Facultad de
INFORMÁTICA

UNIVERSIDAD
NACIONAL
DE LA PLATA

AUDITORÍA DE SISTEMAS – MOTIVACIÓN Y CONCEPTOS

Ariel Pasini
apasini@lidi.info.unlp.edu.ar

OBJETIVO Y AGENDA

OBJETIVO

Explicar las motivaciones para auditar sistemas de información y el concepto de auditoría de sistemas de información.

AGENDA

1	MOTIVACIÓN	¿Cuáles son las razones para auditar sistemas?
2	AUDITORÍA	¿Qué significa una auditoría de sistemas?
3	RESUMEN	¿Qué se cubrió en esta sesión?

RAZONES PARA CONTROLAR

Costos por errores de computación

Costos por abusos computacionales

Valor de hardware, software y personal

Costos por toma de decisiones incorrectas

Evolución controlada de TI

Costos por pérdida de datos

Mantenimiento de privacidad

AUDITORÏA DE SISTEMAS DE INFORMACIÓN

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.

Ejemplo: pérdida de cuentas corrientes, pérdida de los datos de los alumnos,

¿Por qué se producen?

COSTOS POR DECISIONES INCORRECTAS 1

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.

COSTOS POR DECISIONES INCORRECTAS 2

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.

COSTOS POR DECISIONES INCORRECTAS 3

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 DECISIONES INCORRECTAS - EJEMPLO

Dinero: Knight Capital

En agosto de 2012, un error de programa casi provocó la quiebra de la empresa de inversión Knight Capital. La compañía perdió 500 millones de dólares en media hora debido a que sus computadoras comenzaron a comprar y vender millones de acciones sin ningún tipo de control humano. Como resultado, el precio de las acciones de Knight Capital cayó un 75% en dos días, informa el portal popmech.ru.

Ref:[https://actualidad.rt.com/actualidad/view/138158-catastrofes-programacion-culpa-software-computadora]

COSTOS POR ABUSO COMPUTACIONAL

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:

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

1) 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.

GMAIL ESTÁ FUERA DE SERVICIO POR UNAS HORAS

Noticias Seguridad | February 2, 2016 | Incidentes | No Comments

Conocimiento pertenece al mundo

Aunque no parece tratarse de un fallo generalizado, algunos usuarios están reportando problemas con una **caída de Gmail** en diferentes partes del mundo. Los servicios de Google Drive y YouTube también parecen haberse visto afectados por los problemas.

Tal y como podemos leer en el diario inglésIndependent.co.uk, el correo electrónico de **Gmail no funciona** correctamente para algunos usuarios.

El problema parece residir en un error en la conexión con los servidores de Google, lo que impide que el correo electrónico se pueda actualizar correctamente. Este problema se ha detectado tanto en la versión escritorio como en la aplicación móvil de Gmail. YouTube y Google Drive también se han visto afectados, aunque en menor medida.

[Ref: http://noticiasseguridad.com/hacking-incidentes/gmail-esta-fuera-de-servicio-por-unas-horas/]

2) 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].

Estos son los nueve virus más peligrosos para iPhone y Mac

La creencia de que no existen programas informáticos malignos para los sistemas de Apple es un "mito", afirman los expertos

Desde hace años circula la creencia de que no existen virus informáticos para los sistemas operativos de Apple. Hoy los expertos quieren desmitificar con cifras esta leyenda. Desde 2012 hasta ahora se ha cuadruplicado el número de estos programas malignos: se ha pasado de 500, hace cuatro años, a 2.200 en 2015, según los datos que ha recabado la empresa de seguridad informática Panda Security. Estos virus afectan tanto a la versión móvil de iOS como a los ordenadores Mac OS. "El mito de que no hay virus para Mac es historia. Sólo en 2015 hemos detectado el doble de *malware* para estos sistemas que el que detectamos en 2014", explica Luis Corrons, director de Panda Labs.

[Ref: http://tecnologia.elpais.com/tecnologia/2016/10/20/actualidad/1476957274_848801.html]

3) 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

> [entrevista a Felipe Alcántara, Subdirector General de Seguridad Corporativa de Telefónica]
>
> – ¿Tiene Telefónica muchos empleados trabajando en seguridad de la información?… tres de cada cien…
>
> …La Dirección General Adjunta de Seguridad Corporativa, tiene bajo su responsabilidad la defensa patrimonial de Telefónica: protección de personas, bienes, servicios y prevención del fraude… tiene en su estructura las áreas relacionadas con la vigilancia y protección de edificios y personas, los sistemas electrónicos, la seguridad de los sistemas de información y la prevención del fraude...

[http://www.revistasic.com Seguridad en Informática y Comunicaciones - 06/2005]

4) 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.

Minimum of 3 Months Suspension
"Lending" an account or online disk storage to another person.
Using an account or online disk storage that belongs to another person

Minimum of 6 Months Suspension
Using a stolen account

Minimum of 1 Year Suspension
A pattern of any misuse of computing resources

[http://www.uic.edu/depts/accc/policies/

Univeristy of Illinois – Chicago. Academic Computing and Communications Center]

CONSECUENCIAS DE ABUSOS

1) Destrucción de activos. Ejemplo?
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

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.

