Práctica 3 – Auditoría y Peritaje de Sistemas

Parte I: Conceptos generales

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

Razones principales para auditar sistemas y ejemplos:

1. **Costos por pérdida de datos**
   - Ejemplo: Pérdida de cuentas corrientes o datos de alumnos debido a fallas en backups o ataques.
2. **Costos por decisiones incorrectas**
   - Ejemplo: Error en reglas de decisión automatizadas (Knight Capital perdió $500 millones por un algoritmo defectuoso).
3. **Costos por abusos computacionales**
   - *Hacking*: Robo de 7,000 bitcoins (equivalente a €36 millones).
   - *Virus*: Ataques como el ransomware "Clop".
   - *Acceso físico ilegal*: Copia no autorizada de datos en salas de cómputo.
   - *Abuso de privilegios*: Empleado que copia datos confidenciales.
4. **Costos por errores de computación**
   - Ejemplo: Sobredosis de radiación en pacientes por fallas en el software Therac-25 (3 muertes).
5. **Valor de hardware, software y personal**
   - Ejemplo: Pérdida competitiva si la competencia obtiene información confidencial.
6. **Mantenimiento de privacidad**
   - Ejemplo: Robo de datos de 6 millones de licencias de conducir en Argentina.
7. **Evolución controlada del uso de TI**
   - Ejemplo: Implementación de sistemas no confiables que generan riesgos físicos o mentales en usuarios.

(Fuente: Documento, páginas 3–20)

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:

o Gerente de una empresa vinculada a la industria automotriz

- Un gerente de una empresa automotriz podría tomar malas decisiones de negocio relacionadas a que tipo de vehiculó fabricar con respecto a la demanda que en realidad tenga, por lo tanto podría

producir de mas o de menos cierto modelo perder ganancias en el proceso.

o Funcionario de ARBA

- Un funcionario de ARBA podría terminar cobrando menos impuestos de los que se deberían y perder recaudación para la provincia.

o Consejo Directivo de una facultad

- Se puede sobre asignar alumnos a cursos o dejar sin alumnos otros.

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

1. **Hacking**
   - *Ejemplo*: Acceso no autorizado para robar datos (ej. robo de 7,000 bitcoins por $36 millones).
   - *Consecuencias*: Pérdida financiera, daño reputacional y violación de confidencialidad. *(pág. 10-11)*
2. **Virus/Malware**
   - *Ejemplo*: Ransomware "Clop" que cifra datos para extorsión.
   - *Consecuencias*: Interrupción operativa, pérdida de datos y costos de recuperación. *(pág. 12)*
3. **Acceso físico ilegal**
   - *Ejemplo*: Robo de hardware o copia no autorizada de datos en salas de cómputo.
   - *Consecuencias*: Daño a activos, robo de información sensible. *(pág. 13)*
4. **Abuso de privilegios**
   - *Ejemplo*: Empleado que usa permisos para copiar datos confidenciales.
   - *Consecuencias*: Filtración de información, sanciones legales o despidos. *(pág. 14)*

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

1. **Medio de ejecución**
   - *Abuso informático*: Requiere el uso de tecnología (ej: hacking, malware). *(pág. 10)*
   - *Fraude comercial*: Se realiza mediante métodos tradicionales (ej: falsificación de documentos en papel). *(No mencionado en el documento, pero implícito por contraste)*
2. **Velocidad y alcance**
   - *Abuso informático*: Puede causar pérdidas masivas en minutos (ej: pérdida de $500 millones en Knight Capital por error de software). *(pág. 8)*
   - *Fraude comercial*: Suele ser más lento y limitado en impacto (ej: desvío manual de fondos en una sucursal).

