REALIZACIÓN DE UNA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

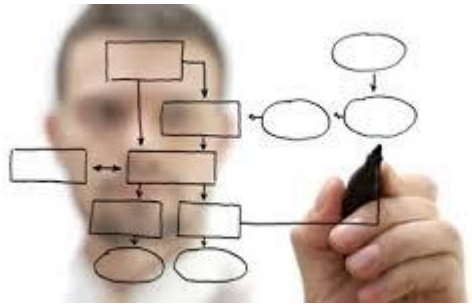
Inga. Evelyn Yesenia Lobos Barrera-M.A.-CISA

CLASIFICACIÓN DE LAS AUDITORÍAS

El auditor de SI debería entender los diversos tipos de auditorias que pueden efectuarse interna o externamente, y los procedimientos de auditoria asociados con cada uno de ellos:

Auditorías Financieras – El propósito de una auditoría financiera es determinar la exactitud de los estados financieros de una organización. Una auditoría financiera a menudo implica pruebas sustantivas detalladas, aunque cada vez más, los auditores están poniendo más énfasis en un enfoque de auditoria basada en riesgo y control. Este tipo de auditoría se relaciona con la **integridad y confiabilidad** de la información financiera.

CLASIFICACIÓN DE LAS AUDITORÍAS



Auditoria Operativas- Una auditoría operativa está diseñada para evaluar la estructuras del control interno en un proceso o área determinada. Las auditorias de SI sobre controles de las aplicaciones o de sistemas de seguridad lógica son algunos ejemplos de auditorias operativas.

Auditorías Integradas- Una auditoría integrada combina pasos de auditorías financiera y operativa. También se realiza para evaluar los objetivos generales dentro de una organización, relacionadas con la información financiera y la salvaguarda de activos, la eficiencia y el cumplimiento. Una auditoría integrada puede ser ejecutada por auditores externos o internos e incluiría pruebas de cumplimiento a los controles internos y los pasos de auditorías sustantivas.

CLASIFICACIÓN DE LAS AUDITORÍAS

Auditorías administrativas- Estas están orientadas a evaluar aspectos relacionados con la eficiencia de la productividad operativa dentro de una organización.

Auditoría de Sistemas de Información – Este proceso recolecta y evalúa la evidencia para determinar si los sistemas de información y los recursos relacionados protegen adecuadamente los activos, mantienen la integridad y disponibilidad de los datos y del sistema, proveen información relevante y confiable, logran de forma efectiva las metas organizacionales, usan eficientemente los recursos y tienen en efecto controles internos que proveen una certeza razonable de que los objetivos del negocio, operacionales y de control serán alcanzados y que los eventos no deseados serán evitados o detectados y corregidos de forma oportuna.

CLASIFICACIÓN DE LAS AUDITORÍAS

Auditorías especializadas- Revisiones especializadas que examinan áreas tales como los servicios realizados por terceros.

Auditorías forenses – Esta ha sido definida como una auditoria especializada en descubrir, revelar y hacer seguimiento a fraudes y crimines. En años recientes, el profesional forense ha sido llamado a participar en investigaciones relacionadas con fraude corporativo y crimen cibernético.

La consideración más importante para un auditor forense es la de obtener una imagen completa (bit-stream) del dispositivo objetivo y examinar esa imagen sin alterar los sellos de fecha u otra información atribuible a los archivos examinados.

