

Administración de Proyectos de Software

Auditoría de Sistemas de Información

E. Estévez - P. Fillottrani

Depto. Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

segundo semestre 2018



Auditoría de Sistemas de Información

- ▶ es el proceso de **recolectar y evaluar evidencia** para determinar si el sistema informático
 - ▶ preserva los activos
 - ▶ mantiene la integridad de los datos
 - ▶ permite que los objetivos organizacionales se alcancen con eficacia
 - ▶ usa los recursos con eficiencia
 - ▶ cumple con determinadas pautas, leyes, normas, estándares o prácticas profesionales



Auditoría de Sistemas de Información

Introducción

Auditoría Interna

Auditoría Externa



Tipos de Auditoría

- ▶ una auditoría puede ser **interna**, es decir llevada a cabo por miembros de la misma organización en la que funciona el sistema
- ▶ en este caso valen los cuatro primeros objetivos
- ▶ o puede ser **externa**, ejecutada por profesionales no pertenecientes e independientes a la organización, contratados sólo al efecto de realizarla
- ▶ en este caso generalmente vale el último de los objetivos anteriores
- ▶ ejemplos: entidades financieras auditadas por el Banco Central, empresas auditadas para certificar normas ISO



La Informática en la Auditoría

- ▶ la función de auditoría no cambia si se trata de sistemas manuales o sistemas automatizados, es por esto que las prácticas de auditoría tiene sus raíces en la auditoría contable
- ▶ pero en sistemas automatizados es más complicado **recolectar evidencia**
- ▶ ejemplos:
 - ▶ controlar los casos de test de un programa,
 - ▶ controles criptográficos
- ▶ es más difícil evaluar las consecuencias de las fortalezas y debilidades de los controles



Controles

- ▶ 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 tienden a ser **determinísticos**, se generan **a mayor velocidad** y tienen consecuencias más costosas
- ▶ ejemplo: un programa erróneo siempre se va a ejecutar erróneamente en determinadas condiciones
- ▶ los controles aseguran la alta calidad en el diseño, implementación, operación y mantenimiento de los sistemas, y por lo tanto son **críticos**



Técnicas de Auditoría Informática



Técnicas de la Auditoría Tradicional

- ▶ aporta conocimientos y experiencia sobre técnicas de control interno y externo
- ▶ aporta la filosofía de los controles. Ejemplo: los programas deben asegurar que todas las transacciones fueron procesadas correctamente
- ▶ involucra examinar los sistemas de información con una mente crítica, siempre con una visión cuestionadora sobre su capacidad para:
 - ▶ salvaguardar activos
 - ▶ mantener integridad de datos
 - ▶ lograr objetivos eficiente y eficazmente



Técnicas de Administración de Sistemas de Información

- ▶ aporta documentación, estándares, presupuestos, buenas prácticas para la administración de proyectos y sistemas existentes
- ▶ 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
- ▶ ejemplo: metodologías de mantenimiento de bases de datos



Técnicas de las Ciencias de la Computación

- ▶ los **ingenieros de software** deben colaborar con los objetivos de la auditoría
- ▶ ejemplo: investigar sobre cómo comprobar 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



Técnicas de las Ciencias del Comportamiento

- ▶ existe siempre una resistencia de comportamiento que 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



Razones para controlar



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 importantes
- ▶ ejemplo: pérdida de datos de clientes o proveedores



Costos por decisiones incorrectas

- ▶ 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 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.
- ▶ otras veces el impacto puede ser considerable...



Costos por 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 sistemas automatizados
- ▶ la importancia de datos exactos depende del tipo de decisiones hechas por personas que tienen algún interés en la organización
- ▶ **alta gerencia**: toma decisiones de planeamiento estratégico. Probablemente acepten algunos errores en los datos
- ▶ **gerencia media**: toma decisiones de control administrativo y de control operativo. Requieren datos más exactos



Costos por abusos computacionales

- ▶ un **abuso computacional** es un incidente asociado con tecnología de computación, 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



Hacking

- ▶ una persona logra un acceso no autorizado a un sistema de computación para leer, modificar o borrar programas o datos, o para discontinuar un servicio

- ▶ ejemplo: caso grupo Anonymous

<http://www.bbc.co.uk/news/uk-20449474>

- ▶ ejemplo: caso Edward Snowden

<http://www.bbc.co.uk/news/world-us-canada-23768248>

- ▶ ejemplo: robo de contraseñas en Adobe

<http://www.bbc.co.uk/news/technology-24740873>



Acceso físico ilegal

- ▶ una persona logra un acceso físico no autorizado a facilidades del sistema informático. 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

- ▶ ejemplo: scammers roban datos de PCs

<http://www.bbc.co.uk/news/uk-england-24143233>



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]

- ▶ ejemplo: virus en Android

<http://www.bbc.co.uk/news/technology-20768996>

- ▶ ejemplo: virus en equipos médicos

<http://www.bbc.co.uk/news/technology-19979936>



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

- ▶ ejemplo:

<http://www.manchestereveningnews.co.uk/news/greater-manchester-news/dozens-public-sector-staff-rapped-5833122>

- ▶ ejemplo:

<http://www.computerweekly.com/news/2240111956/>

One-in-four-IT-security-staff-abuse-admin-rights-survey-shows



Consecuencias de los abusos

- ▶ destrucción de activos. ¿ejemplo?
- ▶ sustracción de activos
- ▶ modificación de activos
- ▶ violación de privacidad
- ▶ interrupción de operaciones
- ▶ uso no autorizado de activos
- ▶ daño físico a personas



Valor del HW, SW y personal

- ▶ son recursos críticos en las organizaciones
- ▶ **datos**: ¿qué pasa si la competencia obtiene información confidencial?
- ▶ **hardware**: ¿qué pasa si un componente crítico deja de funcionar?
- ▶ **software**: ¿qué pasa si se destruye?
- ▶ **personal**: ¿qué pasa si un profesional calificado deja la empresa?