(Basado en ejemplos y definiciones del documento, páginas 8, 10-12)

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

Auditoría de Sistemas de Información es un proceso sistemático que evalúa y verifica si los sistemas informáticos de una organización:

1. **Protegen los activos** (hardware, software, datos). *(pág. 23, 26)*
2. **Mantienen la integridad de los datos** (completos, consistentes y exactos). *(pág. 27)*
3. **Cumplen objetivos eficientemente** (usan recursos adecuados). *(pág. 25, 30)*
4. **Garantizan cumplimiento normativo** (leyes, estándares como ISO). *(pág. 24)*

Ejemplo práctico:

- Auditar un sistema bancario para detectar si hay vulnerabilidades a hackeos o errores que afecten la precisión de los saldos. *(Basado en casos del documento, pág. 8, 11)*

(Definición sintetizada de las páginas 23-24, 56)

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

1. **Preservar los activos**
   - Evaluar controles para proteger hardware, software, datos y personal. *(pág. 23, 26)*
2. **Mantener la integridad de los datos**
   - Verificar que los datos sean completos, consistentes y exactos para evitar decisiones erróneas. *(pág. 23, 27)*
3. **Garantizar eficacia**
   - Asegurar que los sistemas cumplen sus objetivos (ej: satisfacer necesidades de usuarios). *(pág. 23, 29)*
4. **Optimizar eficiencia**
   - Controlar que los recursos (tiempo, costos, infraestructura) se usen de forma óptima. *(pág. 23, 30)*

(Resumen basado en páginas 23-25, 56 del documento)

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

Significado:
Que la alta gerencia establezca políticas, procedimientos y estructuras para **proteger activos**, **garantizar la integridad de los datos** y **lograr objetivos organizacionales** de manera eficiente. *(pág. 31-32)*

Cómo se lleva a cabo (componentes clave):

1. **Separación de obligaciones**

- Dividir funciones críticas (ej: quien ejecuta un programa no debe modificarlo). *(pág. 34)*

2. **Delegación clara**
   - Asignar responsabilidades específicas para evitar ambigüedades (ej: acceso a datos). *(pág. 35)*
3. **Personal calificado**
   - Contratar y capacitar empleados competentes (ej: operadores de backups). *(pág. 38)*
4. **Autorizaciones**
   - Implementar reglas generales (ej: políticas de precios) y específicas (ej: compras costosas). *(pág. 40)*
5. **Documentación y registros**
   - Mantener trazas de auditoría (ej: logs de acceso) para rastrear acciones. *(pág. 41)*
6. **Controles físicos**
   - Restringir acceso a salas de servidores o dispositivos críticos. *(pág. 42)*
7. **Chequeos independientes**
   - Revisar periódicamente el rendimiento del sistema (ej: pruebas de programas). *(pág. 44)*
8. **Comparación de activos**
   - Verificar que los registros coincidan con los activos reales (ej: inventarios). *(pág. 45)*

(Fuente: páginas 31-45 del documento)

Parte II: Controles y riesgos de Auditoría

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

Un control en un sistema de información es un sistema porque no depende de un único elemento, sino de un conjunto de componentes interrelacionados que trabajan juntos para prevenir, detectar o corregir eventos ilegales.

Por ejemplo, una contraseña solo se convierte en un control efectivo cuando forma parte de un sistema que incluye:

1. Seguridad en la elección de contraseñas.
2. Validación correcta de contraseñas.
3. Almacenamiento seguro de contraseñas.
4. Monitoreo de intentos de acceso no autorizados.

(Fuente: IS3 - Clase 8, pág. 8).

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

Control Preventivo:
Evita que ocurran eventos ilegales.

Ejemplo: Instrucciones claras para completar un formulario correctamente *(IS3 - Clase 8, pág. 10)*.

Control Detectivo:
Identifica eventos ilegales después de que ocurren.
Ejemplo: Programa que valida datos de entrada y rechaza los erróneos *(IS3 - Clase 8, pág. 10)*.

Control Correctivo:
Repara o mitiga los efectos de eventos ilegales detectados.
Ejemplo: Programa que corrige datos corruptos por ruido en comunicaciones *(IS3 - Clase 8, pág. 10)*.

(Todos los ejemplos y definiciones provienen del documento proporcionado).

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

La tarea del auditor es determinar si los controles están implementados y funcionan correctamente para:

1. **Prevenir** eventos ilegales (controles preventivos).
2. **Detectar y corregir** eventos ilegales que ya ocurrieron (controles detectivos y correctivos).

El objetivo es **reducir pérdidas materiales** asegurando que los controles sean:

- **Ubicados adecuadamente** (en los subsistemas correctos).
- **Confiables** (efectivos para su propósito).

(Fuente: IS3 - Clase 8, pág. 11).

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.

