Facultad de INFORMÁTICA

UNIVERSIDAD NACIONAL DE LA PLATA

AUDITORÍA DE SISTEMAS – CONTROLES Y RIESGOS

ELSA ESTEVEZ
ecestevez@gmail.com

OBJETIVO Y AGENDA

OBJETIVO

Explicar conceptos de controles y riesgos de auditoría.

AGENDA

1	CONTROLES	¿Cuáles son los controles de sistemas?
2	RIESGOS	¿Cuáles son los riesgos de una auditoría?
3	RESUMEN	¿Qué se cubrió en esta sesión?

MOTIVACIÓN

Felicitaciones!!! Lo han designado Gerente del Departamento de Auditoría de la Empresa “X”.

La empresa posee:

- 520 programadores y analistas
- 1245 PC’s conectadas en red
- 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

Definición.

Un control es un sistema que previene, detecta, o corrige eventos ilegales.

Hay tres aspectos claves en esta definición:

1) un control es un sistema

2) eventos ilegales

3) los controles son usados para prevenir, detectar o corregir eventos ilegales.

UN CONTROL ES UN SISTEMA

Una password, ¿es un control ?

Habitualmente, tendemos a nombrar los controles, teniendo en cuenta sólo un aspecto del control.

Una password se convierte en control, sólo en el contexto de un sistema que asegure:

1) seguridad para elegir passwords,
2) correcta validación de passwords,
3) almacenamiento seguro de las passwords,
4) seguimiento en el uso indebido de passwords
5) ...

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.

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.

OBJETIVO DE LA AUDITORÍA

Reducir las pérdidas esperadas por eventos ilegales mediante:

1) controles preventivos: reducen la probabilidad que estos eventos ocurran.

2) controles detectivos y correctivos: reducen la cantidad de pérdidas cuando los eventos ilegales ocurren.

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

¿CÓMO ADMINISTRAR LA COMPLEJIDAD?

Para administrar la complejidad, se sugiere:

1) factorizar el sistema en subsistemas

2) determinar la confiabilidad de cada subsistema, y las implicancias de cada uno de ellos en el nivel de confiabilidad general del sistema.

FACTORIZACIÓN

El primer paso para comprender un sistema complejo es particionarlo en subsistemas.

Un subsistema es un componente de un sistema que:

1) realiza ciertas funciones básicas necesarias para el sistema en general,
2) le permite atender sus objetivos fundamentales.

Los subsistemas son componentes lógicas y no físicas.

El proceso de particionar en subsistemas se denomina factorización.

CÓMO FACTORIZAR

Para poder factorizar, se necesita un criterio.

Criterio: La esencia de un subsistema es la función que realiza.

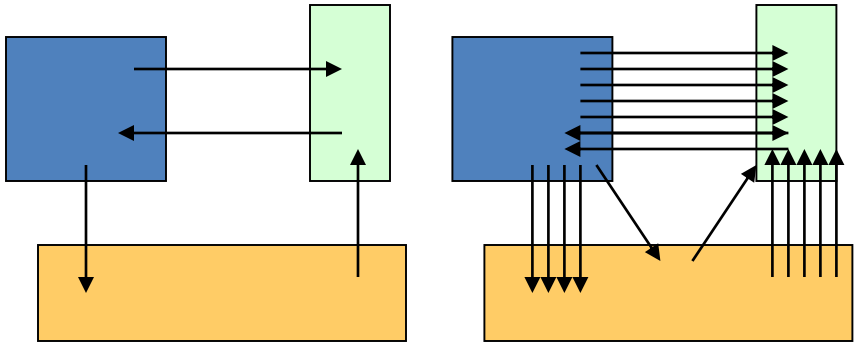
Los auditores deben identificar primero, las principales funciones que el sistema realiza para cumplir sus objetivos.

