



Facultad de
INFORMÁTICA



UNIVERSIDAD
NACIONAL
DE LA PLATA

AUDITORÍA DE SISTEMAS – PROCEDIMIENTOS, TAREAS, INFORME

ELSA ESTEVEZ

ecestevez@gmail.com

RAZONES PARA CONTROLAR

- 1) Hacking
- 2) virus
- 3) acceso físico ilegal
- 4) abuso de privilegios

Costos por abusos computacionales

- 1) pérdida de vida humana,
- 2) privación de libertad,
- 3) daño al medio ambiente.

Costos por errores de computación

- 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?

Valor de hardware, software y personal

Costos por toma de decisiones incorrectas

Ejemplo: cálculo de amortización erróneo en un bien de poco valor.

Evolución controlada de TI

Las consecuencias de usar sistemas no confiables puede ser catastrófica.

Costos por pérdida de datos

Pérdida de cuentas corrientes, pérdida de los datos de los alumnos

Mantenimiento de privacidad

Muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia.



AUDITORÍA DE SISTEMAS DE INFORMACIÓN

AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Definición:

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

- 1) el sistema automático preserva los activos,
- 2) mantiene la integridad de los datos,
- 3) permite que los objetivos organizacionales se alcancen con eficacia,
- 4) usa los recursos con eficiencia.

CONTROL DE EVENTOS ILEGALES

TIPOS DE CONTROLES

Control Preventivo: instrucciones de cómo completar un formulario.

Nota: las instrucciones no son el control.

Control Detectivo: un programa que valida datos de input, rechazando los erróneos.

Control Correctivo: un programa que detecta el ruido en comunicaciones y permite corregir datos corruptos.

DEFINICIÓN DE RIESGO

Definición

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

$$RDA = RI * RC * RD$$

RDA: Riesgo Deseado de Auditoría

RI: Riesgo Inherente

RC: Riesgo de Control

RD: Riesgo de Detección

OBJETIVO Y AGENDA

OBJETIVO

Explicar el proceso de una auditoría de sistemas de información.

AGENDA

1	PROCEDIMIENTOS	¿Qué tipos de procedimientos se realizan?
2	TAREAS	¿Cuáles son las tareas de un proceso de auditoría?
3	INFORME	¿Qué contiene un informe de auditoría?
4	RESUMEN	¿Qué se cubrió en esta sesión?

PROCEDIMIENTOS DE UNA AUDITORÍA

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

- 1) determinar si ocurrieron pérdidas materiales o la información financiera es errónea
- 2) determinar la eficiencia y eficacia de las operaciones

PROCEDIMIENTOS DE UNA AUDITORÍA

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

- 1) **determinar si ocurrieron pérdidas materiales o la información financiera es errónea**
- 2) **determinar la eficiencia y eficacia de las operaciones**

PÉRDIDA O INFORMACIÓN ERRÓNEA

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

- 1) procedimientos para comprender los controles
- 2) testeo de controles
- 3) testeos substantivos de detalle de transacciones
- 4) testeos substantivos de detalle de balances contables
- 5) procedimientos de revisión analítica

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.

2 - TESTEO DE CONTROLES

Son para evaluar si los controles están actuando efectivamente.

Ejemplos:

- 1) cuestionarios
- 2) inspecciones
- 3) observaciones
- 4) reprocesos

3 - 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

4 - DETALLE DE BALANCES CONTABLES

Los tests substantivos de detalle de balances contables se focalizan en los registros contables finales, en el balance.

Ejemplo: se puede circularizar a una muestra de clientes para controlar que los saldos registrados sean correctos.

5 - 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.

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.

PROCEDIMIENTOS DE UNA AUDITORÍA

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

- 1) determinar si ocurrieron pérdidas materiales o la información financiera es errónea
- 2) **determinar la eficiencia y eficacia de las operaciones**

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.

