Práctica 2 – Auditoría y Peritaje de Sistemas

Parte I: Conceptos generales

1. Explique las razones principales para auditar sistemas y dar ejemplos de cada una.

RAZONES PARA CONTROLAR
Problemas que enfrentan las organizaciones por las cuales es necesario pensar en funciones de auditoría:

1. COSTOS POR PÉRDIDAS DE DATOS
"Los datos proveen a la organización de una imagen de sí misma, de su entorno, de su historia, y su futuro". Si la imagen es exacta, la organización aumenta las posibilidades de adaptarse y sobrevivir a un entorno cambiante. Si la imagen es inexacta, se puede incurrir en pérdidas sustanciales.
Ejemplo: pérdida de cuentas corrientes, pérdida de los datos de los alumnos.

2. COSTOS POR DECISIONES INCORRECTAS
La alta calidad en la toma de decisiones depende, en parte, de:
• la calidad de los datos,
• la calidad de las reglas de decisión que existen en los SI automatizados.
La importancia de datos exactos depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.
Alta Gerencia → decisiones de planeamiento estratégico → probablemente acepten algunos errores en los datos
Gerencia Media → decisiones de control administrativo y de control operativo → requieren datos más exactos
El tener reglas de decisión exactas en un sistema de información (SI) depende del tipo de decisiones hechas por personas que tienen algún interés en la organización.
Ejemplo: cálculo de amortización erróneo en un bien de poco valor

3. COSTOS POR ABUSO COMPUTACIONAL
Definición: un abuso computacional es un incidente asociado con tecnología informática, en el cual una víctima sufre o podría haber sufrido pérdida, y un perpetrador con intención logra o podría lograr ganancia
El promedio de pérdidas por abusos computacionales pareciera ser sustancialmente mayor que las pérdidas producidas por fraudes convencionales.
Ejemplo:
hacking: Una persona logra un acceso no autorizado a un sistema de computación para leer, modificar o borrar datos o programas para discontinuar un servicio.
virus: Son programas que atacan a archivos ejecutables, áreas del sistema, o archivos de datos que contienen macros, para causar una disfunción en las operaciones computacionales o dañar datos y programas

abuso de privilegio: Hacen copias no autorizadas de los datos a los cuales se les otorgó acceso.
acceso físico ilegal: a una sala de cómputos o a una terminal.

4. COSTOS POR ERRORES DE COMPUTACIÓN
Los costos por un error de computación pueden ser altos, en términos de:
1) pérdida de vida humana,
2) privación de libertad,
3) daño al medio ambiente.
Ejemplo: Procesos automatizados que producen pérdida de dinero o incluso pérdida de vida humanas, daño al medio ambiente.

5. VALOR DE HW, SW Y PERSONAL
Recursos críticos en las organizaciones:
1) Datos - ¿qué pasa si la competencia obtiene información confidencial?
2) Hardware - ¿qué pasa si un componente crítico deja de funcionar?
3) Software - ¿qué pasa si se destruye?
4) Personal - ¿qué pasa si un profesional calificado deja la empresa?
Ejemplo: Determinar el impacto que alguno de estos valores críticos pueda fallar

6. MANTENIMIENTO DE PRIVACIDAD
Muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia.
Con sistemas automatizados se puede integrar y buscar información.
Prevenir la exposición de datos privados de los usuarios de un sistema.
Ejemplo: Se podrían utilizar datos de genética humana para obtener información detallada sobre una persona y usarla en su contra.

7. EVOLUCIÓN CONTROLADA DEL USO
Se argumenta que la confiabilidad de los sistemas computarizados complejos no está garantizada.
Las consecuencias de usar sistemas no confiables puede ser catastrófica.
Debe existir interés para evaluar y controlar la implementación de esta tecnología.
¿Qué efectos físicos y mentales tienen las computadoras en los usuarios?
Ejemplo

2. Para cada uno de los siguientes interesados, presente un ejemplo de cómo un mal procesamiento de información realizado por un sistema informático, puede conducir a una toma de decisiones incorrecta:

- ➔ **Gerente de una empresa vinculada a la industria automotriz:** Un mal cálculo podría ocasionar información errónea sobre el stock disponible teniendo inconvenientes en el momento de entregar los vehículos.
- ➔ **Funcionario de ARBA:** Un fallo en el cálculo de los valores fiscales de bienes puede ocasionar un error de revalorización, ocasionando pérdidas importantes de recaudación de la provincia.
- ➔ **Consejo Directivo de una facultad:** Una pérdida de datos relacionados con la historia académica de los alumnos.

3. ¿Qué tipo de abusos computacionales conoce? ¿Cuáles son las consecuencias de estos abusos?

