**Ingeniería de Software III**

**Práctica 2 – Auditoría y peritaje de sistemas**

**Parte I: Conceptos generales**

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

IMPACTO DE LA AUDITORÍA EN SI:

1. Salvaguardar activos

Los activos de los SI incluyen: hardware, software, facilidades, personas (conocimientos), archivos de datos, documentación de sistemas, insumos

1. Asegurar integridad de los datos

Es un estado que en el cuál 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

1. Asegurar que los sistemas son efectivos

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.

1. Asegurar que los sistemas son eficaces

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 solo sistema.

Generalmente, la eficiencia se estudia cuando se agotan los recursos.

*Para poder cumplir con los objetivos, se debe recolectar evidencia.*

**Las principales razones para controlar y auditar sistemas (son 7):**

* **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. [Everest,1985]. 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.

EJ: pérdida de cuentas corrientes, pérdida de los datos de los alumnos.

* **Costos por toma de 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

Las decisiones para que los datos sean correctos involucran: detección, investigación y corrección de procesos fuera de control.

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.

Una regla de decisión incorrecta puede tener un impacto menor. Ejemplo: cálculo de amortización erróneo en un bien de poco valor.

En otras, el impacto puede ser considerable. ¿Por ejemplo?

* **Costos por abusos computacionales:** 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. Tipos de abusos: hacking, virus, abuso de privilegio, acceso físico ilegal.
  + **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 [Nachenberg, 1997].
  + **Acceso físico ilegal**: Una persona logra un acceso físico no autorizado a facilidades del computador.

Ejemplo: a una sala de cómputos o a una terminal.

Como resultado, pueden causar daño físico al hardware o hacer copias no autorizadas de programas y datos.

* + **Abuso de privilegios:** Una persona usa privilegios, que le han sido asignados, para propósitos no autorizados.

Ejemplo: hacen copias no autorizadas de los datos a los cuales se les otorgó acceso.

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.

¿Qué pasa con las leyes? En muchos países están evolucionando.

* **Costos por errores de computación**: Procesos automatizados que producen pérdida de dinero o incluso pérdida de vida humanas, daño al medio ambiente.

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.

¿Por qué? Los sistemas controlan:

1) monitoreo de pacientes,

2) cirugías,

3) vuelo de misiles,

4) un reactor nuclear.

* **Valor de hardware y software 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?

(Determinar el impacto que alguno de estos valores críticos pueda fallar)

* **Evolución controlada del uso (TI)**: Se argumenta que la confiabilidad de los sistemas computarizados complejos no está garantizada.

Las consecuencias de usar sistemas no confiables pueden ser catastrófica.

¿Qué efectos físicos y mentales tienen las computadoras en los usuarios?

Debe existir interés para evaluar y controlar la implementación de esta tecnología.

La confiabilidad de los sistemas computarizados complejos no está garantizada.

* **Mantenimiento de privacidad**: Muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia.

Con sistemas automatizados se puede integrar y buscar información.

¿Qué pasa con la privacidad? Se podrían utilizar datos de genética humana para obtener información

Detallada sobre una persona y usarla en su contra. Hoy en día se maneja gran información de los individuos: trabajo, residencia, tarjetas de crédito... Se podría utilizar datos de la genética humana de una persona para usarla en su contra. Prevenir la exposición de datos privados de los usuarios de un sistema.

**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.

Otra: Si la información recolectada por el sistema no es exacta, el gerente tomará decisiones que probablemente sean incorrectas y esto provocará graves perjuicios a la empresa, desde el cierre de una sede de la empresa por falta de fondos para mantenerla a la quiebra total de la firma.

* **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.

Otra: Dado que el puesto no es especialmente crítico, los perjuicios que puede llegar a provocar son limitados al área donde ejerza su influencia. Sin embargo, los daños también podrían ser catastróficos: si, por ejemplo, se produce una carga incorrecta de las deudas de una cantidad X de personas esto afecta seriamente la imagen de ARBA, mucho más si el problema radica en que la gente debe pagar más de lo que se estipula. Podría ser también un error en la carga de un nombre lo cuál no tendría impacto prácticamente.

* **Consejo Directivo de una facultad** Una pérdida de datos relacionados con la historia académica de los alumnos.

Otra: El daño se limita a la facultad. Podrían ignorarse necesidades importantes o tomar decisiones que solucionen problemas no tan críticos. Los fondos se gastarían en problemas que quizá no eran tan urgentes y los problemas críticos se harían aún más críticos de forma que si suelen ser complejos de mitigar, se hacen aún más difíciles de solucionar y sus consecuencias se hacen más profundas.

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

Es un incidente relacionado con tecnología informática, en el cual una víctima sufre una pérdida, y un perpetrador podría lograr alguna ganancia. Las pérdidas por abusos computacionales suele ser sustancialmente mayor que la pérdida por fraudes convencionales

* Hacking
* Virus
* Acceso físico ilegal
* Abuso de privilegios

Las consecuencias pueden ser:

* Destrucción de activos
* Sustracción de activos
* Modificación de activos
* Violación de privacidad
* Interrupción de operaciones
* Uso no autorizado de activos
* Daño físico a personas

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

El incidente está asociado a tecnología informática.