METODOLOGÍA DE AUDITORÍA

3. Nuestra metodología

FASE I

Planeación de la Auditoría

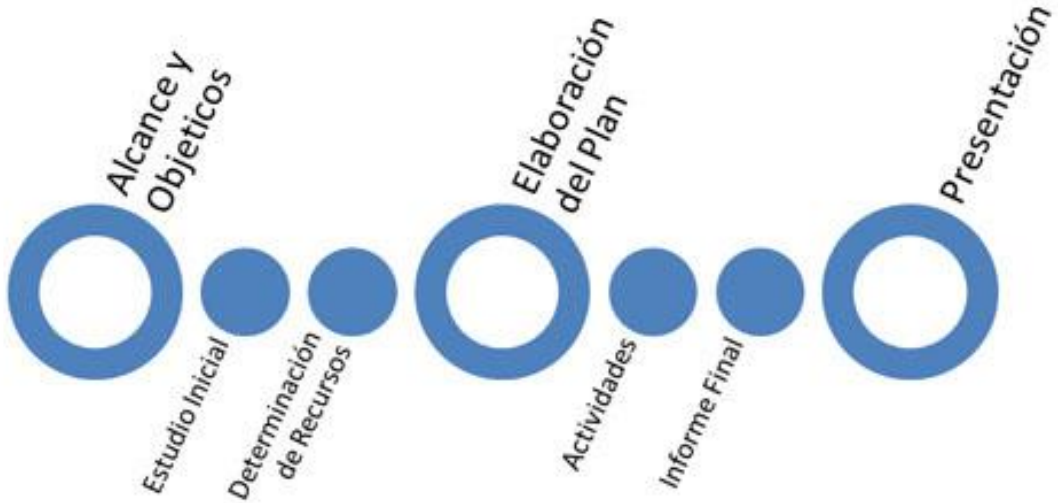
En esta fase obtenemos un entendimiento de:

- ✓ Las fuerzas internas y externas que pueden constituirse en riesgos del negocio y que tienen impacto significativo sobre los estados financieros.
- ✓ Controles de alto nivel (controles de la gerencia)
- ✓ Determinación de las transacciones significativas

METODOLOGÍA DE LA PROGRAMACIÓN DE AUDITORÍA

Es un conjunto de procedimientos documentados de auditoría diseñados para alcanzar los objetivos de auditoría planificados. Sus componentes son:

1. Una declaración del alcance
2. Una declaración de los objetivos de la auditoría
3. Una declaración de los programas de auditoría



PROGRAMAS DE AUDITORÍA

PROGRAMA DE AUDITORIA

OBJETIVO: Verificar el cumplimiento del proceso de Quejas y Solicitudes del programa de Servicio al Cliente utilizado por la Asistente Administrativa de la empresa PROTEMED de la ciudad de Bucaramanga

ALCANCE: La Auditoria Base de Datos tiene como propósito revisar cada uno de los pasos a seguir en el proceso de Quejas y Solicitudes de la empresa PROTEMED, verificando la eficiencia y efectividad en el ingreso de la información y la ejecución del proceso.

RECURSOS
Humanos, Tecnológicos, Físicos de Información Servicio al Cliente

FECHA DE ACTUALIZACION: 07/02/2011 | **DOCUMENTOS DE REFERENCIA** Soportes de Solicitudes y Quejas

PROCESO	SECRETARIA	FECHAS/CRONOGRAMA	RESPONSABLE
Antecedentes, misión, visión, objetivos, políticas, manuales, estructura organizacional	Auxiliar de Servicio al Cliente	07-02-2011 / 13-03-2011	Claudia Patricia Suárez V Ingrid Paola Sanabria B Jennifer Vanessa Caballero C.
Análisis del manejo de solicitudes y quejas de la empresa, control y seguimiento del proceso.	Auxiliar de Servicio al Cliente	14-03-2011 / 03-04-2011	
Indagación del personal que procesa la información de la solicitud o queja.	Auxiliar de Servicio al Cliente	04-04-2011 / 25-04-2011	
Informe Final	Auxiliar de Servicio al Cliente	26-04-2011 / 25-05-2011	

APROBADO: Jefe de Oficina de Control interno

ELABORADO POR : Claudia Patricia Suárez V, Ingrid Paola Sanabria B, Jennifer Vanessa Caballero C.

PROGRAMAS DE AUDITORÍA

Los programas de auditoría financieras, operativas, integradas, administrativas y de sistemas de información se basan en el alcance y el objetivo de la asignación en particular.