Definición: un abuso computacional es un incidente asociado con tecnología informática, en el cual una víctima sufre o podría haber sufrido pérdida, y un perpetrador con intención logra o podría lograr ganancia

Tipos de abusos:

1) hacking: Una persona logra un acceso no autorizado a un sistema de computación para leer, modificar o borrar datos o programas para discontinuar un servicio.

2) virus: Son programas que atacan a archivos ejecutables, áreas del sistema, o archivos de datos que contienen macros, para causar una disfunción en las operaciones computacionales o dañar datos y programas [Nachenberg, 1997].

3) acceso físico ilegal: Una persona logra un acceso físico no autorizado a facilidades del computador.

4) abuso de privilegios: Una persona usa privilegios, que le han sido asignados, para propósitos no autorizados.

CONSECUENCIAS DE ABUSOS

1) Destrucción de activos.
2) Sustracción de activos.
3) Modificación de activos.
4) Violación de privacidad.
5) Interrupción de operaciones.
6) Uso no autorizado de activos.
7) Daño físico a personas.

4. Explique al menos dos características que diferencien entre un abuso informático y otro tipo de fraude comercial.

El promedio de pérdidas por abusos computacionales pareciera ser sustancialmente mayor que las pérdidas producidas por fraudes convencionales.

Dado a que los sistemas controlan monitoreo de pacientes, cirugías, vuelo de misiles, reactores nucleares, etc un abuso informático puede resultar altamente peligroso e incluir (a diferencia de un fraude comercial):

- ➔ La pérdida de vidas humanas
- ➔ Daño al medio ambiente

5. Describa con sus palabras qué entiende por auditoría de sistemas de información.

Definición: La auditoría de sistemas de información es el proceso de recolectar y evaluar evidencia para determinar si:

1) el sistema automático preserva los activos,
2) mantiene la integridad de los datos,

3) permite que los objetivos organizacionales se alcancen con eficacia,
4) usa los recursos con eficiencia.

Muchas veces la auditoría tiene otro propósito: asegurar que la organización cumple con determinadas regulaciones, reglas y condiciones, ya sea voluntaria o involuntariamente.

6. Explique los cuatro objetivos de la auditoría de sistemas de información.

1. SALVAGUARDA DE ACTIVOS
Los activos de los SI incluyen: hardware, software, facilidades, personas (conocimientos), archivos de datos, documentación de sistemas, insumos…

2. INTEGRIDAD DE LOS DATOS
Es un estado que en el cual los datos poseen ciertos atributos:
- ➔ completitud
- ➔ consistencia
- ➔ veracidad
- ➔ correctitud

Si la integridad de los datos de una organización no es mantenida, no posee representación de sí misma o de los eventos. Sin integridad de datos se pueden producir pérdidas de ventajas competitivas.
El valor de un dato depende de:
1) el valor del contenido informacional de un ítem de dato para los tomadores de decisiones [El contenido informacional de un ítem de dato se refiere a cuánto puede aportar el dato para modificar el nivel de incertidumbre que envuelve a una decisión]
2) el grado en el cuál el ítem de dato es compartido entre los tomadores de decisiones
3) el valor del ítem de dato para los competidores

3. EFECTIVIDAD DE LOS SISTEMAS
Un sistema de información es efectivo si satisface sus objetivos.
Formas de evaluar la efectividad de los sistemas:
1) durante el proceso de desarrollo para garantizar que se satisfacen los requerimientos de los usuarios
2) mediante una post-auditoría
Para poder evaluar la efectividad de un sistema de información se deben conocer:
1) las características de los usuarios,
2) el entorno de toma de decisiones .

4. EFICIENCIA DE LOS SISTEMAS
Un SI es eficiente si usa los recursos mínimos para satisfacer sus objetivos. Recursos de un sistema de información:
• tiempo de procesador
• periféricos
• software
• trabajo manual
Muchas veces el uso de los recursos no se puede estudiar con respecto a un sólo sistema. Generalmente, la eficiencia se estudia cuando se agotan los recursos.

Los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un sistema de control interno.

7. ¿Qué significa que la alta gerencia implemente un sistema de control interno? ¿Cómo se lleva a cabo?

Los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un sistema de control interno.

1) SEPARACIÓN DE OBLIGACIONES
En un sistema manual, personas diferentes deben realizar las tareas de iniciar la transacción, registrar la transacción, y prevenir errores o detectar irregularidades
En un sistema automatizado, es el mismo programa el que realiza todas las funciones.
En los sistemas automatizados, la separación de obligaciones se aplica distinto: se tiene que separar la capacidad de ejecutar el programa, de la capacidad de modificar el programa.

2) DELEGACIÓN
Una delegación clara de autoridad y responsabilidad es esencial tanto en sistemas manuales como automatizados.
En un sistema automatizado, hacer esto de una manera no ambigua puede ser dificultoso.

3) PERSONAL COMPETENTE Y CONFIABLE
A las personas responsables de desarrollar, implementar y operar los sistemas de información se les delega mucho poder. El personal responsable de los sistemas automatizados tiene delegado mayor poder que los empleados que realizan tareas manuales.