OBJETIVO Y AGENDA

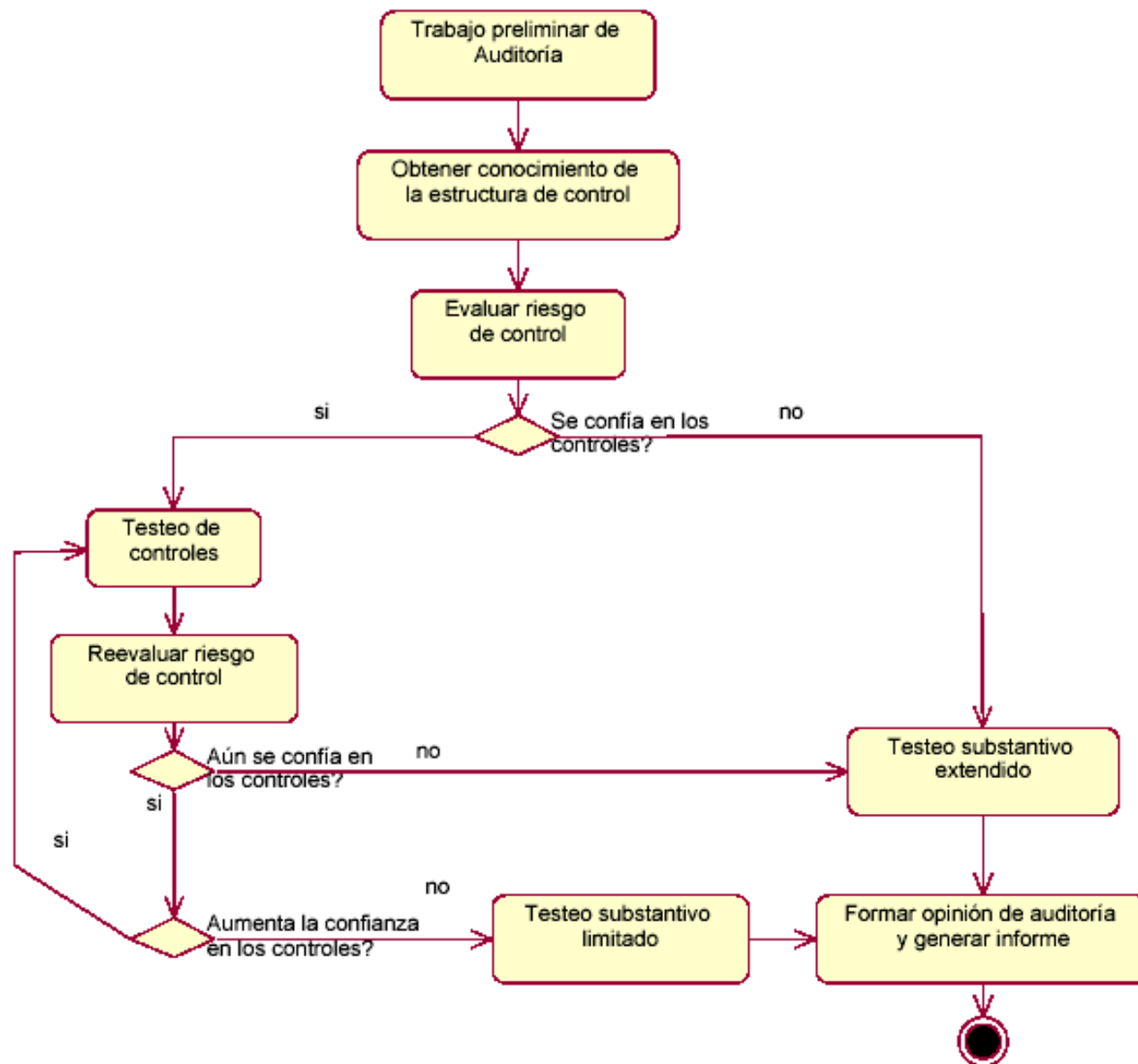
OBJETIVO

Explicar el proceso de una auditoría de sistemas de información.

AGENDA

1	PROCEDIMIENTOS	¿Qué tipos de procedimientos se realizan?
2	TAREAS	¿Cuáles son las tareas de un proceso de auditoría?
3	INFORME	¿Qué contiene un informe de auditoría?
4	RESUMEN	¿Qué se cubrió en esta sesión?

PASOS DE UNA AUDITORÍA



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:

- 1) auditoría interna
- 2) auditoría externa

AUDITORÍA INTERNA

La etapa de planificación incluye:

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

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

AUDITORÍA EXTERNA

La etapa de planificación incluye:

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

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

TAREAS DE PLANIFICACIÓN (TP)

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

TP 1- ALCANCE DE LA AUDITORÍA

Determinar qué se va a auditar:

- 1) un sistema
- 2) un conjunto de sistemas
- 3) un área del tecnología informática

TP 2 - OPINIÓN DE RDA

Se emite un RDA en general para toda la tarea de auditoría.

TP 3 - OPINIÓN SOBRE 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.