Factorizar en subsistemas en auditoría de sistemas consiste en dividir un sistema complejo en partes más pequeñas (subsistemas) para evaluar sus controles y riesgos de manera individual. Esto facilita la comprensión y el análisis del sistema global.

Criterios para factorizar:

1. **Función principal**: Cada subsistema debe cumplir una función específica y necesaria para el sistema general *(IS3 - Clase 8, pág. 13-14)*.
2. **Mínimo acoplamiento**: Los subsistemas deben ser independientes entre sí para simplificar su evaluación *(IS3 - Clase 8, pág. 15)*.
3. **Máxima cohesión**: Las actividades internas de cada subsistema deben estar alineadas con su función principal *(IS3 - Clase 8, pág. 15)*.

Ejemplo de factorización:

- **Funciones gerenciales**: Alta gerencia, desarrollo de sistemas, operaciones *(IS3 - Clase 8, pág. 17-19)*.

- **Funciones de aplicación**: Subsistemas de input, procesamiento, base de datos *(IS3 - Clase 8, pág. 22-23)*.

12. Indique qué otros criterios de factorización existen.

Criterios adicionales de factorización en auditoría de sistemas:

1. **Por funciones gerenciales**
   - Divide el sistema según roles administrativos (ej.: alta gerencia, desarrollo de sistemas, operaciones).
   - *Ejemplo*: Subsistema de "Gerencia de Aseguramiento de Calidad" encargado de verificar estándares *(IS3 - Clase 8, pág. 17-19)*.
2. **Por funciones de aplicación**
   - Segmenta según tareas específicas de procesamiento (ej.: input, comunicaciones, base de datos).
   - *Ejemplo*: Subsistema "Limitrofe" para interfaces usuario-sistema *(IS3 - Clase 8, pág. 22-23)*.

(Documento: IS3 - Clase 8, págs. 16-23).

Nota: Estos criterios complementan los de *función principal*, *acoplamiento* y *cohesión* mencionados previamente. Todos están explícitamente descritos en el material.

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

Medición de la confiabilidad de controles en auditoría de sistemas:

1. **Identificación de eventos ilegales**
   - Se analizan todas las transacciones y procesos para detectar posibles errores o irregularidades (*IS3 - Clase 8, pág. 25-26*).
2. **Evaluación de controles por subsistema**
   - Se verifica si los controles previenen, detectan o corrigen eventos ilegales en cada subsistema (*IS3 - Clase 8, pág. 31*).
3. **Uso de matrices de efectividad**
   - Se aplican tablas que clasifican la eficacia de los controles (ej.: Alta/Media/Baja) frente a tipos específicos de errores (*IS3 - Clase 8, pág. 33*).
4. **Enfoque jerárquico (de abajo hacia arriba)**
   - Primero se evalúan subsistemas de bajo nivel (ej.: validación de inputs) y luego su impacto en sistemas mayores (*IS3 - Clase 8, pág. 34-35*).

Ejemplo:
Un control de "revisión gerencial de ventas" puede tener efectividad *Media* para evitar precios incorrectos (*IS3 - Clase 8, pág. 33*).

Nota: Todo el procedimiento y ejemplos están documentados explícitamente en el material.

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

Tipos de riesgos en auditoría de sistemas y su naturaleza:

1. **Riesgo Inherente (RI)**
   - *Naturaleza:* Probabilidad de que existan errores materiales o fraudes *antes* de considerar los controles internos.
   - *Ejemplo:* Sistemas financieros tienen alto RI por ser blancos comunes de fraude (*IS3 - Clase 8, pág. 40, 45*).
2. **Riesgo de Control (RC)**
   - *Naturaleza:* Probabilidad de que los controles internos *no* prevengan, detecten o corrijan errores.
   - *Ejemplo:* Controles débiles en validación de datos aumentan el RC (*IS3 - Clase 8, pág. 41, 49*).
3. **Riesgo de Detección (RD)**
   - *Naturaleza:* Probabilidad de que los procedimientos del auditor *no* identifiquen errores materiales.
   - *Ejemplo:* Muestreo insuficiente en pruebas de auditoría (*IS3 - Clase 8, pág. 41, 52*).
4. **Riesgo Deseado de Auditoría (RDA)**
   - *Naturaleza:* Nivel máximo de riesgo aceptable que el auditor está dispuesto a asumir.
   - *Ejemplo:* Auditoría de sistemas críticos con RDA bajo (*IS3 - Clase 8, pág. 39-40*).