No es fácil para las organizaciones asegurar que el personal de sistemas sea competente y confiable.
La alta rotación de este personal es común.
La gerencia tiene poco tiempo para evaluar a este personal.
El rápido desarrollo de la tecnología inhibe a la gerencia de evaluar el perfil de este personal.

4) SISTEMA DE AUTORIZACIONES
La gerencia debe establecer dos tipos de autorizaciones:
1) autorizaciones generales: establecen las políticas que la organización debe seguir.
2) autorizaciones específicas: aplicables a transacciones individuales.
En los sistemas automatizados las autorizaciones están embebidas dentro de los programas.
Los auditores deben controlar las autorizaciones definidas en los procedimientos, como así también la veracidad del procesamiento de los programas.

5) DOCUMENTOS Y REGISTROS
Se debe asegurar que los documentos y registros sean adecuados.
En un sistema automatizado no es necesario un documento para iniciar una transacción.

En un sistema bien diseñado debería haber mayores registros de auditoría que en un sistema manual
Se deben prever controles de acceso y facilidades de acceso (login) para asegurar que los rastros de auditoría sean exactos y completos.

6) CONTROL DE ACCESO FÍSICO
El control de acceso físico a los activos y a los registros es crucial, tanto en sistemas manuales como automáticos. Diferencia:
• sistema manual: puede tener que acceder a varios sitios
• sistema automatizado: todos los registros necesarios se pueden mantener en un sólo lugar.
La concentración de información aumenta la posibilidad de pérdida que puede surgir por abuso o desastre.

SUPERVISIÓN GERENCIAL ADECUADA
En sistemas manuales se facilita, ya que empleados y supervisores, generalmente, comparten el lugar físico.
En sistemas automatizados, las comunicaciones permiten que los empleados estén cerca de los clientes.
La supervisión se debe llevar a cabo en forma remota.
Los controles para supervisión deben estar construidos dentro del sistema.
El gerente debe acceder a los registros de auditoría para evaluar la gestión de los empleados
.
7) CHEQUEOS DE PERFORMANCE
En sistemas manuales, los chequeos realizados por otra persona ayudan a detectar errores o irregularidades.
En sistemas automatizados, los programas siempre ejecutan el mismo algoritmo, a excepción de una falla de hardware o de software.
Los auditores deben evaluar los controles establecidos para desarrollar, modificar, operar y mantener programas.

8) COMPARACIÓN PERIÓDICA
Periódicamente, se deben controlar los datos que representan los activos con los activos reales, a fin de determinar falta de completitud o inexactitud de los datos.
En sistemas automatizados se deben preparar programas para que hagan esto.
Son importantes la implementación de estos controles durante el desarrollo de sistemas.
El uso de computadoras afecta de varias maneras la implementación de los componentes de un sistema de control interno.

Sistema de control interno

Podríamos definir el concepto genérico de control como una acción potencial orientada a alcanzar un objetivo definido. Si nos centramos en el control interno puntualizamos que se trata de un proceso llevado a cabo por los directivos de una organización, concebido para garantizar una seguridad suficiente, orientado a alcanzar los objetivos en distintos aspectos: que se lleven a cabo las operaciones de forma eficiente y efectiva, que la información financiera sea fiable y que se cumplan las normativas oportunas.

Fases para implementar el sistema de control interno
Existen una serie de fases que han de seguirse secuencialmente para garantizar una correcta implementación del control interno. Son las siguientes:

Fase 1: Crear una cultura del control mediante la comunicación, la motivación y la capacitación
Fase 2: Recabar información
Fase 3: Clasificar la información obtenida
Fase 4: Diagnosticar
Fase 5: Revisar los procedimientos
Fase 6: Evaluar el control interno y de gestión
Fase 7: Implementar, hacer seguimiento y ajustar
Fase 8: Evaluar indicadores y realizar más ajustes

Parte II: Controles y riesgos de Auditoría

8. Explique por qué un control en un sistema de información es un sistema.

Definición.
Un control es un sistema que previene, detecta, o corrige eventos ilegales.
Hay tres aspectos claves en esta definición:
1) un control es un sistema
2) eventos ilegales
3) los controles son usados para prevenir, detectar o corregir eventos ilegales.

Un control no es una sentencia if en un algoritmo

Un control es un sistema -> Habitualmente tendemos a nombrar los controles, teniendo en cuenta sólo un aspecto del control.
Una password se convierte en control, solo en el contexto de un sistema que asegure:
1) Seguridad para elegir password
2) Correcta validación de password
3) Almacenamiento seguro de las password
4) Seguimiento en el uso indebido de passwords
5) …

Un control es un sistema que utiliza compilaciones de datos para determinar si se cumplen los objetivos. Si los resultados son ineficientes o muestran algún problema basado en los planes iniciales, se pueden hacer ajustes al proceso de organización para garantizar que los recursos se utilicen de la manera más eficaz. Los datos para el proceso de control pueden ser entregados en los Estados financieros de la compañía, informes de trabajo, sistemas de denuncia internos y externos o agencias reguladoras.