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. Describir con sus palabras que entiende por auditoría de sistemas de información.**

*Auditoría en los sistemas de información se****entiende****como la verificación y el control en los sistemas para que los mismos realicen de forma eficiente y segura la tarea para lo cual fueron programados.*

*Otra:* Es un proceso en el que se recolecta y evalúa evidencia para determinar si el sistema automático preserva los activos, mantiene la integridad de los datos, permite que los objetivos organizacionales se alcancen con eficacia y usa los recursos con eficiencia.

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

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

Preservar los activos: es decir, resguardar el hardware, software, personas, insumos, y todos aquellos bienes, derechos y otros recursos de los que disponga la empresa.

Mantener la integridad de los datos: es decir, mantener la completitud, consistencia, veracidad y correctitud de éstos. Si la integridad de los datos no se mantuviera, la organización no posee representación de sí misma o de los eventos.

Alcanzar los objetivos organizacionales con eficacia: es decir, que la organización alcance los objetivos que se proponga con los efectos deseados

Usar con eficiencia los recursos: esto es, usar los recursos mínimos para satisfacer los objetivos que se le planteen a la organización.

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

**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

Un sistema de control interno es aquel implementado por la alta gerencia con el fin de alcanzar los objetivos de la auditoría. El uso de computadoras afecta de varias maneras la implementación de los componentes de un sistema de control interno.

Ejemplo:

1) en un sistema automatizado deben existir registros

2) las funciones son realizadas por un programa

Incluye:

* Separación de obligaciones: es decir, tener en cuenta que la automatización que proveen los sistemas hace que un mismo programa realice múltiples funciones que, de forma manual, personas diferentes realizarían.

En un sistema manual, personas diferentes deben realizar las tareas de:

1) iniciar la transacción

2) registrar la transacción

3) 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.

* Delegación clara de autoridad y responsabilidades: Una delegación clara de autoridad y responsabilidad es esencial tanto en sistemas manuales como automatizados. Es una parte esencial ya que en un sistema automatizado hacer esto de una manera no ambigua puede ser dificultoso.

Ejemplo: cuando múltiples usuarios tienen acceso a los mismos datos y la integridad es violada de alguna manera, no es fácil ubicar quién es el responsable, para identificar y corregir el error.

* Reclutamiento y entrenamiento de personal calificado (PERSONAL COMPETENTE Y CONFIABLE): en otras palabras, personas responsables que puedan manejar el poder que supone regular los sistemas automatizados. Con la rotación de personal y el poco tiempo de evaluación, no es algo fácil de asegurar.

A las personas responsables de desarrollar, implementar y operar los sistemas de información se les delega mucho poder.  
Ejemplos:  
1) un analista puede aconsejar a la gerencia sobre el equipamiento de alta tecnología y de altos costos  
2) un operador asume la responsabilidad de salvaguardar el software crítico y los datos realizando los back ups.  
El personal responsable de los sistemas automatizados tiene delegado mayor poder que los empleados que realizan tareas manuales.

PROBLEMAS DE PERSONAL  
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.  
Importante – algunas de estas personas también parecen tener poco desarrollado  
su sentido de ética.

* Sistema de autorizaciones: dicho de otra manera, deben ser consideradas las diferentes autorizaciones, desde una lista de precios hasta la compra de activos de alto valor. En los sistemas automatizados, las autorizaciones están embebidas dentro de los programas, por lo que los auditores no solo deben controlar la autorización en sí, sino también si se lleva a cabo exitosamente.

La gerencia debe establecer dos tipos de autorizaciones:  
1) autorizaciones generales: establecen las políticas que la organización debe seguir. Ejemplo: lista de precios.  
2) autorizaciones específicas: aplicables a transacciones individuales. Ejemplo: compra de activos de alto valor.  
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.

* Documentos y registros adecuados: en otros términos, asegurar que los documentos y los registros sean apropiados. En un sistema bien diseñado deberían haber mayores registros de auditoría que en un sistema manual. Se deben prever controles de acceso y facilidades de acceso para asegurar que los rastros de auditoría sean exactos y completos.

Se debe asegurar que los documentos y registros sean adecuados.  
En un sistema automatizado no es necesario un documento para iniciar una transacción, por ejemplo:  
1) un pedido telefónico,  
2) un sistema de reposición automático de stock.  
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.

* Control físico y documentación sobre los activos: o sea, controles de acceso y registro de éstos. Tanto en los sistemas manuales como en los automatizados es un factor crucial, la diferencia es que en los segundos todos los registros necesarios pueden mantenerse en un solo lugar. En tal contexto, la posibilidad de abuso o desastre por la concentración de información aumenta radicalmente, por lo que el sistema debe prevenir controles internos de supervisión. El auditor solamente accederá a los registros de auditoría para evaluar la gestión de los empleados.

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.

* Chequeos independientes de performance: dicho de otro modo, evaluar los controles establecidos para desarrollar, modificar, operar y mantener programas. En sistemas automatizados, los programas siempre ejecutan el mismo algoritmo a menos que haya una falla en el software o en el hardware.

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.

