Practica 2 - Auditoria y peritaje de sistemas [Resolución]

Parte I - Conceptos generales

La necesidad de auditar

Es necesario auditar para prevenir las siguientes situaciones

- Costos por perdidas de datos. La preservación de los datos, su protección, representan una imagen de la empresa, su confiabilidad. La perdida de datos tales como cuentas corrientes, datos de alumnos generan que la entidad poseedora de esos datos pierda credibilidad.
- Costos por toma de decisiones incorrectas. La calidad de una decisión esta íntimamente relacionada con la calidad de los datos que se tienen y de las reglas de decisión. Datos inexactos concluirán en decisiones inexactas. Dependiendo del nivel jerárquico, los errores son mas o menos aceptables. Esto esta relacionado a que las altas gerencias manejan datos mas generales y son tolerantes a ciertos fallos, mientras que las gerencias medias y operacionales necesitan de datos mas detallados y son menos tolerantes a fallos. Las decisiones se toman para detectar, investigar y corregir procesos fuera de control. Las reglas de decisión serán mas o menos exactas en base al tipo de decisiones hechas por personas que tienen algún interés en la organización.
- Costos por abusos computacionales. Un abuso computacional es un incidente asociado con tecnología informática, en el cual una víctima sufre o podría haber sufrido perdida, y un perpetrador con intención logra o podría lograr una ganancia, mediante hacking, uso de virus, acceso físico ilegal o mediante abuso de privilegios.
- Costos por errores de computación. Los costes son variados, pero pueden ir desde daños menores, pasando por daños ambientales, perdida de libertad hasta la perdida de la vida humana.
- Valor del hardware y el personal. Se tiene que tener en cuenta el valor de los datos que se tienen, que sucedería si estuviera en las manos equivocadas. O si un componente critico no funciona. Si el software es destruido o si un profesional calificado deja la empresa
- Evolución controlada de TI. Las nuevas tecnologías deben ser evaluadas en cuanto a confiabilidad, su implementación y el efecto que esta tiene en los usuarios.
- Mantenimiento y privacidad. Tener en cuenta que los sistemas almacenan mucha información de cada individuo, se debe buscar la privacidad y protección de cada uno de esos datos.

Para evitarlos, se realiza lo que se conoce como auditoria de sistemas de información, que es un proceso en el cual se recolectan pruebas y se evalúa la evidencia.Al prevenirse, se pueden lograr los siguientes objetivos

- Preservar activos
- Mantener la integridad de los datos
- Alcanzar con eficacia los objetivos organizacionales
- Usar los recursos eficientemente
- Cumplir con determinadas regulaciones, reglas y condiciones

Para que los objetivos anteriores puedan cumplirse, se debe crear un sistema de control interno. El mismo se compone de

- Separación de obligaciones,
- Delegación clara de autoridad y responsabilidades,
- Reclutamiento y entrenamiento de personal calificado,
- Sistema de autorizaciones,
- Documentos y registros adecuados,
- Control físico y documentación sobre los activos,
- Chequeos independientes de performance,
- Comparación periódica de activos con registros contabilizados

Parte II - Controles y riesgos de Auditoria

Controles

Un control es un sistema que previene, detecta, o corrige eventos ilegales. Un elemento se convierte en control, solo en el contexto de un sistema. Los controles pueden ser

Preventivos. En donde se toman medidas para evitar que los eventos ilegales ocurran.
Detectivos. En donde se examinan los eventos
Correctivos. En donde se reparan los errores ya cometidos.

En una auditoria, el auditor debe determinar si los controles están ubicados y funcionan para prevenir los eventos ilegales. En general estos controles están dispersos en un vasto sistema, pero responden a un subsistema mas pequeño. Para poder manejar el nivel de complejidad, se divide al gran sistema en subsistemas pequeños. Esto permite al auditor, focalizarse en los aspectos de interés a evaluar en cada subsistema, intentado determinar el nivel de confiabilidad. La división esta basada en el criterio de que cada subsistema solo realiza una serie de funciones básicas. Luego se presenta un enfoque acoplado en donde existe una fuerte relación entre los subsistemas, siendo mas fácil de comprender. Y por otro lado, la factorizacion cohesiva busca que cada sistema también lo sea.

Confiabilidad de controles

Para evaluar la confiabilidad de los controles se deben identificar todos los posibles tipos de eventos que pueden ocurrir en el subsistema. Se deben considerar rodos los eventos validos e ilegales. Los auditores deben recolectar evidencias sobre la existencia y confiabilidad de los controles para determinar si las perdidas por los eventos ilegales se reducen a niveles aceptables. Para eso se debe considerar ante un evento ilegal, como es cubierto mediante controles, cuan confiables son y si el error puede incurrir un error material o una irregularidad. Se puede realizar una tabla de doble entrada en donde en la columna se ponen los errores y en la fila los controles.

