Auditoría de Sistemas

Módulo 2: Normativas

Dra. Marcela Capobianco

Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

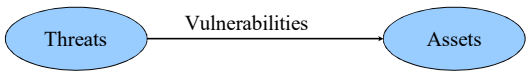
1

Copyright

-2-

Resumiendo

- Las regulaciones modernas nos piden:
  - Evidencia de la integridad del negocio
  - Evidencia de que existen controles internos para proteger los activos



-3-

Regulaciones

- Antes las organizaciones podían funcionar con menos controles
- Los inversores, clientes y el gobierno buscan seguridad de que la gerencia ha tomado medidas para prevenir eventos ilegales
- La gerencia debe diseñar un sistema que cumpla con estos objetivos
- Como auditor se debe comprender las políticas, estándares y procedimientos que tiene su compañía u organización. Además se debe comprender el propósito de la auditoría

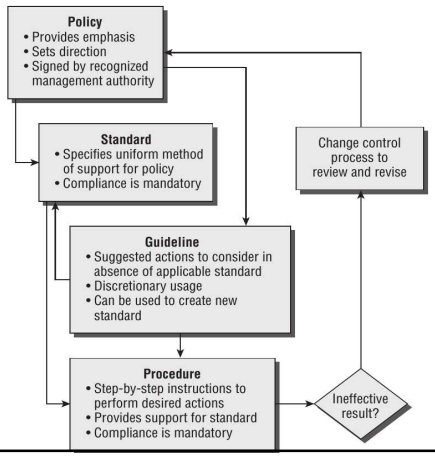
-4-

Documentación de una empresa u organización

- **Políticas:** son obligatorias y establecen un objetivo de alto nivel
- **Estándares:** asegurar aplicación uniforme de políticas
- **Guías:** son pautas generales discrecionales y nos aconsejan como alcanzar objetivos en la ausencia de un estándar
- **Procedimientos:** "recetas" de como realizar tareas específicas respetando los estándares establecidos

El auditor debe comprender todos estos elementos antes de auditar!

-5-



-6-

Propósito

- Una auditoría es simplemente una revisión de la historia pasada. Se espera que el auditor de SI (Sistemas de Información) siga el proceso de auditoría definido, establezca criterios de auditoría, reúna evidencia significativa y brinde una opinión independiente sobre los controles internos.

-7-

Motivación

- Suponga que lo han designado gerente del Departamento de Auditoría Interna de la UNS.
- Cómo planea encarar su nuevo trabajo?

-8-

Motivación

- Pregunta:

  ¿cómo puede ejecutar la auditoría, de tal forma de obtener una seguridad razonable sobre:

  - la salvaguarda de activos en el procesamiento de datos,
  - integridad de los datos,
  - la eficiencia y eficacia de los sistemas ?

-9-

Como auditores, debemos asegurarnos de:

- Alcanzar los objetivos de la auditoría
- Mantener la independencia
- Contribuir a un manejo eficiente de IT
- Contribuir a que la organización alcance sus objetivos de negocio

-10-

Organización de la función de auditar

- Puede ser interna o externa
- El rol del auditor interno debe establecerse claramente mediante un **audit charter** aprobado por la gerencia
- La auditoría en SI puede ser parte del departamento de auditoría
- Puede ser un grupo independiente

-11-

Organización de la función de auditar

- Estar integrada dentro de una auditoría financiera y operacional para proveer seguridad con respecto a los controles de IT para lo auditores financieros o para la gerencia
- La auditoría de SI es en este caso un soporte

-12-

Dos tipos de auditoría

- Existen dos tipos básicos de auditorías: una que verifica compliance (conformidad) a un conjunto de normas **(compliance test)** y otras que testean la sustancia e integridad de una dada aserción **(substantive test)**
- ¿Cómo podemos llevarlas a cabo?
- Afortunadamente existen varios recursos que nos asistirán en la tarea

-13-

Algunas normativas

- Financial Accounting Standards Board (FASB)
- Generally Accepted Accounting Principles (GAAP)
- American Institute of Certified Public Accountants (AICPA)
- Statement on Auditing Standards (SAS), standards 1 through 101, which are referenced and applied by the AICPA.

-14-

Algunas normativas (Cont..)