TP 4 - OPINIÓN SOBRE 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:

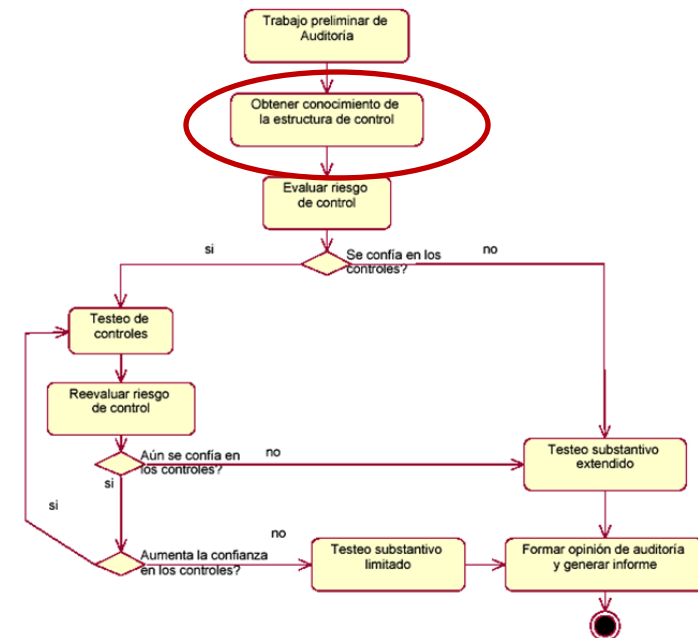
- 1) controles de entorno
- 2) evaluación de riesgo
- 3) actividades de control
- 4) información y comunicación
- 5) monitoreo

TP 4 - 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...



TP 4 - 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

TP 4 - 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.

TP 4 - 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.

TP 4 - 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

TP 4 - 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.

TP 4 - EJEMPLO DE CONTROLES

Controles Internos	Implementación
Actividades de Control	Procedimiento para instalar programas en producción (control gerencial)
Controles de Entorno y Evaluación de Riesgos	Existencia de comité de seguimiento de proyectos (control gerencial)
Información y Comunicación	Procedimiento para comunicar información (control gerencial) Procedimiento para capturar, registrar y procesar transacciones (control de aplicación)
Monitoreo	Procedimiento para medir la productividad del personal (control gerencial)

TP 5 - CALCULAR EL RD

Calcular el RD que se debe lograr para cumplir con el RDA

TP 6 - RECOLECTAR EVIDENCIAS

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

TP 7 - DOCUMENTAR EVIDENCIAS

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.

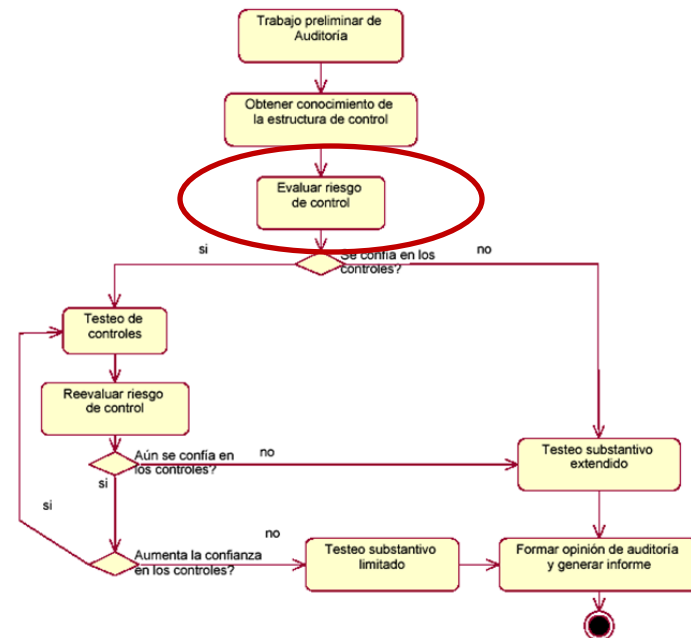
Finalmente se debe evaluar el riesgo.

EVALUACIÓN DE RIESGO DE CONTROL – 1

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 sustantivo.



EVALUACIÓN DE RIESGO DE CONTROL – 2

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.