Costos por errores computacionales

- ▶ los costos por un error de computación pueden ser altos en términos de: pérdida de vidas humanas, privación de libertad, daño al medio ambiente, etc
- ▶ esto se debe a que los sistemas informáticos controlan monitoreo de pacientes, cirugías, vuelo de misiles, reactores nucleares, etc



Mantenimiento de la privacidad de datos

- ▶ muchos datos se recolectan sobre los individuos: impuestos, obras sociales, trabajo, residencia
- ▶ con sistemas automatizados se puede integrar y buscar información muy fácilmente. ¿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



Salvaguarda de activos

- ▶ los activos de los sistemas de información incluyen:
 - ▶ hardware
 - ▶ software
 - ▶ facilidades
 - ▶ personas (conocimientos)
 - ▶ datos
 - ▶ documentación de sistemas
 - ▶ insumos



Impacto de la Auditoría de Sistemas de Información

- ▶ la auditoría resulta en
 - ▶ mejora en la salvaguarda de activos
 - ▶ mejora en la integridad de los datos
 - ▶ mejora en la efectividad de los sistemas
 - ▶ mejora en la eficiencia de los sistemas



Integridad de datos

- ▶ es un estado que en el cuál los datos poseen ciertos atributos:
 - ▶ completitud
 - ▶ 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



Valor de los datos

- ▶ el valor de un dato depende de:
 - ▶ 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
 - ▶ el grado en el cuál el ítem de dato es compartido entre los tomadores de decisiones
 - ▶ el valor del ítem de dato para los competidores



Eficiencia de los sistemas

- ▶ un sistemas de información 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



Efectividad de los sistemas

- ▶ un sistema de información es **efectivo** si satisface sus objetivos
- ▶ formas de evaluar la efectividad de los sistemas:
 - ▶ durante el proceso de desarrollo para garantizar que se satisfacen los requerimientos de los usuarios
 - ▶ mediante una post-auditoría
- ▶ para poder evaluar la efectividad de un sistema de información se deben conocer:
 - ▶ las características de los usuarios
 - ▶ el entorno de toma de decisiones



Auditoría interna

- ▶ los objetivos de la auditoría sólo se pueden lograr si la alta gerencia implementa un **sistema de control interno**, que puede incluir:
 - ▶ separación de obligaciones
 - ▶ delegación clara de autoridad y responsabilidades
 - ▶ reclutamiento y entrenamiento de personal calificado
 - ▶ sistema de autorizaciones
 - ▶ documentos y registros adecuados
 - ▶ control físico y documentación sobre los activos
 - ▶ chequeos independientes de performance
 - ▶ comparación periódica de activos con registros contabilizados



Implementación

- ▶ el uso de computadoras afecta de varias maneras la implementación de los componentes de un sistema de control interno
- ▶ ejemplo:
 - ▶ en un sistema automatizado deben existir registros
 - ▶ las funciones son realizadas por un programa



Delegación de responsabilidades

- ▶ 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 difícil
- ▶ 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



Separación de obligaciones

- ▶ en un sistema manual, personas diferentes deben realizar las tareas de
 - ▶ iniciar una transacción
 - ▶ registrar la transacción
 - ▶ 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



Responsabilidades

- ▶ debido a que los lenguajes de alto nivel son más fáciles de leer, muchos usuarios están desarrollando, modificando y operando sus propias aplicaciones.
- ▶ entonces los desarrollos hechos por usuarios tienen importantes beneficios para el usuario, pero **aumentan los problemas de control**



Personal competente y confiable

- ▶ a las personas responsables de desarrollar, implementar y operar los sistemas de información se les delega mucho poder
- ▶ ejemplos:
 - ▶ un analista puede aconsejar a la gerencia sobre el equipamiento de alta tecnología y de altos costos
 - ▶ un operador asume la responsabilidad de salvaguardar 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



Sistema de autorizaciones

- ▶ la gerencia debe establecer dos tipos de autorizaciones:
 - ▶ **autorizaciones generales**: establecen las políticas que la organización debe seguir. Ejemplo: lista de precios
 - ▶ **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



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



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:
 - ▶ un pedido telefónico
 - ▶ 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 proveer controles de acceso y facilidades de login para asegurar que los rastros de auditoría sean exactos y completos



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: en un sistema manual puede ser necesario tener que acceder a varios sitios; en un sistema automatizado todos los registros se pueden mantener en un sólo lugar
- ▶ la concentración de información aumenta la posibilidad de pérdida que puede surgir por abuso o desastre



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.



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 contruidos dentro del sistema
- ▶ el gerente debe acceder a los registros de auditoría para evaluar la gestión de los empleados



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



Auditoría Externa

- ▶ las prácticas de las auditorías externas están generalmente reguladas por los [Consejos Profesionales](#)
- ▶ la ley provincial 13.016 creó y reglamentó en 2003 la actividad del Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires (CPCIBA) www.cpciba.org.ar
- ▶ el CPCIBA ha establecido un [código de ética](#) para el ejercicio profesional
- ▶ el CPCIBA todavía no ha definido prácticas para realizar [auditoría externas](#)
- ▶ se pueden analizar los reglamentos de profesiones afines (como los de ciencias económicas)