* Comparación periódica de activos con registros contabilizados: es decir, que los datos que representan los activos deben ser controlados con los activos reales, a fin de determinar falta de complexitud o inexactitud de los datos. En sistemas automatizados, se deben preparar programas que se encarguen de dicha tarea. Nuevamente es importante la implementación de controles en dichas tareas.

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.  
Ejemplo: control de inventarios.  
Nuevamente, son importantes la implementación de estos controles durante el desarrollo de sistemas.

**Control interno - Implementación**

El uso de computadoras afecta de varias maneras la implementación de los componentes de un sistema de control interno.

Ejemplo:

1. En un sistema automatizado deben existir registros
2. Las funciones son realizadas por un programa

LA COMPUTACIÓN EN AUDITORÍA 1

La función de auditoría no cambia  
En sistemas automatizados es más complicado recolectar evidencia.  
Ejemplos:  
1) controlar los casos de test de un programa,  
2) controles criptográficos.  
Es más difícil evaluar las consecuencias de las fortalezas y debilidades de los controles en pro de la confiabilidad general del sistema.

LA COMPUTACIÓN EN AUDITORÍA 2  
Los errores en los sistemas manuales tienden a ser estocásticos. Ejemplo: periódicamente el empleado se equivoca al actualizar un precio.  
Los errores en los sistemas automáticos:  
1) tienden a ser determinísticos  
2) se generan a mayor velocidad  
3) es mas costoso arreglarlos  
Ejemplo: un programa erróneo siempre se va a ejecutar erróneamente.  
Los controles internos que aseguran la alta calidad en el diseño, implementación, operación y mantenimiento de los sistemas, son críticos.

FUNDAMENTOS DE LA AUDITORÍA

La auditoría de sistemas de información se fundamenta en:

AUDITORÍA TRADICIONAL  
Aporta conocimientos y experiencia sobre técnicas de control interno.  
Aporta la filosofía de los controles. Ejemplo: los programas deben asegurar que todas las transacciones fueron procesadas correctamente.  
Involucra examinar los SI con una mente crítica, siempre con una visión cuestionadora sobre la capacidad de los SI para:  
1) salvaguardar activos,  
2) mantener integridad de datos,  
3) lograr objetivos eficiente y eficazmente.

ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN  
Aporta:  
1) técnicas de administración de proyectos.  
2) documentación, estándares, presupuestos.  
A raíz de los fracasos al comienzo, ahora aporta nuevos métodos para mejorar el desarrollo y la implementación de sistemas.  
Ejemplo: metodologías de desarrollo de sistemas.

CIENCIAS DEL COMPORTAMIENTO  
Una resistencia de comportamiento para con el sistema pone en peligro los objetivos de la auditoría.  
Usuarios descontentos pueden intentar sabotaje o circunscribir controles.  
Lo mismo sucede con diseñadores, y entre estos y los usuarios.  
Los auditores deben comprender las situaciones que dan lugar a conflictos de comportamiento y como resultado posible, el fracaso del sistema.

CIENCIAS DE LA COMPUTACIÓN  
Los Ingenieros de Software deben colaborar con los objetivos de la auditoría.  
Ejemplo: investigar sobre cómo probar la correctitud de un programa formalmente.  
El conocimiento técnico en profundidad desarrollado por esta disciplina causa problemas y beneficios a los auditores.  
• beneficios: se pueden preocupar menos por la confiabilidad de algunas componentes.  
• problemas: pueden tener dificultades para determinar abusos.

**Parte II: Controles y riesgos de Auditoría**

MOTIVACIÓN  
Felicitaciones!!! Lo han designado Gerente del Departamento de Auditoría de la Empresa “X”.  
La empresa posee:  
o 520 programadores y analistas  
o 1245 PC’s conectadas en red  
o 5378 bases de datos.  
Pregunta: ¿cómo puede ejecutar la auditoría, de tal forma de obtener una seguridad razonable sobre:  
1) la salvaguarda de activos en el procesamiento de datos,  
2) integridad de los datos,  
3) la eficiencia y eficacia de los sistemas ?

SOLUCIÓN  
Implementar sistemas de control.  
1) saber qué es un control y cómo funcionan los controles  
2) determinar qué controlar  
3) estimar la confiabilidad de los controles  
4) estimar el riesgo de la auditoría

LA NATURALEZA DE LOS CONTROLES  
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

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

Porque un control solo puede ser control en el contexto de un sistema que asegure la prevención, detección y corrección de eventos ilegales.

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 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

CONTROL DE EVENTOS ILEGALES  
¿Cómo puede surgir un evento ilegal?  
1) si se ingresan al sistema inputs no autorizados, inexactos, incompletos, redundantes, ineficaces o ineficientes,  
2) si el sistema transforma el input de una manera no autorizada, inexacta, incompleta, ineficiente o ineficaz  
Ejemplos:  
1) inputs incorrectos en un programa interactivo.  
2) un programa que contiene instrucciones erróneas que resultan en una ejecución incorrecta.

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

Ej:

* **Control preventivo:** Instrucciones de cómo completar un formulario. *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.