Fórmula clave:

$$\text{RDA} = \text{RI} \times \text{RC} \times \text{RD}$$

(IS3 - Clase 8, pág. 39).

Nota: Todos los conceptos y ejemplos están documentados explícitamente en el material.

Parte III: Proceso de Auditoría

15. Explique brevemente el proceso de auditoría.

El proceso incluye:

1. **Planificación**: se definen alcance, riesgos y se recolecta información del cliente.
2. **Recolección de evidencia**: se usan procedimientos y testeos.
3. **Testeo de controles**: se verifica si los controles operan efectivamente.
4. **Testeos substantivos**: se analiza si hay errores o pérdidas.
5. **Evaluación final**: se formula una opinión en un informe.

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

- **Comprensión de controles**: entrevistas, observación, inspecciones.

- **Testeo de controles**: se verifica si los controles funcionan correctamente.
- **Detalle de transacciones**: detectar errores o irregularidades en transacciones.
- **Detalle de balances contables**: verificar registros contables finales.
- **Revisión analítica**: analizar relaciones entre datos para identificar áreas riesgosas

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

- **Testeo de controles**: se aplica si se espera que los controles sean efectivos.
- **Testeo de transacciones**: para ver si errores o irregularidades generan pérdidas.
- **Testeo de resultados generales**: para emitir juicio sobre salvaguarda de activos, integridad de datos y eficiencia. Es el más costoso.

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

La planificación es la primera etapa del proceso de auditoría. Involucra definir qué se va a auditar y cómo se va a realizar. Las tareas principales son:

1. **Determinar el alcance**: puede ser un sistema, un conjunto de sistemas o un área de tecnología informática.
2. **Emitir una opinión sobre el Riesgo Deseado de Auditoría (RDA)**: el nivel de riesgo que se acepta correr en la auditoría.
3. **Emitir una opinión sobre el Riesgo Inherente (RI)**: se evalúan factores como complejidad del sistema, manejo de efectivo o tecnología utilizada.
4. **Emitir una opinión sobre el Riesgo de Control (RC)**: se analizan los controles internos existentes y su confiabilidad.
5. **Calcular el Riesgo de Detección (RD)** necesario para cumplir con el RDA.
6. **Recolectar evidencia**: mediante entrevistas, revisión de documentación, observación de actividades, etc..
7. **Documentar evidencia**: usando cuestionarios, diagramas de flujo, narrativas, tablas de decisión, herramientas CASE.

Diferencias entre auditoría interna y externa:

Auditoría interna:

- Se enfoca en **eficiencia y eficacia operativa**.
- Le preocupa el **tamaño de las pérdidas por operaciones ineficientes o ineficaces**.
- Etapa de planificación incluye: asignar personal, obtener información del cliente, análisis del negocio, identificar áreas de riesgo.

Auditoría externa:

- Se enfoca en **errores en los estados financieros**.
- Le preocupa el **tamaño de los errores contables**.
- Planificación incluye: investigar nuevos clientes, obtener contrato, asignar personal, obtener información del cliente, análisis del negocio, identificar riesgos.

19. Describa el contenido de un informe de auditoría.

El informe de auditoría se redacta al final del proceso, después de realizar todos los testeos y recolectar la evidencia necesaria. Resume los hallazgos y presenta la **opinión del auditor** sobre el sistema auditado.

Contenido principal:

1. **Grado de pérdidas materiales** o registros incorrectos que podrían ocurrir o han ocurrido.
2. **Evaluación de los controles internos**: si son efectivos o no.
3. **Resultados de los testeos**: testeo de controles, transacciones y resultados generales.
4. **Juicio final del auditor** sobre la capacidad del sistema para:
   - Salvaguardar activos
   - Mantener la integridad de los datos
   - Lograr eficiencia y efectividad

El informe es el **documento formal** que entrega la auditoría y sirve como base para tomar decisiones dentro de la organización.

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

1. **Opinión excusada**: no se puede emitir opinión.
2. **Opinión adversa**: hubo pérdidas materiales o distorsión en los estados.
3. **Opinión con calificación**: hubo pérdidas o errores no considerables.
4. **Opinión sin calificación**: no hay objeciones importantes.