Los auditores de SI evalúan a menudo las funciones y los sistemas de TI desde perspectivas diferentes, tales como la seguridad (Confidencialidad, integridad y disponibilidad), la calidad (efectividad, eficiencia), fiduciaria (cumplimiento, confiabilidad), el servicio y la capacidad.

El programa de trabajo de auditoría es la estrategia de auditoria y el plan de auditoría- éste identifica el alcance, los objetivos y los procedimientos de auditoria para lograr evidencia suficiente, competente y confiable para obtener y sustentar las conclusiones y opiniones de auditoría.

PROCEDIMIENTOS GENERALES DE AUDITORÍA

Son los pasos básicos en la ejecución de una auditoría y habitualmente incluyen lo siguiente:

1. Obtención y documentación del conocimiento sobre el área/objeto de la auditoría.
2. Evaluación de riesgos y planificación general de la auditoría y cronograma.
3. Planificación de auditoría detallada.
4. Revisión preliminar del área/objeto de la auditoría
5. Evaluación del área/objeto de la auditoría
6. Verificación y evaluación de la pertinencia de los controles diseñados para cumplir los objetivos de control
7. Pruebas de cumplimiento (pruebas de la implementación de controles y su aplicación consistente)
8. Pruebas sustantivas (que confirmen la exactitud de la información)
9. Reporte (Comunicación de los resultados)
10. Seguimiento en casos en los hay una función de auditoría interna.

FASES DE LA AUDITORÍA

Fases de la auditoría	Descripción
Sujeto de la auditoría	Identificar el área que será auditada.
Objetivo de la auditoría	Identificar el propósito de la auditoría. Por ejemplo, un objetivo podría ser determinar si los cambios del código fuente del programa ocurren en un ambiente bien definido y controlado.
Alcance de la auditoría	Identificar los sistemas, funciones o unidades específicos de la organización que serán incluidos en la revisión. Por ejemplo en el ejemplo de cambios de programas anterior el enunciado de alcance podría limitar la revisión a solo un sistema de aplicación o a un periodo limitado.

FASES DE LA AUDITORÍA

Fases de la auditoría	Descripción
Planificación de pre auditoría	• Identificar habilidades y recursos técnicos necesarios. • Identificar las fuentes de información para prueba o revisión tales como flujogramas, políticas estándares, procedimientos y papeles de trabajo de auditorías anteriores. • Identificar las localidades o instalaciones que serán auditadas.
Procedimientos de auditoría y pasos para recolección de datos	• Identificar y seleccionar el enfoque de auditoria para verificar y comprobar los controles. • Identificar una lista de individuos que serán entrevistados. • Identificar y obtener las políticas, estándares y directrices departamentales para realizar la revisión. • Desarrollar herramientas y metodología de auditoría para probar y verificar el control.

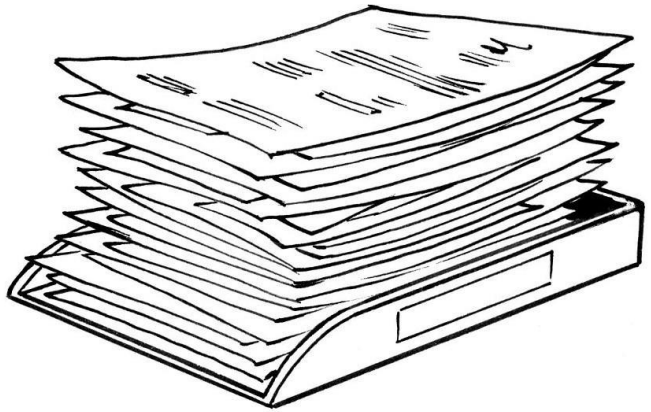
FASES DE LA AUDITORÍA

Fases de la auditoría	Descripción
Procedimientos para evaluar los resultados de la prueba o la revisión	Especifico de la organización
Procedimientos para la comunicaciones con la Gerencia	Especifico de la organización
Preparación del reporte de auditoría	• Identificar los procedimientos de seguimiento de la revisión. • Identificar los procedimientos para evaluar/probar la eficiencia y efectividad operacional. • Identificar los procedimientos para probar los controles. • Revisar y evaluar la calidad de los documentos, políticas y procedimientos

METODOLOGÍA DE AUDITORÍA

Todos los planes, programas, actividades, pruebas, hallazgos e incidentes de auditoría deberán estar debidamente documentados en papeles de trabajo.