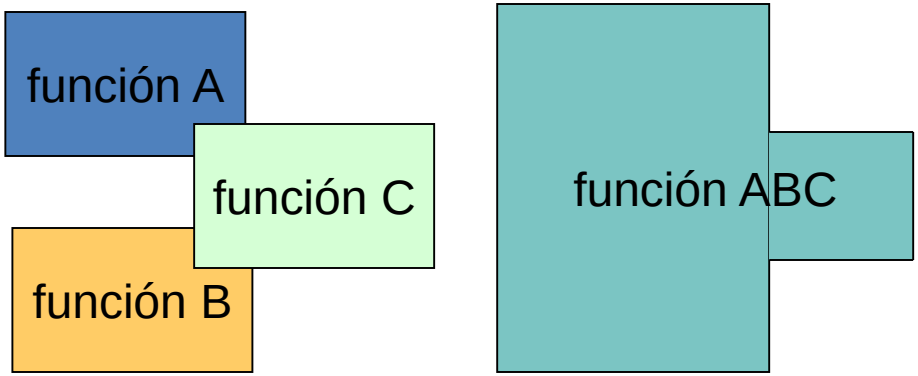
El proceso de factorización termina cuando se ha particionado el sistema en partes lo suficientemente pequeñas, de tal modo que puedan ser entendidas y evaluadas.

OTRO CRITERIO DE FACTORIZACIÓN

Además de las funciones, existen otras dos guías:

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





FORMAS DE FACTORIZACIÓN

1) funciones gerenciales - las funciones que se deben realizar para asegurar que el desarrollo, la implementación, operación y mantenimiento de los sistemas de información proceden de una forma planificada y controlada.

2) funciones de aplicación - tareas que son necesarias ejecutar para realizar un procesamiento de información confiable. Relacionado con “ciclos”.

EN BASE A FUNCIONES GERENCIALES – 1

Subsistema Gerencial	Descripción
Alta gerencia	Debe asegurar que las funciones de los SI estén bien administradas. Decisiones de políticas a largo plazo de cómo serán usados los SI.
Gerencia de Sistemas de Información	Responsabilidad general de planificar y controlar todas las actividades de los SI. Aconseja a la alta gerencia de las decisiones políticas de largo plazo y las traduce en metas y objetivos de corto plazo.

EN BASE A FUNCIONES GERENCIALES – 2

Subsistema Gerencial	Descripción
Gerencia de Desarrollo de Sistemas	Responsable del diseño, implementación y mantenimiento de los sistemas.
Gerencia de Programación	Responsable de la programación de nuevos sistemas, mantenimiento de los viejos y soporte general.
Administración de Datos	Responsable de lograr los objetivos de planificación y control en relación al uso de los datos de la organización.

EN BASE A FUNCIONES GERENCIALES – 3

Subsistema Gerencial	Descripción
Gerencia de Aseguramiento de Calidad	Responsable de asegurar que el desarrollo, operación y mantenimiento de los sistemas es conforme a los estándares de calidad establecidos.
Administración de Seguridad	Responsable por los controles de acceso y seguridad física de las funciones de los SI.
Gerencia de Operaciones	Responsable de la planificación y control de las operaciones diarias.

EN BASE A FUNCIONES DE APLICACIÓN - 1

Los sistemas de información que soportan una organización, se dividen en ciclos.

Los ciclos varían de acuerdo al tipo de organización: industria, entidad financiera, etc.

En general incluyen:

1) ventas y cobranzas,
2) administración de personal, sueldos y jornales,
3) compras y pagos,
4) producción, inventario y almacenaje,
5) tesorería (contabilidad).

EN BASE A FUNCIONES DE APLICACIÓN - 2

Cada ciclo es factorizado en uno o más sistemas de aplicación.

Ejemplo: Ventas puede subdividirse en:

1) administración de clientes
2) captura de pedidos
3) facturación

El conjunto de subsistemas de aplicación incluyen lo siguiente:

EN BASE A FUNCIONES DE APLICACIÓN - 3

Subsistema de Aplicación	Descripción
Limítrofe	Componentes que establecen las interfaces entre el usuario y el sistema.
Input	Componentes que capturan, preparan e ingresan comandos y datos al sistema.
Comunicaciones	Componentes que transmiten datos entre los subsistemas y sistemas.

EN BASE A FUNCIONES DE APLICACIÓN - 4

Subsistema de Aplicación	Descripción
Procesamiento	Componentes que realizan toma de decisiones, cálculos, clasificación, ordenamiento y sumarización de datos dentro del sistema.
Base de Datos	Componentes que definen, agregan, acceden, modifican o eliminan datos.
Output	Componentes que buscan y presentan los datos al usuario.

CONFIABILIDAD DE SUBSISTEMAS

Primero - determinar el menor nivel de los subsistemas.

Segundo - evaluar la confiabilidad de los controles en cada subsistema.

CONFIABILIDAD DE CONTROLES

Para evaluar la confiabilidad de los controles:

1) se deben identificar todos los posibles tipos de eventos que pueden ocurrir en el subsistema.