OBJETIVO DE LA AUDITORÍA: Reducir las pérdidas esperadas por eventos ilegales mediante:

1. Los **controles preventivos** reducen la probabilidad que ocurran eventos ilegales.
2. Los **controles detectivos** son aquellos que identifican los eventos en el momento en que se presentan. Son más costosos que los preventivos. Reducen la cantidad de pérdidas cuando un evento ilegal ocurre.

Los **correctivos**  aquellos que aseguran que las acciones correctivas sean tomadas para revertir un evento no deseado. También reducen la cantidad de pérdidas cuando un evento ilegal ocurre.

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

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**.

Es necesario un **criterio (**La esencia de un subsistema es la función que realiza.**)** para poder factorizar. Los auditores deben identificar primero, las principales funciones que el sistema realiza para cumplir sus objetivos.

El proceso de factorización termina cuando se han particionado el sistema en partes lo suficientemente pequeñas, de tal modo que puedan ser atendidas y evaluadas.

**12. Indique qué otros criterios de factorización existen.**

Además de las funciones, existen otras dos guías:

* **Acoplamiento:**
  + Cada subsistema debería ser relativamente independiente de otros subsistemas.
  + Sistemas con *poco acoplamiento* son mas 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.

**Formas de factorización**

Para realizar una auditoría se debe factorizar en subsistemas:

* 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.
* 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.

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

CONFIABILIDAD DE SUBSISTEMAS  
Primero - determinar el menor nivel de los subsistemas.  
Segundo - evaluar la confiabilidad de los controles en cada subsistema.

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 este 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:

* Las caídas en los sistemas de información
* 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.*

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.

EVENTOS Y TRANSACCIONES  
Cuando un evento ocurre, el sistema recibe una transacción de input.  
Cuando la transacción se recibe como input el sistema cambia de estado.  
Otros cambios de estado ocurren a medida que el sistema procesa la transacción.  
Ejemplo: toma de pedidos.  
Para identificar todos los eventos que pueden ocurrir en un sistema como resultado de la transacción, se debe entender cómo el sistema procesa la transacción.

Pasos:  
1) identificar los componentes que procesan cada transacción  
2) comprender el procesamiento de cada componente  
3) considerar errores o irregularidades que puedan ocurrir durante el procesamiento  
4) trabajar con clases de transacciones.

PROCESAMIENTO DE TRANSACCIONES  
Generalmente los auditores aplican técnicas de walk-through:  
1) se considera una transacción particular,  
2) se identifican todos los componentes del sistema que procesan la transacción  
3) se trata de entender cada paso de procesamiento que ejecuta cada componente  
4) se considera cualquier error o irregularidad (evento ilegal) que pueda ocurrir en el camino.

CLASES DE TRANSACCIONES  
Generalmente es muy costoso realizar este proceso para todas las transacciones.  
Por eso, se trabaja con clases de transacciones:  
1) se agrupan transacciones que tengan un procesamiento similar,  
2) se trata de entender esas transacciones, y los eventos que puedan surgir como resultado de esas transacciones como grupo,  
3) se tratan sólo aquellas transacciones que se consideran importantes para los objetivos de la auditoría.

¿QUÉ EVENTOS?  
Usando esta técnica, no se identifican todos los eventos que puedan surgir en un sistema.  
A pesar de esto, los auditores deberían examinar todas aquellas transacciones y eventos que consideren importantes.  
Una vez que se han identificado los eventos que pueden ocurrir, los auditores deben evaluar:  
1) si los controles están correctamente ubicados, y  
2) si funcionan para detectar eventos ilegales.

CONFIABILIDAD DE LOS CONTROLES - 1  
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:

La evaluación de la confiabilidad procede de abajo hacia arriba en el nivel de estructura de los sistemas.  
Los subsistemas de menor nivel son componentes de los de mayor nivel.  
Cuando se haya evaluado la confiabilidad de los subsistemas de menor nivel, se puede analizar:  
1) el impacto  
2) la naturaleza, y  
3) la frecuencia de los eventos ilegales en los sistemas de mayor nivel.

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 debido a:  
1) Los controles en sistemas de bajo nivel pueden funcionar mal. Ejemplo: se divide el trabajo en varias personas y un superior controla el funcionamiento general.  
2) Podría ser más efectivo en costos implementar controles a alto nivel. Ejemplo: en lugar de que cada uno controle su trabajo, un superior aleatoriamente supervisa el trabajo por muestreo.  
3) Algunos eventos no se manifiestan como ilegales excepto en los niveles altos. Ejemplo: consultas a una base de datos sin violar confidencialidad.

**14. Identificar cuatro tipos de riesgos. Explicar 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 riesgos incorrectos.

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

RDA = RI \* RC \* RD

* + ***Riesgo deseado:****el riesgo que se desea correr.*

Primero los auditores eligen el nivel de RDA.  
Evalúan las consecuencias de fracasar en detectar las pérdidas materiales reales o  
potenciales.

* + **Riesgo inherente:** refleja la probabilidad que una pérdida material o una imputación errónea exista en algún segmento de la auditoría, antes que sea considerada la confiabilidad de los controles internos.

Luego, se considera el nivel de RI.  
Los auditores consideran factores generales tales como:  
1) la naturaleza de la organización (la posición en el mercado),  
2) la industria en la que opera (¿la industria está sujeta a cambios rápidos?)  
3) las características del gerenciamiento (¿es agresivo y autocrático?)  
4) intereses contables y de auditoría (¿se usan técnicas?)