9. Explique las diferencias entre un control preventivo, control detectivo, y control correctivo. Provea ejemplos para cada tipo de control.

TIPOS DE CONTROLES
Control Preventivo: instrucciones de cómo completar un formulario. Nota: las instrucciones no son el control.
Control Detectivo: un programa que valida datos de input, rechazando los erróneos.
Control Correctivo: un programa que detecta el ruido en comunicaciones y permite corregir datos corruptos.
Reducir las pérdidas esperadas por eventos ilegales mediante:
1) controles preventivos: reducen la probabilidad que estos eventos ocurran.
2) controles detectivos y correctivos: reducen la cantidad de pérdidas cuando los eventos ilegales ocurren.

10. ¿Cuál es la tarea del auditor en cuanto a los controles?

La tarea del auditor es determinar si los controles están ubicados y funcionan para prevenir los eventos ilegales.

11. Explique desde el punto de vista de auditoría de sistemas de información el concepto de "factorizar en subsistemas" y qué criterio(s) se aplica(n) para factorizar un sistema en subsistemas.

Para administrar la complejidad, se sugiere:
1) factorizar el sistema en subsistemas
2) determinar la confiabilidad de cada subsistema, y las implicancias de cada uno de ellos en el nivel de confiabilidad general del sistema.

FACTORIZACIÓN
El primer paso para comprender un sistema complejo es particionarlo en subsistemas.
Un subsistema es un componente de un sistema que:
1) realiza ciertas funciones básicas necesarias para el sistema en general,
2) le permite atender sus objetivos fundamentales.
Los subsistemas son componentes lógicas y no físicas.
El proceso de particionar en subsistemas se denomina factorización.

CÓMO FACTORIZAR
Para poder factorizar, se necesita un criterio.
Criterio: La esencia de un subsistema es la función que realiza.
Los auditores deben identificar primero, las principales funciones que el sistema realiza para cumplir sus objetivos.
El proceso de factorización termina cuando se ha particionado el sistema en partes lo suficientemente pequeñas, de tal modo que puedan ser entendidas y evaluadas.

Un control es un sistema que previene, detecta y corrige eventos ilegales.
Para realizar una auditoría se debe factorizar en subsistemas:

1) funciones gerenciales
2) funciones de aplicación

1) funciones gerenciales - las funciones que se deben realizar para asegurar que el desarrollo, la implementación, operación y mantenimiento de los sistemas de información proceden de una forma planificada y controlada.
2) funciones de aplicación - tareas que son necesarias ejecutar para realizar un procesamiento de información confiable. Relacionado con “ciclos”.

Se debe evaluar la confiabilidad de los controles en cada subsistema.

12. Indique qué otros criterios de factorización existen.

OTRO CRITERIO DE FACTORIZACIÓN
Otro criterio para factorizar es considerar subsistemas que presenten mínimo acoplamiento y máxima cohesión.

ACOPLAMIENTO: Cada subsistema debería ser relativamente independiente de otros subsistemas. Sistemas con poco acoplamiento son más fáciles de comprender.
COHESIÓN: Cada subsistema debe ser internamente cohesivo. Todas las actividades realizadas por el sistema apuntan a cumplir la función principal del subsistema.

13. ¿De qué manera se mide la confiabilidad de los controles?

CONFIABILIDAD DE CONTROLES
Para evaluar la confiabilidad de los controles:
1) se deben identificar todos los posibles tipos de eventos que pueden ocurrir en el subsistema.
2) se deben considerar todos los eventos válidos o ilegales.

Para identificar los eventos, hay que considerar las principales funciones que realiza el subsistema.

-> CONSIDERAR LAS PRINCIPALES FUNCIONES
Para cada función:
1) analizar cómo debería realizarse
2) evaluar cómo el subsistema cumple con esa visión normativa.

Para determinar si un evento es legal o ilegal se deben considerar las transacciones que pueden ocurrir como input al subsistema.
Todos los eventos en un sistema de aplicación deben surgir de una transacción.

CONFIABILIDAD DE LOS CONTROLES
Los auditores deben recolectar evidencias sobre la existencia y confiabilidad de los controles, para determinar si las pérdidas por los eventos ilegales se reducen a niveles aceptables.

Para cada evento ilegal, se debe considerar:
1) cómo los controles cubren a ese tipo de evento,
2) cuánto de confiable son los controles,
3) si puede ocurrir un error material o una irregularidad.