Los documentos de trabajo se pueden considerar los puentes bridges o interfaces entre los objetivos y el informe final de auditoría.



OBJETIVOS DE LA AUDITORIA

OBJETIVOS DE LA AUDITORIA

Los objetivos de la auditoría se refieren a las metas especificas que deben cumplirse por parte de la auditoría.

Los objetivos de la auditoría se centran a menudo en validar que existen controles internos para minimizar los riesgos del negocio.

Un elemento clave en la planificación de una auditoría de sistemas de información es traducir los objetivos de auditoria básicos y de amplio alcance en objetivos específicos de auditoria de sistemas de información.

PRUEBAS DE CUMPLIMIENTO VRS. PRUEBAS SUSTANTIVAS

PRUEBAS DE CUMPLIMIENTO VRS. PRUEBAS SUSTANTIVAS

Las pruebas de cumplimiento consisten en recolectar evidencia con el propósito de probar el cumplimiento de una organización con procedimientos de control.

Esto difiere de la prueba sustantiva, en la que la evidencia se recoge para evaluar la integridad de transacciones individuales, datos u otra información.

Una prueba de cumplimiento determina si los controles están siendo aplicados de manera que cumplen con las políticas y los procedimientos de gestión. Este tipo de pruebas pueden usarse para probar la existencia y efectividad de un proceso definido, el cual puede incluir una pista de la evidencia documental y/o automatizada.

Una prueba sustantiva fundamente la integridad de un procesamiento real. Provee evidencia de la validez e integridad de los saldos en los estados financieros y de las transacciones que respaldan dichos saldos.

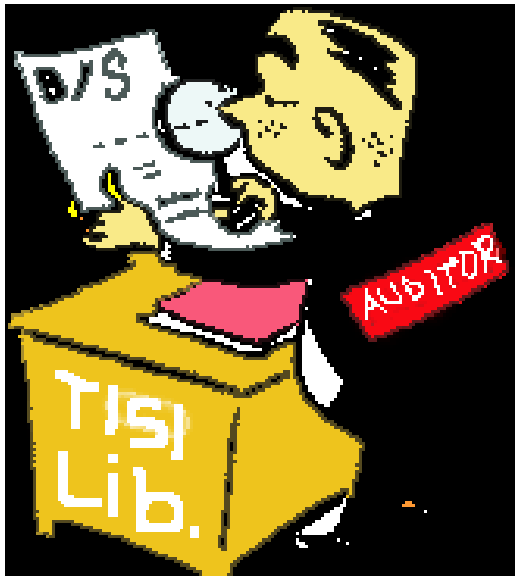
EVIDENCIA

EVIDENCIA

La evidencia es cualquier información usada por el auditor de Sistemas de Información para determinar si la entidad o los datos que están siendo auditados cumplen con los criterios u objetivos establecidos y soporta las conclusiones de auditoría.

Las siguientes son técnicas para la recopilación de evidencia:

- Revisión de las estructuras organizacionales de SI
- Revisión de políticas y procedimientos de SI
- Revisión de los estándares de SI
- Revisión de la documentación de SI
- Entrevista al personal apropiado
- Observación de procesos y desempeño de empleados



EVIDENCIA

En cuanto a la “evidencia” contenida en los papeles de trabajo, estos deberán cumplir los siguientes requisitos:

- Suficiencia. Será suficiente la evidencia objetiva y convincente que baste para sustentar los resultados y recomendaciones que se presenten en el informe de auditoría.
- Competencia. Para que sea competente, la evidencia deberá ser válida y confiable; es decir, las pruebas practicadas deberán corresponder a la naturaleza y características de las materias examinadas.
- Importancia. La información será importante cuando guarde una relación lógica y patente con el hecho que se desee demostrar o refutar.
- Pertinencia. La evidencia deberá ser congruente con los resultados, conclusiones y recomendaciones de la auditoría.