¿Cómo? Se consideran luego los RI asociados con diferentes segmentos de la auditoría (ciclos, sistemas de aplicación, ...).  
Para cada segmento, se consideran factores tales como:  
1) sistemas financieros  
2) sistemas estratégicos  
3) sistemas de operación crítica  
4) sistemas de tecnología avanzada

RIESGO INHERENTE DE SISTEMAS FINANCIEROS  
Proveen controles financieros sobre los principales activos de la organización.  
Poseen alto RI.  
Son el blanco de acciones delictivas y fraudes.  
Ejemplo: sistema de facturación

RIESGO INHERENTE DE SISTEMAS ESTRATÉGICOS  
Proveen ventajas competitivas para la organización.  
Comprometen clientes, proveedores, secretos de marca.  
Tienen alto RI.  
Son blanco de espionaje industrial, o acciones indebidas de la competencia.  
Ejemplo: el sistema que soporta la operatoria comercial de una empresa

RIESGO INHERENTE DE SISTEMAS DE OPERACIÓN CRÍTICA  
Aquellos sistemas que pueden paralizar a la organización si fallan.  
Generalmente tienen alto RI.  
Ejemplo: sistemas de control de producción, sistemas de reservas.

RIESGO INHERENTE DE SISTEMAS DE TECNOLOGÍA AVANZADA  
Sistemas que usan tecnología de punta.  
Tienen alto RI, debido a la falta de experiencia en ese tipo de sistemas.

* + **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.  
Generalmente, se identifican y evalúan primero los controles en los subsistemas gerenciales.

CONTROLES GERENCIALES - 1  
Los controles gerenciales actúan como capas de cebolla protectivas, por encima de los controles de aplicación.  
^ Alta Gerencia  
| Gerencia de Sistemas de Información  
| Gerencia de Desarrollo de Sistemas  
| Gerencia de Programación  
| Administración de Datos  
| Aseguramiento de Calidad  
| Administración de Seguridad  
| Gerencia de Operaciones

El buen nivel de los controles externos garantizan el nivel de los controles internos.  
Los controles gerenciales se evalúan en general, y no para cada aplicación

* + **Riesgo de detección:** refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas.

Finalmente, se calcula el nivel de RD que se debe lograr para cumplir con el RDA.  
Se diseñan procedimientos de recolección de evidencia para intentar lograr el nivel de RD.  
En general:  
1) los auditores no recolectan la cantidad de evidencia que ellos desearían  
2) deben ser astutos para determinar en dónde aplicar los procedimientos de auditoría, y cómo interpretar la evidencia recolectada.

**Parte III: Proceso de Auditoría**

**15. Explicar brevemente el proceso de auditoría.**

Una auditoría

Existen diferentes procedimientos de auditoria, dependiendo de lo que se desee controlar:

1. Determinar si ocurrieron pérdidas materiales o la información financiera es errónea
2. Determinar la eficiencia y eficacia de las operaciones

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

A fin de recolectar evidencia, para determinar si ocurrieron pérdidas materiales o  
la información financiera es errónea, se usan los siguientes procedimientos:

Se usan los siguientes procedimientos para recolectar evidencia

1. Procedimientos para comprender los controles

Los procedimientos incluyen:  
1) cuestionarios,  
2) inspecciones,  
3) observaciones  
Para determinar:  
1) si los controles existen,  
2) analizar cómo están diseñados,  
3) si funcionan.

1. Testeo de controles

Son para evaluar si los controles están actuando efectivamente.  
Ejemplos:  
1) cuestionarios  
2) inspecciones  
3) observaciones  
4) reprocesos

1. 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. Testeos substantivos de:

4.1) 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. (Para el caso de determinar pérdidas materiales o información financiera errónea)

4.2) de resultados generales. (Para determinar eficiencia y eficacia de las operaciones. La noción de balances contables no es aplicable en este caso. Ej.: testeos de performance.)

1. 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, modelos de simulación.

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

1. Testeo de controles
2. Testeos substantivos de detalle de transacciones
3. Testeos substantivos de: (resultados gerenciales o balances contables) 4.1) Balances Contables (Para el caso de determinar pérdidas materiales o información financiera errónea) 4.2) de resultados generales. (Para determinar eficiencia y eficacia de las operaciones. Ej.: testeos de performance.)

* Cuestionarios.
* Inspecciones.
* Observaciones.

ORDEN DE LOS TESTEOS  
El orden de los testeos de menos costosos a más costosos es:  
1) procedimientos de revisión analítica  
2) procedimientos para comprender los controles  
3) testeo de controles  
4) testeos sustantivos de detalle de transacciones  
5) testeos sustantivos de resultados generales/balances contables  
El orden es a la inversa si se evalúa la confiabilidad y el contenido de la información de la evidencia provista por los procedimientos.

**18. ¿Cómo se lleva a cabo la planificación de una auditoría? 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:

* Auditoría interna
  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 las áreas de riesgo

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

* Auditoría externa
  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. (Se emite un RDA en general para toda la tarea de auditoría.)
3. Emitir una opinión sobre el RI.