Se publican listas que ayudan a realizar esta tarea.
Estas listas muestran por ejemplo:
1) las caídas en los sistemas de información,
2) errores e irregularidades que ocurren en diferentes tipos de transacciones.
Las listas muestran los controles que se pueden realizar para reducir las pérdidas esperadas por errores o irregularidades.

Ejemplo de la tabla (transparencia Auditoria - Clase 2 - 31)

Controles/Errores-irregularidades	Cantidad incorrecta	Precio incorrecto
Operador bien entrenado	M	M
Revisión gerencial de ventas	B	M

Efectividad del Control: A: Alta; M: Media; B: Baja

Para estimar la confiabilidad: En cualquier nivel de la estructura, los pasos de evaluación son:

1. Identificar las transacciones que ingresan al sistema
2. Considerar los eventos legales e ilegales que puedan ocurrir
3. Asegurar la confiabilidad de los controles que detectan los eventos ilegales.

Detectar nuevos controles -> A medida que se evalúan los sistemas de mas alto nivel, se pueden encontrar nuevos controles

14. Identifique cuatro tipos de riesgos. Explique la naturaleza de cada uno de ellos.

Def: El riesgo de auditoría es el riesgo de que un auditor fracase al detectar las pérdidas materiales reales, o potenciales, o los registros incorrectos.

- RDA: Riesgo deseado de Auditoría
- RI: Riesgo inherente
- RC: Riesgo de control
- RD: Riesgo de detección

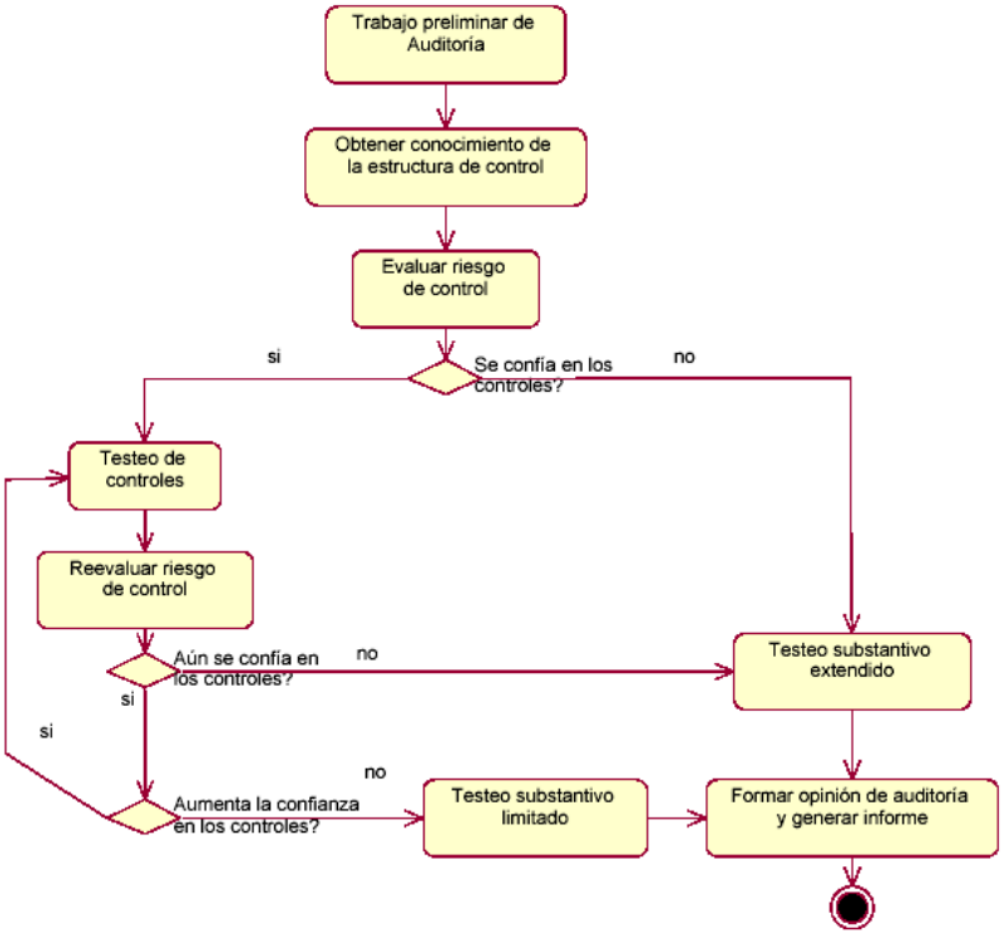
RDA = RI * RC * RD

TIPO DE RIESGOS
1) Riesgo Deseado: el riesgo que se desea correr. Se calcula evaluando las consecuencias de fracasar en detectar las pérdidas materiales reales o potenciales.
2) Riesgo Inherente: refleja la probabilidad que una pérdida material o una imputación errónea exista en algún segmento de la auditoría, antes de que sea considerada la confiabilidad de los controles internos.Los auditores consideran factores generales tales como la naturaleza de la organización, la industria en la que opera, las características del gerenciamiento, intereses contables y de auditoría, etc.