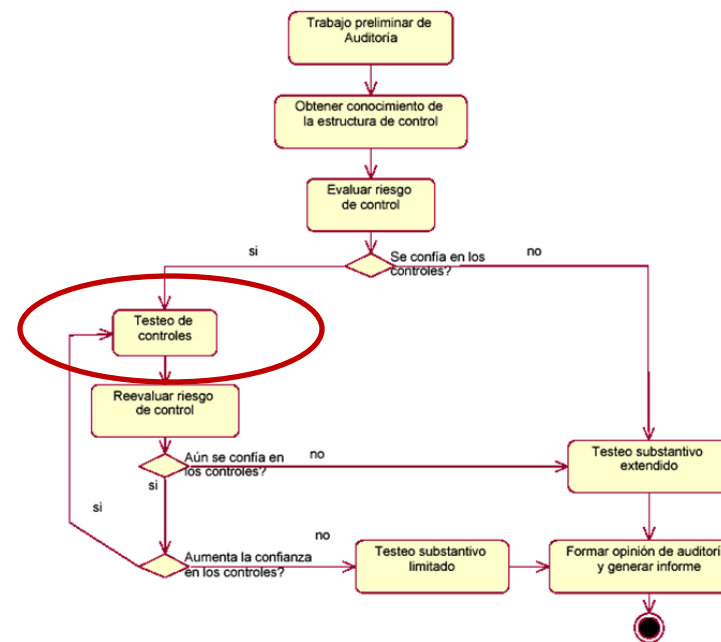
TESTEO DE CONTROLES - 1

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

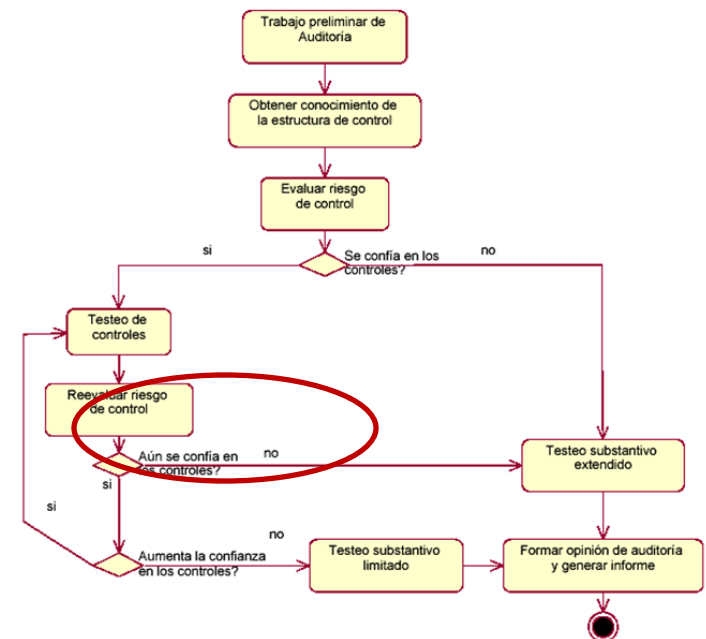
Luego de evaluados los controles, se vuelve a estimar el riesgo.

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.

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.

OBJETIVO Y AGENDA

OBJETIVO

Explicar el proceso de una auditoría de sistemas de información.