TÉCNICAS DE AUDITORÍA

ENTREVISTAS Y OBSERVACIÓN DEL PERSONAL DURANTE LA EJECUCIÓN DE SUS FUNCIONES

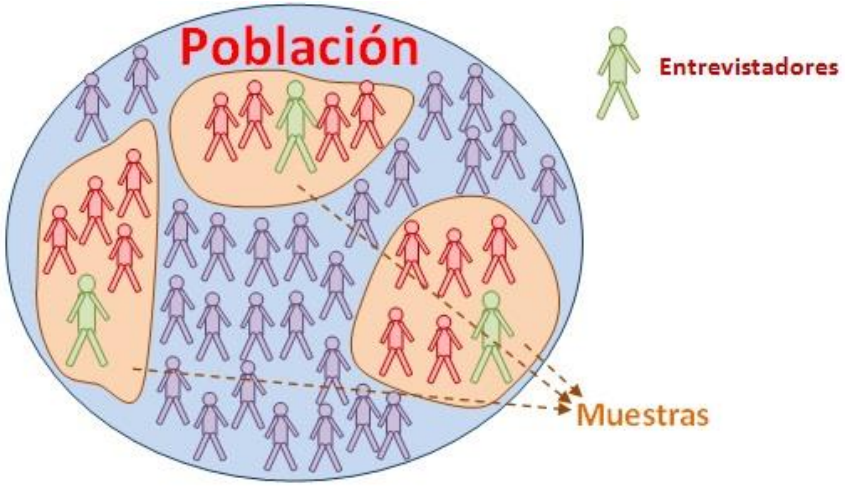
La observación al personal en el desempeño de sus funciones ayuda a un auditor de Sistemas de Información a identificar:

- Funciones reales- La observación podría ser una prueba adecuada para asegurar que la persona asignada y autorizada para realizar una función en particular es la persona que está realmente haciendo el trabajo.
- Procesos/procedimientos reales – La ejecución de un recorrido de proceso/procedimiento permite que el auditor se SI obtenga evidencia de cumplimiento y observe desviaciones, si las hubiera.
- Concienciación sobre seguridad – Se debe observar el grado de concienciación sobre seguridad que una persona tiene para verificar la comprensión y la práctica de buenas medidas.

ENTREVISTAS Y OBSERVACIÓN DEL PERSONAL DURANTE LA EJECUCIÓN DE SUS FUNCIONES

- Concienciación sobre seguridad – Se debe observar el grado de concienciación sobre seguridad que una persona tiene para verificar la comprensión y la práctica de buenas medidas.
- Líneas de reporte – Las líneas de reporte deben observarse para asegurar que se practiquen las responsabilidades asignadas y una segregación de funciones adecuada.

MUESTREO



El muestreo es usado cuando las consideraciones de tiempo y de costo impiden una verificación total de todas las transacciones o eventos en una población definida previamente.

Una muestra es un subconjunto de miembros de una población utilizada para realizar pruebas.

Los dos enfoques generales para muestreo de auditoría son el estadístico y el no estadístico:

- Muestreo Estadístico: Usa leyes matemáticas de la probabilidad para calcular el tamaño de la muestra, seleccionar los objetos y evaluar los resultados.
- Muestreo no estadístico : Utiliza el juicio del auditor para determinar el tamaño de la muestra, seleccionar los objetos y evaluar los resultados.

USO DE LOS SERVICIOS DE OTROS AUDITORES Y EXPERTOS.

Estos expertos podrían incluir:

Tecnologías especificas tales como redes, cajeros automáticos (ATM), integración de sistemas y conocimientos digitales forenses o expertos en la materia tales como especialistas en una industria o área de especialización en particular, tales como banca, comercio de títulos-valores, seguros expertos legales, entre otros.