Estimación de la confiabilidad de los controles

La estimación parte de un análisis de subsistemas menores a subsistemas mayores, ya que los menores son componentes de un subsistema mayor. Una vez analizados los de menor nivel, se puede analizar el impacto, la naturaleza y la frecuencia de eventos ilegales en un sistema de mayor nivel. Para esto es necesario

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

Riesgos en una auditoria

El riesgo de auditoria es el riesgo de que un auditor fracase al detectar las perdidas materiales reales o potenciales, o los registros incorrectos

RDA = RI * RC * RD

RDA: Es el riesgo deseado, el riesgo que se desea correr. Se evalúan las consecuencias de fracasar en detectar las perdidas materiales reales o potenciales.
RI: Es el riesgo inherente. Refleja la posibilidad de que una perdida material o una imputación errónea exista en algún segmento de la auditoria, antes de que sea considerada la confiabilidad de los controles internos. La naturaleza de la organización, la industria en la que opera, las características del gerenciamiento y los intereses contables y de auditoria son factores considerados
RC: Es el riesgo de control. Refleja la probabilidad que algún segmento de la auditoria, los controles internos no prevengan, detecten o corrijan perdidas materiales o imputaciones erróneas que puedan surgir.
RD: Es el riesgo de detección. Refleja la probabilidad que los procedimientos de auditoria utilizados en algún segmento, fallen en detectar perdidas materiales o imputaciones erróneas

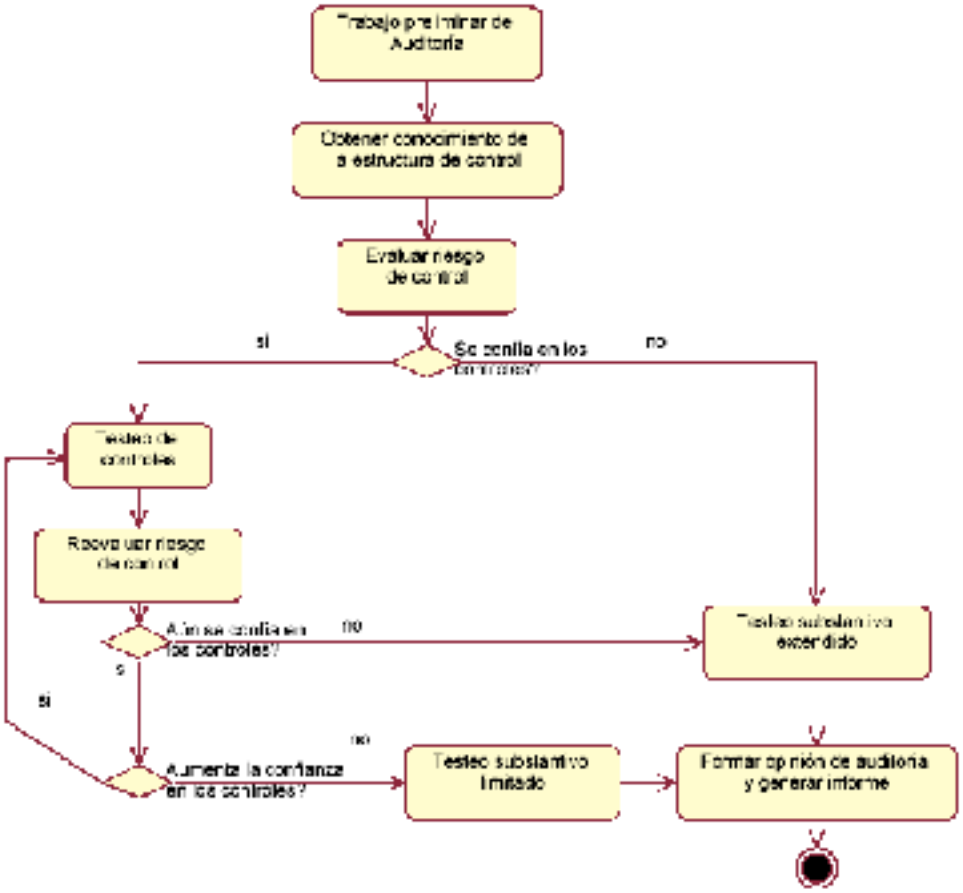
Auditoria por perdida o información errónea

- A - Procedimientos para comprender los controles
  - Mediante cuestionarios, inspecciones u observaciones
  - Se busca determinar si los controles existen, su diseño y si funcionan
- B - Testeo de controles
  - Mediante cuestionarios, inspecciones, observaciones, reprocesos
  - Se evalúa si los controles están actuando efectivamente.
- C - Testeos substantivos de detalle de transacciones
  - Se intenta detectar errores monetarios o irregularidades en transacciones que afectan los estados financieros.
- D - Testeos substantivos de detalle de balances contables. Se focaliza el test en los registros contables finales. Se necesita demostrar que los saldos registrados son los correctos.
- E - Procedimientos de revisión analítica. Se analizan las relaciones entre los datos. El objetivo es identificar áreas que requieran un posterior trabajo de auditoria.

El orden de estos pasos varia, dependiendo de que finalidad se busca

Para determinar eficacia y eficiencia: A - B - C - D - E
Para determinar confiabilidad: D - C - B - A - E

Pasos de una auditoria



Planificación de una auditoria interna

Los auditores internos se preocupan por el tamaño de las perdidas que pudiera haber por operaciones ineficientes o ineficaces.