AGENDA

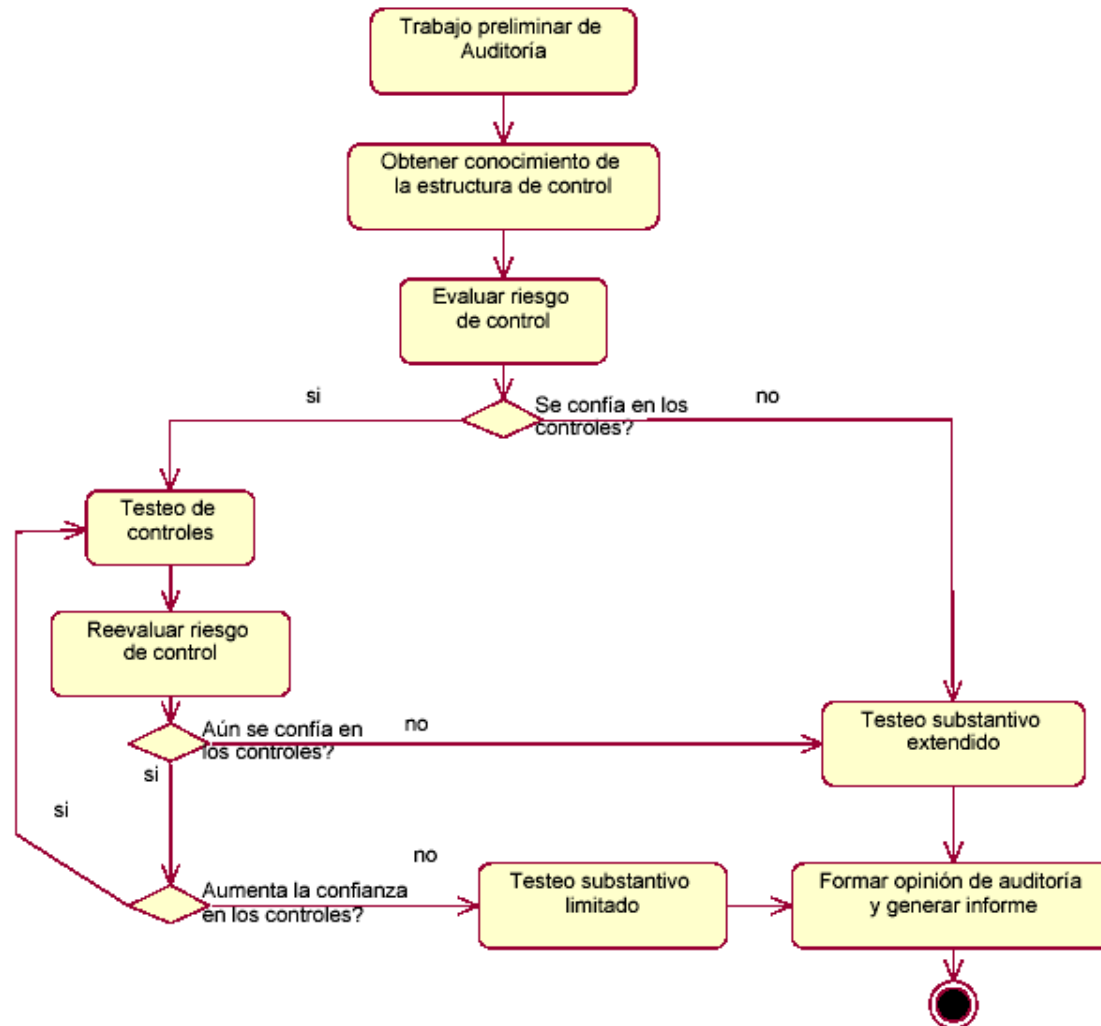
1	PROCEDIMIENTOS	¿Qué tipos de procedimientos se realizan?
2	TAREAS	¿Cuáles son las tareas de un proceso de auditoría?
3	INFORME	¿Qué contiene un informe de auditoría?
4	RESUMEN	¿Qué se cubrió en esta sesión?

OPINIONES DE AUDITORÍA

Los estándares en varios países requieren que la opinión sea:

- 1) **opinión excusada**: en base al trabajo realizado no se puede emitir opinión.
- 2) **opinión adversa**: se concluye que han ocurrido pérdidas materiales o que los estados financieros están distorsionados.
- 3) **opinión con calificación**: se concluye que han ocurrido pérdidas materiales o existen registros incorrectos, pero las cantidades no son considerables.
- 4) **opinión sin calificación**: el auditor considera que no han ocurrido pérdidas materiales o no existen registros incorrectos.

PASOS DE UNA AUDITORÍA



OBJETIVO Y AGENDA

OBJETIVO

Explicar el proceso de una auditoría de sistemas de información.

AGENDA

1	PROCEDIMIENTOS	¿Qué tipos de procedimientos se realizan?
2	TAREAS	¿Cuáles son las tareas de un proceso de auditoría?
3	INFORME	¿Qué contiene un informe de auditoría?
4	RESUMEN	¿Qué se cubrió en esta sesión?

RESUMEN – PROCEDIMIENTOS

- 1) procedimientos para comprender los controles
- 2) testeo de controles
- 3) testeos substantivos de detalle de transacciones
- 4) testeos substantivos de detalle de balances contables
- 5) procedimientos de revisión analítica

RESUMEN – 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.

RESUMEN – OPINIÓN DE AUDITORÍA

- 1) **opinión excusada** - en base al trabajo realizado no se puede emitir opinión.
- 2) **opinión adversa** - se concluye que han ocurrido pérdidas materiales o que los estados financieros están distorsionados.
- 3) **opinión con calificación** - se concluye que han ocurrido pérdidas materiales o existen registros incorrectos, pero las cantidades no son considerables.
- 4) **opinión sin calificación** - el auditor considera que no han ocurrido pérdidas materiales o no existen registros incorrectos.

BIBLIOGRAFÍA Y MATERIAL DE LECTURA

BIBLIOGRAFÍA

Information Systems Audit and Control – Ron Weber – capítulo 2

BIBLIOGRAFÍA ADICIONAL

Information Technology Control and Audit (third edition) – Sandra Senft, Frederick Gallegos – capítulos 3 y 4

Muchas gracias!

Elsa Estevez
ecestevez@gmail.com
www.elsaestevez.com