3) Riesgo de Control: refleja la probabilidad que en algún segmento de la auditoría, los controles internos no prevengan, detecten o corrijan pérdidas materiales o imputaciones erróneas que puedan surgir. Para evaluar el nivel de RC asociado con cada segmento de la auditoría, se debe considerar la confiabilidad de los controles gerenciales y de aplicación.
4) Riesgo de Detección: refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas. Se calcula el nivel de RD que se debe lograr para cumplir con el RDA.

Parte III: Proceso de Auditoría

15. Explique brevemente el proceso de auditoría.



(Aca creo que iría una explicación de ese diagrama)

ETAPAS
1- Recopilación de información básica
2- Identificación de riesgos potenciales
3- Objetivos de control
4- Determinación de los procedimientos de control
5- Pruebas a realizar
6- Obtención de los resultados

7- Conclusiones y comentario
8- Redacción y presentación del borrador del informe al responsable del área de informática
9- Redacción del informe, resumen y conclusiones y entrega a los directivos

Etapas componentes del proceso de auditoría

La labor de auditoría comparte una serie de pasos estandarizados en la mayoría de ocasiones, resumidos en los siguientes puntos:

1. Planificación previa: Abarca desde reuniones previas con los profesionales gestores de la organización a auditar hasta la obtención de estudios e inventarios sobre la misma. Por ejemplo, medios logísticos, análisis DAFO(El análisis FODA, también conocido como análisis DAFO, es una herramienta de estudio de la situación de una empresa, institución, proyecto o persona, analizando sus características internas y su situación externa en una matriz cuadrada) previos, conocimiento del sector en que opera, entre otros. Al mismo tiempo, se establece un calendario que delimite los plazos para la auditoría y cada etapa.
2. Realización de labores de investigación y observación: En un clima de constante comunicación y colaboración con el ente auditado, el auditor realiza comprobación de documentación, de ratios productivos y la evolución de la empresa o institución dentro de su actividad habitual.
3. Verificación y contraste de datos obtenidos: Un profesional auditor debe adecuar el funcionamiento observado al marco normativo en que se encuentre la organización. De existir puntos discordantes, debe señalizarlos y sugerir formalmente soluciones para su desaparición y asegurar un correcto funcionamiento en base a la ley.
4. Publicación de conclusiones y actuaciones a tener en cuenta por medio de un informe de auditoría: Más allá de dar validez legal al funcionamiento organizativo, un informe final debe destacar puntos positivos y negativos. Esta información debe ser útil y válida para la empresa frente a terceros.

Planificación
Para que la auditoría sea exitosa es primordial elaborar un plan de ejecución en el cual se presentan, entre otros, los siguientes puntos:
- Propósito de la auditoría
- El alcance
- Actividades a desarrollarse
- Asignación del equipo auditor
- Cronograma y tiempos de ejecución establecidos
- Detalles de los procedimientos
- Detalle de los departamentos, procesos o las empresas que serán auditadas.
- Personas que serán entrevistadas y sus agendamientos correspondientes

Preparación
En esta etapa el auditor líder asigna funciones y prepara la lista de chequeo de todos los procesos que tienen que ser verificados. Por medio de esta lista de chequeo los auditores tienen una hoja de ruta que les permite evaluar y registrar todo lo que sea necesario para

obtener información de calidad. Obtén la lista de chequeo ISO 9001:2015 para auditar la fase de planificación

Ejecución
Durante esta fase se desarrolla toda la auditoría siguiendo los procedimientos, políticas y estándares establecidos en la etapa de planificación. Se colecta toda la información, la evidencia, los testimonios y se realiza un informe con todos los hallazgos encontrados para sacar conclusiones y poder presentar los resultados finales. Lee también: Una norma mamá ISO 19011:2018 directrices para auditorías

Finalización y seguimiento
Luego de concluido el procedimiento, los auditores revisan los problemas encontrados y plantean las recomendaciones a seguir para corregir estos inconvenientes. Con los resultados de la auditoría se establece un plan de seguimiento que tenga la posibilidad de verificar que se estén cumpliendo las recomendaciones de mejora en el tiempo.

16. Enuncie cinco tipos de procedimientos de auditoría que pueden ser usados para recolectar evidencia en una auditoría.

PROCEDIMIENTOS DE UNA AUDITORÍA
Existen diferentes procedimientos de auditoría, dependiendo de lo que se desee controlar:
1) determinar si ocurrieron pérdidas materiales o la información financiera es errónea
A fin de recolectar evidencia, se usan los siguientes procedimientos:
1.1) procedimientos para comprender los controles
1.2) testeo de controles
1.3) testeos substantivos de detalle de transacciones
1.4) testeos substantivos de detalle de balances contables
1.5) procedimientos de revisión analítica

2) determinar la eficiencia y eficacia de las operaciones
Para determinar esto, se utilizan procedimientos similares:
2.1) procedimientos para comprender los controles
2.2) testeo de controles
2.3) testeos sustantivos de detalle de transacciones.
2.4) testeos sustantivos de resultados generales - la noción de balances contables no es aplicable en este caso. Ejemplo: testeos de performance.
2.5) procedimientos de revisión analítica. Ejemplo: modelos de simulación.