COSTOS POR ERRORES DE COMPUTACIóN - EJEMPLO

Medicina: radioterapia

Un error de programación de la unidad de control de la máquina de radioterapia Therac-25 causó entre 1985 y 1987 al menos seis accidentes en los que los pacientes recibieron sobredosis masivas de radiación. Al menos tres de estos pacientes fallecieron como consecuencia directa del exceso de radiación. Los expertos creen que el fallo fue causado por un error en el código que obligó al programa a realizar la misma acción varias veces.

[Ref: https://actualidad.rt.com/actualidad/view/138158-catastrofes-programacion-culpa-software-computadora]

VALOR DE HW, SW Y 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?

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.

EVOLUCIóN CONTROLADA DEL USO

Se argumenta que la confiabilidad de los sistemas computarizados complejos no está garantizada.

Las consecuencias de usar sistemas no confiables puede 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.

TRABAJO GRUPAL

Identificar un problema relacionado con sistemas informáticos que hayan afectado activos de una organización o la seguridad física de los usuarios.

Explique:

- el problema
- los activos afectados
- formas de prevención del problema

OBJETIVO Y AGENDA

OBJETIVO

Explicar las motivaciones para auditar sistemas de información y el concepto de auditoría de sistemas de información.

AGENDA

1	MOTIVACIÓN	¿Cuáles son las razones para auditar sistemas?
2	AUDITORÍA	¿Qué significa una auditoría de sistemas?
3	RESUMEN	¿Qué se cubrió en esta sesión?

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.

OTROS OBJETIVOS

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

IMPACTO DE LA AUDITORÍA EN SI

AUDITORIA DE SISTEMAS DE INFORMACIÓN

- Mejora la salvaguarda de activos
- Mejora la integridad de los datos
- Mejora la efectividad de los sistemas
- Mejora la eficiencia de los sistemas

SALVAGUARDA DE ACTIVOS

Los activos de los SI incluyen:

- hardware
- software
- facilidades
- personas (conocimientos)
- archivos de datos
- documentación de sistemas
- insumos

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 LOS DATOS

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

EFECTIVIDAD DE LOS SISTEMAS

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.

EFICIENCIA DE LOS SISTEMAS

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 sólo sistema.

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

LOGRO DE OBJETIVOS

Los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un sistema de control interno.

SISTEMA DE CONTROL INTERNO 1

Un sistema de control interno incluye:

1) separación de obligaciones,
2) delegación clara de autoridad y responsabilidades,
3) reclutamiento y entrenamiento de personal calificado,
4) sistema de autorizaciones,
5) documentos y registros adecuados,
6) control físico y documentación sobre los activos,
7) chequeos independientes de performance,
8) comparación periódica de activos con registros contabilizados

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

1) SEPARACIÓN DE OBLIGACIONES

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.

2) DELEGACIÓN

Una delegación clara de autoridad y responsabilidad es esencial tanto en sistemas manuales como automatizados.

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.

RESPONSABILIDAD – PARA PENSAR

Hay un viejo cuento con cuatro personajes. **Todos**, **alguien**, **cualquiera** y **nadie**.

Ocurre que había que hacer un trabajo importante, y **todos** sabían que **alguien** lo haría, **cualquiera** podría haberlo hecho pero **nadie** lo hizo.

Alguien se enojó cuando se enteró, porque le hubiera correspondido a **todos**.

El resultado fué que **todos** creían que lo haría **cualquiera** y **nadie** se dio cuenta de que **alguien** lo haría.

¿Cómo terminó la historia?

Alguien reprochó a **todos** porque en realidad **nadie** hizo lo que hubiera podido hacer **cualquiera**.

RESPONSABILIDAD - ¿DE QUIÉN?

Muchos usuarios desarrollan, modifican y operan sus propias aplicaciones.

3) PERSONAL COMPETENTE Y CONFIABLE

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.

4) SISTEMA DE AUTORIZACIONES

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.

5) DOCUMENTOS Y REGISTROS

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.

6) CONTROL DE ACCESO FÍSICO

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.

7) CHEQUEOS DE PERFORMANCE

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.

8) COMPARACIÓN PERIÓDICA

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.

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.