El RI depende del segmento a auditar.  
Algunos segmentos son más susceptible a errores, irregularidades, ineficiencias, o ineficacias.  
Para cada segmento evaluar los factores que conducen a RI, por ejemplo:  
- sistema con manejo de efectivo: posibilidades de defraudaciones.  
- sistema complejo tecnológicamente: posibilidades de mal uso de recursos.

1. Emitir una opinión sobre el RC.

La decisión más difícil está en emitir el juicio en el nivel de RC asociado con cada segmento de la auditoría.  
Para esto, los auditores deben comprender los controles internos usados dentro de la organización.  
Los controles internos (CI) comprenden 5 componentes relacionados:  
1) controles de entorno  
2) evaluación de riesgo  
3) actividades de control  
4) información y comunicación  
5) monitoreo

1. Calcular el RD que se debe lograr para cumplir con el RDA,
2. Recolectar evidencia

Existen distintas técnicas para recolectar evidencia:  
1) revisión de papeles de trabajo de auditorías previas  
2) entrevistas con alta gerencia y personal superior  
3) observación de cómo se desarrollan las actividades  
4) revisión de documentación de sistemas

1. Documentar evidencia

La evidencia se documenta:  
1) completando cuestionarios  
2) construyendo diagramas de flujo de alto nivel  
3) construyendo tablas de decisión  
4) redactando descripciones narrativas.  
5) utilizando herramientas CASE  
No invertir demasiado tiempo en esta etapa. El necesario para comprender los controles internos y decidir cómo proseguir con la auditoría.  
Finalmente se debe evaluar el riesgo.

RDA: Riesgo deseado de auditoría RI: Riesgo Inherente RC: Riesgo de control RD: Riesgo de detección

| **Categoría a evaluar** | **Auditoría interna** | **Auditoría externa** |
| --- | --- | --- |
| Planificación | Incluye asignar personal adecuado a las auditorías, obtener información del cliente, realizar procedimientos de revisión analíticos para comprender el negocio del cliente e identificar áreas de riesgo. | Incluye 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 e identificar áreas de riesgo. |
| Mayor preocupación | El tamaño de las pérdidas que pudiera haber por operaciones ineficientes o ineficaces. | El tamaño de los errores en los estados financieros. |
| Actitud del auditor ante un control débil(por ejemplo, para entender las implicancias) | Expandir sus investigaciones para lograr una mejor comprensión acerca de la naturaleza e implicancias de estas debilidades. | Cortar sus investigaciones(sobre causas) y realizar testeos más amplios. |

**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.

ALCANCE DE LA AUDITORÍA  
Determinar qué se va a auditar:  
1) un sistema  
2) un conjunto de sistemas  
3) un área del tecnología informática

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

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 riesgos 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.

CONTROLES INTERNOS – 1) CONTROLES DE ENTORNO  
Incluye evaluar los elementos que establecen el contexto de control en el cual deben operar los sistemas y los procedimientos de control.  
Ejemplos:  
1) filosofía y estilo de gerenciamiento y operación,  
2) formas de asignar autoridad y responsabilidad,  
3) métodos para monitorear performance…

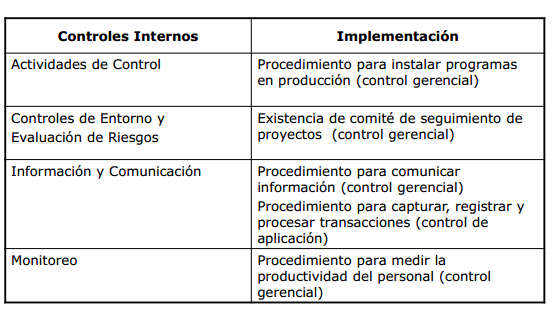
CONTROLES INTERNOS – 2) EVALUACIÓN DE RIESGO  
Incluye evaluar:  
1) los elementos que identifican y analizan los riesgos a los cuales se enfrenta la organización y  
2) cómo son administrados.  
Ejemplos:  
1) planificaciones de proyectos  
2) documentos de administración de riesgos

CONTROLES INTERNOS – 3) ACTIVIDADES DE CONTROL  
Incluye evaluar los elementos que operan para asegurar que:  
1) las transacciones son autorizadas,  
2) las responsabilidades se separan,  
3) los documentos y registros se mantienen adecuadamente, etc.  
Se clasifican en:  
1) controles contables: elementos que operan para asegurar distintos niveles de autorizaciones y responsabilidades  
2) controles administrativos: elementos para asegurar eficiencia y eficacia

CONTROLES INTERNOS – 4) INFORMACIÓN Y COMUNICACIÓN  
Incluye evaluar los elementos en los cuales se:  
1) identifica,  
2) captura,  
3) intercambia información  
en tiempo y forma.  
Permite asignar responsabilidades del personal adecuadamente.  
Ejemplos: notificaciones, minutas de reuniones.

CONTROLES INTERNOS – 5) MONITOREO  
Incluye evaluar los elementos que aseguran que los controles internos operan de manera confiable en el tiempo.  
Ejemplos:  
1) monitoreos de performance,  
2) control de calidad

COMPRENDER LOS CONTROLES  
Comprender los controles internos incluye factorizar y examinar los controles gerenciales y de aplicación.  
Los controles gerenciales varían sustancialmente de organización a organización.  
Ejemplo: los controles gerenciales son distintos si la empresa tiene:  
1) sistemas centralizados,  
2) sistemas descentralizados.