PROCEDIMIENTOS PARA COMPRENDER LOS CONTROLES
Los procedimientos incluyen cuestionarios, inspecciones, observaciones
Para determinar si los controles existen, analizar cómo están diseñados, sí funcionan.

PROCEDIMIENTOS DE REVISIÓN ANALÍTICA
Los procedimientos de revisión analítica se focalizan en las relaciones entre los ítems de datos. El objetivo es identificar áreas que requieran un trabajo de auditoría posterior.
Ejemplo: medir ingresos por ventas durante un período.

17. Enumere tres tipos de testeos que se pueden realizar durante una auditoría.

1.2) testeo de controles
TESTEO DE CONTROLES
Son para evaluar si los controles están actuando efectivamente. Ejemplos: cuestionarios, inspecciones, observaciones, reprocesos.

1.3) testeos substantivos de detalle de transacciones
Los testeos substantivos de detalle de transacciones están diseñados para detectar:
1) errores monetarios o
2) irregularidades
en transacciones que afectan los estados financieros. Ejemplo: controlar la facturación

1.4) testeos substantivos de detalle de balances contables
Los tests substantivos de detalle de balances contables se focalizan en los registros contables finales, en el balance. Ejemplo: se puede circularizar a una muestra de clientes para controlar que los saldos registrados sean correctos.

2.4) testeos substantivos de resultados generales
La noción de balances contables no es aplicable en este caso. Ejemplo: testeos de performance.
Se realizan con el fin de obtener evidencia suficiente para realizar un juicio final sobre el grado de pérdidas que podrían ocurrir cuando el sistema falla en: salvaguardar activos, mantener la integridad de los datos y lograr efectividad y eficiencia.
En general, este tipo de testeos, son los más caros de las auditorías.

18. ¿Cómo se lleva a cabo la planificación de una auditoría? Cite diferencias entre auditoría interna y externa.

PLANIFICACIÓN DE UNA AUDITORÍA
La primera etapa es la planificación.
Las tareas que se realizan en la etapa de planificación varían dependiendo si es una:

a) auditoría interna
La etapa de planificación incluye:
1) asignar personal adecuado a las auditorías
2) obtener información del cliente
3) realizar procedimientos de revisión analíticos para comprender el negocio del cliente
4) identificar áreas de riesgo
Los auditores internos se preocupan por el tamaño de las pérdidas que pudiera haber por operaciones ineficientes o ineficaces.

b) auditoría externa
La etapa de planificación incluye:
1) investigar nuevos clientes

2) asignar personal adecuado a las auditorías
3) obtener el contrato
4) obtener información del cliente
5) realizar procedimientos de revisión analíticos para comprender el negocio del cliente
6) identificar áreas de riesgo

Los auditores externos se preocupan por el tamaño de los errores en los estados financieros.

TAREAS DE PLANIFICACIÓN
1) determinar el alcance de la auditoría,
2) emitir una opinión sobre el RDA,
3) emitir una opinión sobre el RI,
4) emitir una opinión sobre el RC,
5) calcular el RD que se debe lograr para cumplir con el RDA,
6) recolectar evidencia
7) documentar evidencia

19. Describa el contenido de un informe de auditoría.

Un informe típico debería incluir:
1) una introducción que describa los objetivos de la auditoría,
2) el enfoque general utilizado,
3) un resumen de las conclusiones críticas,
4) recomendaciones para abordar las conclusiones críticas,
5) datos que respalden las conclusiones críticas.

20. Describa los cuatro tipos de opinión que un auditor puede emitir.

OPINIONES DE AUDITORÍA
Los estándares en varios países requieren que la opinión sea:
1) opinión excusada: en base al trabajo realizado no se puede emitir opinión.
2) opinión adversa: se concluye que han ocurrido pérdidas materiales o que los estados financieros están distorsionados.
3) opinión con calificación: se concluye que han ocurrido pérdidas materiales o existen registros incorrectos, pero las cantidades no son considerables.
4) opinión sin calificación: el auditor considera que no han ocurrido pérdidas materiales o no existen registros incorrectos.

Parte IV: Gobernanza de TI

21. Explique el significado del concepto “Gobernanza de TI”.

La Gobernanza de TI es un subconjunto de Gobierno Corporativo de las organizaciones que se centra en los sistemas de TI, su desempeño y los riesgos asociados.