- [ ] Asignar personal adecuado a las auditorías
- [ ] Obtener información del cliente
- [ ] Realizar procedimientos de revisión analíticos para comprender el negocio del cliente
- [ ] Identificar áreas de riesgo

Planificación de una auditoria externa

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

- [ ] Investigar nuevos clientes
- [ ] Asignar personal adecuado a las auditorías
- [ ] Obtener el contrato
- [ ] Obtener información del cliente
- [ ] Realizar procedimientos de revisión analíticos para comprender el negocio del cliente
- [ ] Identificar áreas de riesgo

Tareas de planificación

- Determinar el alcance de la auditoría, se determina que se va a auditar: un sistema, un conjunto de sistemas o un area de tecnología informática
- Emitir una opinión sobre el RDA
- Emitir una opinión sobre el RI del segmento que se va auditar. Si se trata de un sistema que maneja efectivo o una tecnología compleja
- Emitir una opinión sobre el RC, que es compleja de arribar. Se tiene en consideración aspectos como controles de entorno, evaluación de riesgo, actividades de control, información y comunicación y monitoreo.
    - Si RC < nivel máximo -> se identifican los controles y se testean
    - Si RC = nivel máximo -> No se testean los controles, ya que se los considera poco efectivos. Se debería realizar un testeo amplio.
- Calcular el RD que se debe lograr para cumplir con el RDA,
- Recolectar evidencia, mediante la revisión de papeles de trabajo de auditorias previas, entrevistas con el personal, observación de como se desarrollan las actividades, revisión de documentación de sistemas.
- Documentar evidencia

Al detectarse que los controles son débiles, el auditor tomara una determinada actitud dependiendo de si es interno (expandirá las investigaciones, para lograr una mejor comprensión) o externo (reducirá las investigaciones, para realizar testeos mas amplios)

Al finalizar la auditoria, el auditor tendrá una opinión que puede ser
Excusada. No puede emitir opinión
Adversa. Evidencia que hay perdidas materiales o estados financieros distorsionados.
Opinión con calificación. Se concluye que hay perdidas materiales no significativas
Opinión sin calificación. El autor considera que no han ocurrido perdidas materiales o no existen registros incorrectos.

Gobernanza de IT

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

- Trata con la relación entre el enfoque empresarial y la gestión de TI
- Destaca la importancia de las cuestionesde 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

La diferencia entre administración de TI y gobernanza de TI radica en que la administración trata de la toma e implementación de decisiones de TI mientras que la gobernanza trata de quien toma las decisiones (quien tiene la autoridad, responsabilidad e información para hacerlo)

COBIT

OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT) es un conjunto de recursos que contienen toda la información que las organizaciones necesitan para adopterun marco de gobernanza y control de TI.
Fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, www.isaca.org) y el Instituto de Gobernanza de TI en 1992.
COBIT 5 consolida COBIT 4.1, Val IT y RiskIT 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).

- Incorpora los principales estándares internacionales
- Está centrado en los negocios, orientado a procesos, controlado y medido
- Opera a un nivel más alto que los estándares de tecnología pura para la administración de sistemas de información
- Puede ser adaptado por organizaciones mundiales comerciales, gubernamentales y profesionales

Principios COBIT

- 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 recursos y la gestión de riesgos.

- 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

- Aplicar un marco integrado. Alinearse con otros estándares y buenas practicas relacionadas con TI, sirviendo de marco general para la gobernanza y administración de TI empresarial.

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

- Establecer una distinción clara entre las funciones de gobernanza y administración.

Organización de procesos según COBIT

Contiene 5 procesos, para cada uno se definen prácticas de evaluar, dirigir y monitorear (EDM).

EDM se interesa en:
- Establecer un marco de gobernanza
- Crear valor para las partes interesadas

- Asegura que los objetivos de la empresa sean alcanzados
- EVALUANDO las necesidades, condiciones y opciones de las partes interesadas,
- Estableciendo DIRECCIÓN mediante la priorización y la toma de decisiones, y
- MONITOREANDO el desempeño, el cumplimiento y el progreso contra la dirección y los objetivos acordados (EDM).

Clasificación de procesos

EDM –PROCESOS DE TI	
EDM1	Asegurar el marco de gobernanza, el establecimiento y el mantenimiento
EDM2	Asegurar la entrega de beneficios
EDM3	Asegurar la optimización de riesgos
EDM4	Asegurar la optimización de recursos
EDM5	Asegurar la transparencia de las partes interesadas

Clasificación de la administración

Alinear, Planear y Organizar (APO)	proporciona direccionesa la entrega de soluciones y servicios
Construir, Adquirir e Implementar (BAI)	provee soluciones a DSS para la entregade servicios
Entrega, Servicioy Soporte (DSS)	recibe soluciones y las hace utilizablespara los usuarios finales
MonitorearyEvaluar (MEA)	monitorea todos los procesos para asegurar que sesiga la dirección provista

Beneficios de la aplicación de COBIT

- Permite a los administradores públicos cerrar la brecha entre los requisitos de control, los problemas técnicos y los 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