2) se deben considerar todos los eventos válidos o ilegales.

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

CONSIDERAR LAS PRINCIPALES FUNCIONES

Para cada función:

1) analizar cómo debería realizarse
2) evaluar cómo el subsistema cumple con esa visión normativa.

Para determinar si un evento es legal o ilegal se deben considerar las transacciones que pueden ocurrir como input al subsistema.

Todos los eventos en un sistema de aplicación deben surgir de una transacción.

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.

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.

CONFIABILIDAD DE LOS CONTROLES - 2

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.

CONFIABILIDAD DE LOS CONTROLES - EJEMPLO

Controles / Errores-Irregular.	Clte.no autoriz	Térms/Cr. No autoriz	Cantidad Incorrecta	Precio Incorr.	Proces. Tardío
Operador bien entrenado	M	M	M	M	M
Interface amigable			M	M	M
Pgm.input alta calidad	A	A	A	A	
Revisión gerencial de ventas	M	M	B	M	
Reporte diario de órdens no cumpl.					A
Revisión gerencial volum.trans.diarias					M

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

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.

ESTIMAR LA CONFIABILIDAD – PASOS

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 más 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.

OBJETIVO Y AGENDA

OBJETIVO

Explicar conceptos de controles y riesgos de auditoría.

AGENDA

1	CONTROLES	¿Cuáles son los controles de sistemas?
2	RIESGOS	¿Cuáles son los riesgos de una auditoría?
3	RESUMEN	¿Qué se cubrió en esta sesión?

RIESGOS DE LA AUDITORÍA

Recordemos los objetivos de la auditoría:

1) salvaguardar activos
2) asegurar integridad de los datos
3) asegurar que los sistemas son efectivos
4) asegurar que los sistemas son eficaces

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

Para esto, se debe medir, y se podría fallar al detectar las pérdidas materiales reales o potenciales.

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

TIPO DE RIESGOS – 1

1) Riesgo Deseado: el riesgo que se desea correr.

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

TIPO DE RIESGOS – 2

3) Riesgo de Control: refleja la probabilidad que en algún segmento de la auditoría, los controles internos no prevengan, detecten o corrijan pérdidas materiales o imputaciones erróneas que puedan surgir.

4) Riesgo de Detección: refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas.

1) RIESGO DESEADO PARA UNA AUDITORÍA

Primero los auditores eligen el nivel de RDA.

Evalúan las consecuencias de fracasar en detectar las pérdidas materiales reales o potenciales.

2) RIESGO INHERENTE DE SISTEMAS

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?)

2) RIESGO INHERENTE DE SISTEMAS - ¿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

2) RIESGO INHERENTE DE SISTEMAS - FINANCIEROS

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

2) RIESGO INHERENTE DE SISTEMAS - ESTRATÉGICOS

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

2) RIESGO INHERENTE DE SISTEMAS - CRÍTICOS

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.

2) RIESGO INHERENTE DE SISTEMAS - AVANZADOS

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.

3) RIESGO DE CONTROL

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

CONTROLES GERENCIALES - 2

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.

4) RIESGO DETECCIÓN

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.

OBJETIVO Y AGENDA

OBJETIVO

Explicar conceptos de controles y riesgos de auditoría.

AGENDA

1	CONTROLES	¿Cuáles son los controles de sistemas?
2	RIESGOS	¿Cuáles son los riesgos de una auditoría?
3	RESUMEN	¿Qué se cubrió en esta sesión?

RESUMEN 1 – CONTROLES Y FACTORIZACIÓN

Un control es un sistema que previene, detecta y corrige eventos ilegales.

Para realizar una auditoría se debe factorizar en subsistemas:

1) funciones gerenciales
2) funciones de aplicación

Otro criterio para factorizar es considerar subsistemas que presenten mínimo acoplamiento y máxima cohesión.

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

RESUMEN 2 – EVALUAR CONFIABILIDAD 1

Se deben evaluar los eventos.

Para identificar eventos, se consideran las principales funciones del sistema.

Para cada función se debe:

1) definir cómo debería realizarse
2) cómo el sistema cumple con esa función

RESUMEN 3 – EVALUAR CONFIABILIDAD 2

Cuando ocurre un evento el sistema recibe una 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.

RESUMEN 4 – RIESGOS

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

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 2 y 3

Muchas gracias!

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