación de funciones dentro del esquema funcional del procesamiento de la información.
b) Revisión de documentación de sistemas de información: La documentación es un elemento fundamental para evitar malos entendidos, producir mejores sistemas de información y facilitar la auditoría. Lo que se documenta es el resultado de los pasos que integran la metodología de desarrollo de sistemas. Los usuarios documentan sus requerimientos y los diseños documentan el diseño de los procesos.
c) Aplicación de técnicas de muestreo: El muestreo se aplica para reducir el tiempo y el costo de una auditoría. El mismo puede ser o no estadístico, en cuyo caso uno dependerá exclusivamente de algún método objetivo para la selección del tamaño de la muestra y los criterios de selección de la misma, mientras que en el otro se basará exclusivamente en el criterio del auditor para definir el tamaño la muestra y el método de selección de la misma.

Los informes de auditoría

La auditoría deberá concluir con un informe y en su posterior seguimiento, y también con los cursos de acción que debieran seguir como consecuencia de las recomendaciones contenidas en el informe.

Dicho informe debe reflejar las conclusiones a las cuales arribó el auditor luego del desarrollo de la auditoría.

El informe tiene la opinión del auditor, por tanto él deberá definir cuáles han sido las fortalezas y las debilidades del proceso de auditoría al que se ha sometido el objeto de estudio.

Para poder determinar esas debilidades, el auditor puede utilizar una matriz de control, en la que registrará: sobre el eje vertical, los errores que puedan presentarse, y sobre el horizontal, los controles a través de los cuáles se pueden detectar o corregir esos errores.

El auditor deberá apelar a su juicio profesional en el momento de decidir cuáles de las evidencias detectadas incorporará en su informe de auditoría. Para ello evaluará el grado de materialidad de los hallazgos, teniendo en cuenta el nivel de la estructura empresaria que se verá afectado por las observaciones y recomendaciones. El informe de auditoría conforma uno de los productos finales del trabajo del auditor. Es el elemento de

comunicación entre el auditor y la alta gerencia, como también, el elemento de transmisión de observaciones y recomendaciones.
Los informes de auditoría tienen por lo general, una determinada estructura y un determinado contenido:

INFORME DE AUDITORÍA

1) **Introducción**
   Debe incluir los objetivos de auditoría, el área o funciones abarcadas, el período que cubrió la revisión y el alcance o extensión de los procedimientos de auditoría utilizados.

2) **Descripción de hallazgos y formulación de recomendaciones**
   Se incluirán las fuentes de las evidencias.

3) **Detalles de las acciones correctivas a desarrollar**

4) **Expresión de la opinión del auditor sobre la situación encontrada**
   Se refiere a la adecuación de los controles, grado de cumplimiento de los mismos y conclusión sobre los procedimientos que fueron sujetos a revisión. La opinión del auditor debe quedar respaldada en el informe a través de las evidencias recopiladas durante la ejecución de la revisión.

5) **Anexos**
   Tienen el propósito de mencionar información muy detallada a la que el lector podrá recurrir o no de acuerdo a su interés o predisposición. Se trata de detalles que podrían ser importantes, pero cuya inclusión en el texto principal puede provocar en el lector la desviación de su atención del tema básico hacia detalles secundarios. Cuando el informe incluye anexos en el texto del mismo deberá hacerse referencia a la información ampliatoria o aclaratoria.

Cuando el informe es elaborado y presentado por un auditor independiente, existen cuatro posibilidades en cuanto a tipos de informe:

Informe sin salvedades
Informe con salvedades
Informe con opinión adversa
Informe sin opinión

Bibliografía utilizada:

Sistemas de información para la gestión empresaria, de Alberto R. Lardent. Editorial Prentice Hall