EVALUACIÓN DE RIESGO DE CONTROL   
Si se evalúa que el RC < el nivel máximo =>  
1) identificar los controles materiales que se relacionan con la evaluación  
2) testear los controles para determinar si operan efectivamente.  
Premisa: los testeos de controles probarán, que si los controles funcionan  
correctamente, se puede reducir la necesidad de un testeo

Si se evalúa que el RC es de nivel máximo => no se testean los controles.  
Se podría concluir que los controles internos no son efectivos.  
Se debería realizar un testeo amplio.

TESTEO DE CONTROLES - 1  
El testeo de controles evalúa cuan confiables y específicos son los controles.  
Se testean, sólo si el RC se determinó menor al máximo.  
Se confía en los controles como una base para reducir el costo de un testeo más amplio.  
A esta altura, los auditores no saben si los controles identificados operan efectivamente.

CONTROLES GERENCIALES – TESTEO  
Se comienza por los controles gerenciales.  
Si los controles gerenciales, demuestran contrariamente a lo supuesto, que no operan eficientemente => no tiene sentido testear los controles de aplicación.  
Ejemplo:

|  |  |
| --- | --- |
| Los gerentes afirman que se informa periódicamente de los avances de proyectos | solicitar informes de avances o minutas de las reuniones. |
| Los gerentes afirman que existen estándares de desarrollo | solicitar programas fuentes e inspeccionar una muestra |

CONTROLES DE APLICACIÓN – TESTEO  
Si los controles gerenciales funcionan efectivamente, se procede a evaluar los controles de la aplicación.  
Ejemplo:

|  |  |
| --- | --- |
| Se limpian diariamente los errores detectados | pedir muestreo |
| Existen niveles de autorización para realizar transacciones | pedir muestreo |

Luego de evaluados los controles, se vuelve a estimar el riesgo.

TESTEO DE CONTROLES – CONCLUSIÓN  
Se puede concluir que los controles internos son más fuertes o más débiles a lo anticipado.  
Si los controles son más fuertes a lo pensado, se puede pensar en reducir testeos.  
Si los controles son más débiles, se pueden ampliar los testeos.

ACTITUD DEL AUDITOR  
Durante esta etapa los auditores externos e internos pueden tener distintas actitudes.  
Situación: se detecta que los controles son débiles

1) auditor interno: puede expandir sus investigaciones para lograr una mejor comprensión a cerca de la naturaleza e implicancias de estas debilidades.  
2) auditor externo: puede cortar sus investigaciones (sobre causas) y realizar testeos más amplios.

TESTEO DE TRANSACCIONES  
Se realiza para evaluar si un procesamiento erróneo o irregular puede ocasionar pérdidas.  
Ejemplo: examinar cálculos, precios.  
Desde un punto de vista operativo, el testeo de transacciones sirve para determinar si el procesamiento es efectivo y eficiente.  
Ejemplo: consultas a una base de datos, carga de máquina.

TESTEO DE RESULTADOS GENERALES  
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.  
Ejemplo:

|  |  |
| --- | --- |
| Evaluar objetivos de salvaguarda de activos e integridad de datos | Testeos de control de inventario físico Confirmación de recepción de mercaderías Recálculo de amortizaciones |

TESTEO DE RESULTADOS…  
Si los auditores confían en que los controles son confiables, pueden limitar el número y alcance de estos testeos.  
Si es a la inversa, aumentarán el grado de control para estimar mejor las pérdidas.

EVALUAR EFECTIVIDAD Y EFICIENCIA  
Evaluar efectividad y eficiencia es más complejo.  
Se puede trabajar con los usuarios estimando las pérdidas por no haber tomado una decisión por no contar con la información en tiempo y forma.  
Ejemplo: evaluar la ineficiencia por compra de hardware inapropiado.

COMPLETAR LA AUDITORÍA  
En la etapa final, se realizan testeos adicionales para cerrar la evidencia.  
Finalmente, se formula la opinión sobre cómo ocurrieron las pérdidas materiales o registros incorrectos en un informe.

**Parte IV: Gobernanza de TI**

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

Concepto: La gobernanza de TI es un subconjunto de Gobierno Corporativo de las organizaciones que se centra en los sistemas 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 de TI generen valor
* Mitigar riesgos asociados con TI

Definiciones:

Son estructuras y procesos de liderazgo y organizativos que aseguran que las TI de la organización sostienen y extienden las estrategias y los objetivos de la organización. *Instituto de gobernanza de TI*

Se trata de especificar los derechos de decisión en el marco de rendición de cuentas para fomentar el comportamiento deseable en el uso de TI.

es el sistema por el cual se dirige y controla el uso actual y futuro de las TIC. Implica evaluar y dirigir los planes para el uso de las TIC para apoyar a la organización y monitorear este uso para alcanzar los planes. Incluye la estrategia y las políticas para el uso de las TIC dentro de una  
organización.