GOBERNANZA DE TI

- trata con la relación entre el enfoque empresarial y la gestión de TI
- destaca la importancia de las cuestiones de TI
- promueve que las decisiones estratégicas de TI deben ser tomadas por una junta directiva corporativa

METAS

- asegurar que las inversiones en TI generen valor
- mitigar riesgos asociados con TI

GOBERNANZA DE TI se trata de quién toma las decisiones de TI

- quién tiene autoridad para tomar las decisiones importantes
- quién tiene información para tomar las decisiones importantes
- quién es responsable por implementar las decisiones importantes

22. Explique qué es COBIT y cuáles son sus elementos.

OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT)
Enfoque para estandarizar buenas prácticas de TI y control. Provee herramientas para acceder y medir el desempeño de los procesos de gobernanza y administración de TI de una organización. Desarrollado y mantenido por el Instituto de Gobernanza de TI
COBIT es un conjunto de recursos que contienen toda la información que las organizaciones necesitan para adoptar un marco de gobernanza y control de TI.
COBIT 5 consolida COBIT 4.1, Val IT y Risk IT en un marco y se ha actualizado para alinearse con las mejores prácticas actuales, por ejemplo ITIL V3 2011, TOGAF (El Marco de Arquitectura de Grupo Abierto).

ELEMENTOS
1 Procesos de TI y Dominios
2 Objetivos de Control
3 Prácticas de Control
4 Guías de Auditoría
5 Guías de Administración

23. Explique la diferencia entre Gobernanza y Administración de TI.

ADMINISTRACIÓN DE TI se trata de tomar e implementar decisiones de TI
GOBERNANZA DE TI se trata de quién toma las decisiones de TI

- quién tiene autoridad para tomar las decisiones importantes
- quién tiene información para tomar las decisiones importantes
- quién es responsable por implementar las decisiones importantes

GOBERNANZA asegura:

- que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar objetivos empresariales a alcanzar equilibrados y acordados
- establecer la dirección a través de la priorización y la toma de decisiones
- supervisando el desempeño y cumplimiento contra la dirección y objetivos acordados

ADMINISTRACIÓN
planifica, construye, ejecuta y monitorea las actividades en consonancia con la dirección establecida por el cuerpo de gobierno para alcanzar los objetivos empresariales

24. ¿Cuáles son los principios de COBIT?

Principios
1) Satisfacer las necesidades de las partes interesadas:
Garantizar que las empresas aporten valor a sus partes interesadas mediante la obtención de beneficios, la optimización del uso de los recursos y la gestión de riesgos.

2) Cubrir la empresa de extremo a extremo:
Tener en cuenta todos los sistemas de gobernanza y administración relacionados con TI para que sean integrales y de extremo a extremo –incluyendo tanto sistemas internos como externos.

3) Aplicar un marco integrado:
Alinearse con otros estándares y buenas prácticas relacionadas con TI, sirviendo de marco general para la gobernanza y administración de TI empresarial.

4) Habilitar un enfoque holístico:
Tener en cuenta los elementos que interactúan, especificar un conjunto de habilitadores para definir un sistema integral de gobernanza y administración de TI empresarial.

5) Separar las funciones principales:
Establecer una distinción clara entre las funciones de gobernanza y administración.

25. Indique de qué forma organiza COBIT los procesos de TI.

COBIT 5.0 divide los procesos en 2 dominios:
1)GOBERNANZA –incluye 5 procesos, dentro de cada uno de ellos se definen prácticas de Evaluar, Dirigir y Monitorear.
2)ADMINISTRACIÓN –incluye 32 procesos clasificados en 4 dominios –APO, BAI, DSS y MEA.

26. Explique cómo COBIT clasifica la administración de TI.

COBIT clasifica la Administración de TI en 4 dominios:

Alinear, Planear y Organizar (APO)proporciona direcciones a la entrega de soluciones y servicios.
Construir, Adquirir e Implementar (BAI)provee soluciones a DSS para la entrega de servicios.
Entrega, Servicio y Soporte (DSS)recibe soluciones y las hace utilizables para los usuarios finales.
Monitorear y Evaluar (MEA)monitorea todos los procesos para asegurar que se siga la dirección provista.

27. Justifique la importancia de aplicar COBIT en una organización.

- permite a los administradores públicos cerrar la brecha entre los requisitos de control, los problemas técnicos y lo s riesgos comerciales
- permite un desarrollo claro de políticas y buenas prácticas para el control de TI en todas las organizaciones gubernamentales
- enfatiza el cumplimiento regulatorio
- ayuda a las organizaciones del sector público a aumentar el valor obtenido de TI
- permite la alineación y simplifica la implementación de la gobernanza de TI en el sector público
- ayuda a los gobiernos a proporcionar servicios mejores y más personalizados a los ciudadanos y las empresas
- optimiza las inversiones en TI, garantiza una prestación de servicios efectiva y proporciona medidas