Parte IV: Gobernanza de TI

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

La Gobernanza de TI es un subconjunto de la gobernanza corporativa que se enfoca en la dirección y control del uso de las tecnologías de la información para cumplir con los objetivos empresariales. Su propósito es asegurar que las inversiones en TI generen valor, mitiguen los riesgos y se alineen con las estrategias organizacionales .

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

COBIT (Control Objectives for Information and Related Technologies) es un conjunto de recursos que ayudan a las organizaciones a adoptar un marco de gobernanza y control de TI. Fue creado por ISACA y el

Instituto de Gobernanza de TI.

Sus elementos son:

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.

La **Gobernanza de TI** se enfoca en **quién toma las decisiones de TI**, quién tiene la autoridad, la información y la responsabilidad para hacerlo.

La **Administración de TI** se enfoca en **tomar e implementar** esas decisiones.

24. ¿Cuáles son los principios de COBIT?

Los cinco principios de COBIT 5 (ahora COBIT 2019) son:

1. **Satisfacer las necesidades de las partes interesadas**:
   Busca crear valor mediante beneficios, uso óptimo de recursos y gestión de riesgos. Las necesidades se traducen en metas empresariales, metas de TI y metas de habilitadores.
2. **Cubrir la empresa de extremo a extremo**:
   Incluye todos los sistemas de gobernanza y administración de TI, internos y externos, aplicables a toda la organización.
3. **Aplicar un marco integrado**:
   COBIT se alinea con otros marcos y estándares, y sirve como marco general para la gobernanza y administración de TI.
4. **Habilitar un enfoque holístico**:
   Considera todos los factores que influyen en la gobernanza de TI. Define siete habilitadores: principios, procesos, estructuras, cultura, información, infraestructura y personas.
5. **Separar las funciones principales**:
   Distingue entre gobernanza (evalúa, dirige y monitorea) y administración (planifica, ejecuta y controla actividades).

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

COBIT organiza los procesos de TI en dos grandes grupos:

1. **Gobernanza**:
   Incluye 5 procesos bajo el dominio **EDM (Evaluar, Dirigir y Monitorear)**.

2. **Administración**:
   Incluye 32 procesos divididos en 4 dominios:
   - **APO**: Alinear, Planear y Organizar
   - **BAI**: Construir, Adquirir e Implementar
   - **DSS**: Entrega, Servicio y Soporte
   - **MEA**: Monitorear y Evaluar

26. Explique cómo COBIT clasifica la administración de TI.

COBIT clasifica la Administración de TI en estos 4 dominios, cada uno con un enfoque específico:

1. **APO – Alinear, Planear y Organizar**:
   Define cómo TI puede contribuir a los objetivos del negocio. Incluye la gestión de estrategias, arquitectura, innovación, presupuesto, riesgos, seguridad, proveedores, calidad, entre otros.
2. **BAI – Construir, Adquirir e Implementar**:
   Abarca el desarrollo o adquisición de soluciones de TI y su implementación. Se ocupa de programas y proyectos, definición de requerimientos, cambios organizacionales, activos y configuración.
3. **DSS – Entrega, Servicio y Soporte**:
   Garantiza que los servicios de TI funcionen correctamente. Incluye operaciones, gestión de incidentes, continuidad del servicio, seguridad y soporte al usuario.
4. **MEA – Monitorear y Evaluar**:
   Evalúa regularmente los procesos de TI. Se enfoca en el desempeño, cumplimiento de normas y controles internos.

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

La importancia de aplicar COBIT en una organización radica en que:

1. **Alinea TI con los objetivos del negocio**: Proporciona un marco para asegurar que las inversiones en TI generen valor y estén alineadas con la estrategia empresarial (págs. 3, 19).
2. **Gestiona riesgos y recursos**: Optimiza el uso de recursos y mitiga riesgos asociados a TI, asegurando un control efectivo (págs. 3, 17).

Ejemplos:

- En el **Gobierno de Dubai**, COBIT mejoró la gobernanza de TI y los controles (pág. 51).
- En la **Oficina de Servicios Civiles de Bahréin**, redujo riesgos y fortaleció la infraestructura de TI (pág. 51).