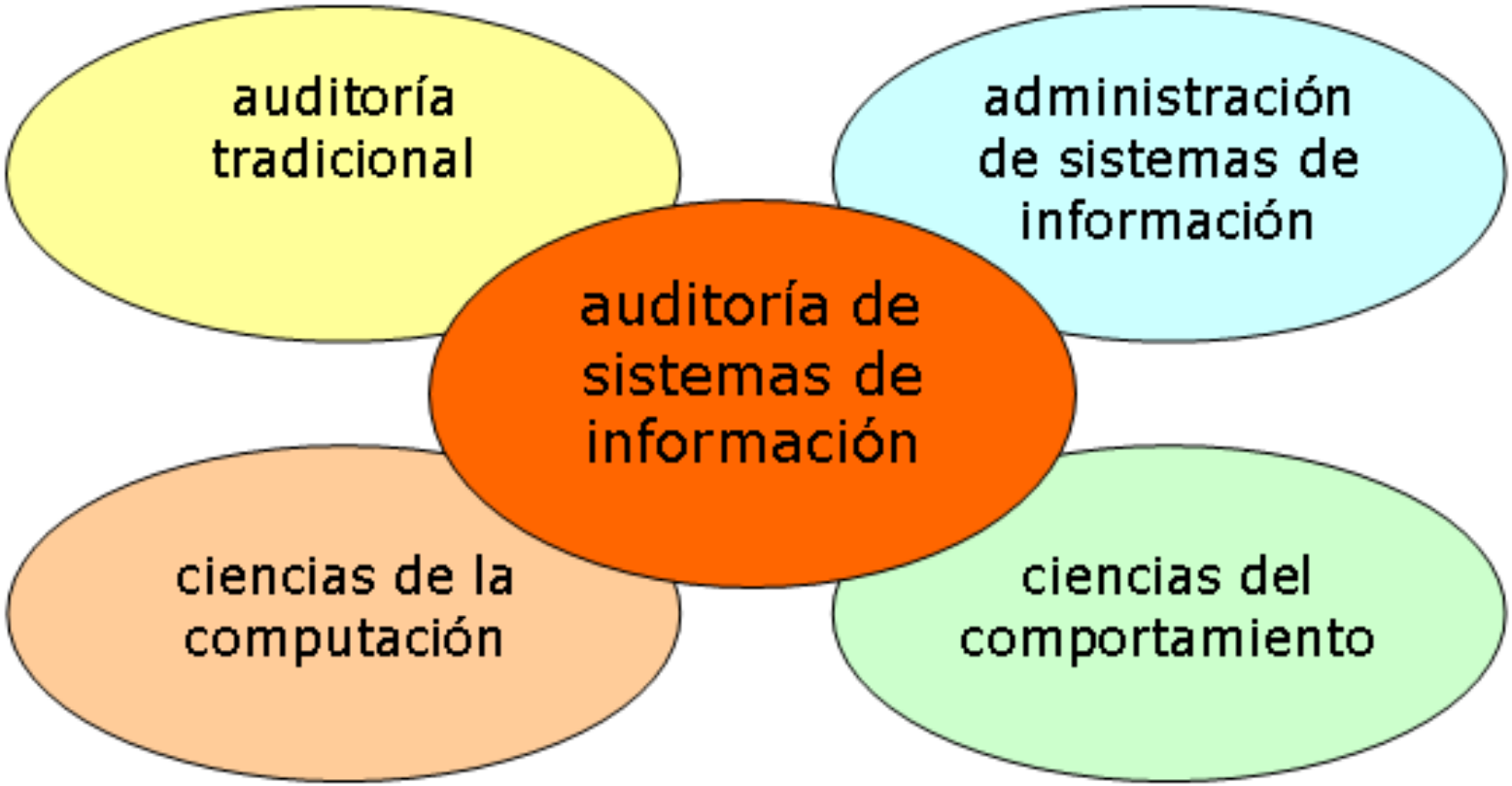
Los errores en los sistemas automáticos:

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



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.

OBJETIVO Y AGENDA

OBJETIVO

Explicar las motivaciones para auditar sistemas de información y el concepto de auditoría de sistemas de información.

AGENDA

1	MOTIVACIÓN	¿Cuáles son las razones para auditar sistemas?
2	AUDITORÍA	¿Qué significa una auditoría de sistemas?
3	RESUMEN	¿Qué se cubrió en esta sesión?

RESUMEN 1

Problemas que enfrentan las organizaciones por las cuales es necesario pensar en funciones de auditoría:

1) costos por pérdida de datos
2) costos por decisiones incorrectas
3) costos por abusos computacionales
4) costos por errores de computación
5) valor de hardware, software y personal
6) mantenimiento de privacidad
7) evolución controlada del uso de computadoras

RESUMEN 2

Definición de 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.

RESUMEN 3

Los objetivos de la auditoría se pueden alcanzar implementando un sistema de control interno, que incluya:

1) separación de obligaciones,
2) delegación clara de autoridad y responsabilidades,
3) reclutamiento y entrenamiento de personal calificado,
4) sistema de autorizaciones,
5) documentos y registros adecuados,
6) control físico y documentación sobre los activos,
7) chequeos independientes de performance,
8) comparación periódica de activos con registros contabilizados

RESUMEN 4

La auditoría de sistemas de información se fundamenta en:

1) auditoría tradicional
2) administración de sistemas de información
3) ciencias del comportamiento
4) ciencias de la computación

BIBLIOGRAFÍA Y MATERIAL DE LECTURA

BIBLIOGRAFÍA

Information Systems Audit and Control – Ron Weber – capítulo 1

BIBLIOGRAFÍA ADICIONAL

Information Technology Control and Audit (third edition) – *Sandra Senft, Frederick Gallegos* – capítulo 1

Muchas gracias!

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