PAPELES DE TRABAJO

PAPELES DE TRABAJO

Los papeles de trabajo cumplen principalmente los siguientes objetivos:

- Registrar de manera ordenada, sistemática y detallada los procedimientos y actividades realizados por el auditor.
- Documentar el trabajo efectuado para futura consulta y referencia.
- Proporcionar la base para la rendición de informes.
- Facilitar la planeación, ejecución, supervisión y revisión del trabajo de auditoría.
- Minimizar esfuerzos en auditorías posteriores.
- Dejar constancia de que se cumplieron los objetivos de la auditoría y de que el trabajo se efectuó de conformidad con las Normas de Auditoría del Órgano de Control y demás normatividad aplicable.
- Estudiar modificaciones a los procedimientos y al programa de auditoría para próximas revisiones.

NATURALEZA Y CARACTERÍSTICAS

Los papeles de trabajo deberán:

- Incluir el programa de trabajo y, en su caso, sus modificaciones; el programa deberá relacionarse con los papeles de trabajo mediante índices cruzados.
- Contener índices, marcas y referencias adecuadas, y todas las cédulas y resúmenes que sean necesarios.
- Estar fechados y firmados por el personal que los haya preparado.
- Ser supervisados e incluir constancia de ello.

NATURALEZA Y CARACTERÍSTICAS

- Ser completos y exactos, a fin de que muestren la naturaleza y alcance del trabajo realizado y sustenten debidamente los resultados y recomendaciones que se presenten en el informe de auditoría.
- Redactarse con concisión, pero con tanta precisión y claridad que no requieran explicaciones adicionales.
- Ser pertinentes, por lo cual sólo deberán contener la información necesaria para el cumplimiento de los objetivos de la auditoría.
- Ser legibles, estar limpios y ordenados, y tener espacio suficiente para datos, notas y comentarios (los papeles de trabajo desordenados reflejan ineficiencia y permiten dudar de la calidad del trabajo realizado).

COMUNICACIÓN DE LOS RESULTADOS DE LA AUDITORÍA

COMUNICACIÓN DE LOS RESULTADOS DE LA AUDITORÍA

La entrevista final, llevada a cabo al final del proceso de auditoría, provee al auditor de Sistemas de información de discutir los hallazgos y las recomendaciones con la gerencia.

Durante la entrevista final, el auditor de SI debería:

- Asegurarse de que los hechos presentados en el informe estén correctos.
- Asegurarse de que las recomendaciones sean realistas y eficientes, y si no lo fueran, buscar alternativas negociando con la gerencia del auditado.
- Sugerir fechas de implementación para las recomendaciones acordadas.

IMPLEMENTACIÓN DE LAS RECOMENDACIONES

IMPLEMENTACIÓN DE LAS RECOMENDACIONES

Los auditores de Sistemas deben de estar consientes de que la auditoria es un proceso continuo. El auditor de SI no es eficaz si se realizan las auditorias y se emiten los informes, pero no se realiza el seguimiento para determinar si la gerencia ha emprendido las acciones correctivas apropiadas.

El plazo del seguimiento dependerá de la gravedad de los hallazgos y estaría sujeto al criterio del auditor se sistemas.

PREGUNTAS

PREGUNTA 1

El primer paso en la planificación de una auditoría una auditoría es:

a) Definir los productos de la auditoría.
b) Finalizar el alcance de la auditoría y los objetivos de la auditoría.
c) Lograr una comprensión de los objetivos del negocio.
d) Desarrollar el método de auditoría o la estrategia de la auditoría.

PREGUNTA 2

El enfoque de un auditor de Sistemas debe usar para planificar la cobertura de la auditoría de Sistemas de Información debe estar basada en:

A. Riesgo
B. Importancia
C. Escepticismo profesional.
D. Suficiencia de la evidencia de auditoría.

PREGUNTA 3

Mientras se desarrolla un programa de auditoría basada en el riesgo, ¿en cual de los siguientes es MÁS probable que el auditor de SI se concentre?

A. Los procesos del negocio
B. Las aplicaciones críticas de TI
C. Los controles operacionales
D. Las estrategias del negocio.