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

**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 adoptar un marco de gobernanza y control de TI.

Fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, [www.isaca.org](http://www.isaca.org)) y el Instituto de Gobernanza de TI en 1992.  
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).

* Auditoría
* Control
* Administración
* Gobernanza de TI
* Gobernanza de TI empresarial

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

Son dos conceptos diferentes.

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

La diferencia es que la gobernanza asegura que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar objetivos empresariales a alcanzar equilibrados y acordados. Establece la dirección a través de la priorización y la toma de decisiones supervisando el desempeño y cumplimiento contra la dirección y objetivos acordados. La administración planifica, construye, ejecuta y monitorea las actividades en consonancia con la dirección establecida por el cuerpo de gobierno para alcanzar los objetivos empresariales. Es algo así como una vez ejecutada la administración, se da la gobernanza. La gobernanza asegura y la administración planifica y construye.

**24. ¿Cuáles son los principios de COBIT?**

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. Indicar de qué forma organiza COBIT los procesos de TI.**

*COBIT 5*\* es un conjunto de recursos que contienen todas las organizaciones de información que necesitan para adoptar una gobernanza de TI y un marco de control. Los procesos de TI se dividen en 5 dominios (COBIT 5):

GOBERNANZA

1. Evaluar, dirigir y monitorear

EDM se interesa en:  
o establecer un marco de gobernanza  
o crear valor para las partes interesadas  
o 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).

ADMINISTRACIÓN

1. Alinear, planear y organizar: proporciona direcciones a la entrega de soluciones y servicios. abarca estrategias y tácticas y se interesa en la forma que TI puede contribuir a alcanzar los objetivos de negocio.

APO se interesa en: la comprensión de la vision a planificar, comunicar y gestionar, una organización e infraestructura adecuadas para su puesta en marcha

1. Construir, adquirir e implementar: provee soluciones a DSS para la entrega de servicios. (BAI) abarca soluciones de TI que necesitan ser identificadas,  
   desarrolladas o adquiridas, implementadas e integradas en el proceso de negocio.

BAI se enfoca en: los cambios en las soluciones de TI existentes, el mantenimiento de sistemas existentes, asegurar que las soluciones continúan cumpliendo con las metas empresariales

1. Entrega, servicio y soporte: recibe soluciones y las hace utilizables para los usuarios finales

(DSS) trata sobre la entrega efectiva de los servicios requeridos, incluyendo operaciones, seguridad y capacitaciones de continuidad.

DSS se enfoca en: la gestión de seguridad y continuidad  
del servicio, el soporte de servicios para usuarios, la administración de datos, instalaciones operacionales

1. Monitorear y evaluar: monitorea todos los procesos para asegurar que se siga la dirección provista

(MEA) trata de la evaluación regular de los procesos de TI para controlar su calidad y el cumplimiento de los requisitos de control.

MEA se enfoca en: la gestión de desempeño, el cumplimiento normativo, el control interno

Elementos sobre el enfoque de COBIT a la Gobernanza de TI

1. Procesos de TI y dominios
2. Objetivos de control

Declaración del resultado o propósito a alcanzar mediante la implementación de procesos de control en una actividad particular de TI.

COBIT proporciona objetivos de control de alto nivel, uno para cada uno de los procesos de TI.

Cada objetivo de control de alto nivel se subdivide en una lista de objetivos de control detallados.

COBIT contiene 318 objetivos de control detallados

1. Prácticas de control

Las prácticas de control de TI proporcionan el más detallado POR QUÉ y CÓMO que necesitan los administradores, los proveedores de servicios, los usuarios finales y los profesionales de control para implementar controles específicos basados en un análisis de los riesgos operacionales y de TI.

1. Guías de auditoría

Las guías de auditoria describen y sugieren las actividades de evaluación que se corresponderán a cada uno de los objetivos de TI de alto nivel  
Proporcionan direcciones sobre:  
- a quién entrevistar y qué preguntas hacer  
- cómo evaluar el cumplimiento de los controles y las evaluaciones  
- cómo comprobar el riesgo de que no se cumplan los controles identificados

1. Guías de administración

Las guías de administración proporcionan direcciones para:  
- tener bajo control la información de la empresa y los procesos relacionados  
- alcanzar los objetivos de la organización  
- monitorear y mejorar el desempeño de cada proceso de TI  
- comparar logros organizacionales  
Para cada proceso de TI, las guías de administración incluyen:  
- modelos de madurez (MMs),  
- factores de éxito críticos (CSFs)  
- Indicadores claves de metas (KGIs)  
- indicadores claves de rendimiento (KPIs)

* PROCESOS DE TI -> (auditados por) Guías de auditoría
* PROCESOS DE TI -> (satisfacen) Requerimientos de negocio
* PROCESOS DE TI -> (clasificados en) Dominios
* PROCESOS DE TI -> (control facilitado por) Objetivos de control -> (Considerando) Prácticas de control
* PROCESOS DE TI -> (administrados por) Guías de administración

**26. Explicar 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. Justificar la importancia de aplicar COBIT en una organización.**

Beneficios generales de aplicar 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
* Optimiza las inversiones en TI, garantiza una prestación de servicios efectiva y proporciona medidas
* 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