- Committee of Sponsoring Organizations of the Treadway Commission (COSO), providing the COSO internal control framework that is the basis for PCAOB standards
- U.S. National Institute of Standards and Technology (NIST), providing federal IS standards

-15-

Algunas normativas (Cont..)

- U.S. Federal Information Security Management Act (FISMA), which specifies minimum security compliance standards for government systems including the military
- IS Audit and Control Association (ISACA) and IT Governance Institute (ITG) issue
- COBIT guidelines that were derived from COSO with a more specific emphasis on information systems.
- International Organization for Standardization (ISO)

-16-

ITAF: (2014)

ITAF: Information Technology Assurance Framework

- Professional practice framework for IS Audit/Assurance
- ISACA
  - 118000 miembros es 180 países
  - Cobit, Nexus cybersecurity, CISA, CISM, etc (certificaciones)
  - Código de ética
- A continuación analizaremos el framework ITAF con más detalle

-17-

Audit Charter

- Autoridad general, alcance y responsabilidades del auditor
- Tiene que estar aprobada por el máximo gerente de la empresa
- Si la auditoría la realiza una firma externa se necesita un contrato
- En cualquier caso se debe mantener la independencia

-18-

Audit Charter

- Ver 1001 ITAF
- Es importante comprender la norma y su importancia para el trabajo del auditor

-19-

Leyes, estándares y Regulaciones para auditores de SI

20

Importancia de la independencia profesional

- El reporte debe estar *libre de condicionamientos o influencias*
- Las organizaciones profesionales han abordado este tópico
- Para que una persona actúe como auditor debe tener un alto estándar de ética
- El término auditor proviene del latín (alguien que escucha disputas y juzga sobre ellas)

-21-

Importancia de la independencia profesional

- Existe una línea muy fina entre lo que es ético y lo que es legal
- Existen cosas que pueden ser legales pero no son éticamente incorrectas
- Sin embargo, algunas cosas que comienzan a pensarse como no éticas se convierten ilegales al pasar el tiempo
- Si una gran cantidad de gente se opone a un comportamiento porque lo considera no ético se introducirá legislación al respecto

-22-

Responsabilidad profesional

- **Confidencialidad:** los ingenieros deben respetar la confidencialidad de sus empleados o clientes independientemente de si se firmó un contrato al respecto.
- **Competencia:** No se deben aceptar trabajos que estén fuera del área de competencia.
- **Derecho de propiedad intelectual:** se deben conocer los derechos de propiedad, patentes, etc. Se debe también proteger la propiedad intelectual de los empleados y clientes.

-23-

Responsabilidad profesional

- **Uso incorrecto de las computadoras:** los ingenieros de SW no deben usar sus habilidades técnicas para hacer un uso incorrecto de las comp. de otras personas. Ejemplos de esto varían desde usar las computadoras para jugar hasta infectar las computadoras con virus.

-24-

Código de ética del ACM

Association for Computing Machinery

- Sociedades profesionales de los EEUU han cooperado para producir este código.
- Los miembros de estas organizaciones automáticamente se adhieren al código al ingresar.
- El código contiene 8 principios que involucran a distintos profesionales de la Ing. de SW (ingenieros, educadores, supervisores y estudiantes).

-25-

Preámbulo

- La versión corta del código resume las aspiraciones en un alto nivel de abstracción.
- Las cláusulas en la versión completa dan detalles y ejemplos.
- Entre las dos permiten entender el código.

-26-

Preámbulo

- Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

-27-

Principios

1)Interés Público: Los I de SW actuarán en forma consistente con el interés público.

2)Cliente y empleado: Los I de SW actuarán de manera que este en los mejores intereses de su empleador y su clientes, consistentemente con el interés público.

3)Producto: los productos deben alcanzar los estándares más altos posibles.

-28-

Principios

4)Juicio: Los I de SW mantendrán integridad e independencia en el juicio profesional.

5)Gestión: los directores de proyectos deben subscribirse a un manejo ético del desarrollo y mantenimiento de SW.

6)Profesión: Los I de SW harán progresar la integridad y reputación de la profesión consistentemente con el interés público.

-29-

Principios

6)Colegas: Los I de SW serán justos y proveerán soporte a sus colegas.

7)Los I de SW participarán en un **aprendizaje de por vida** de su profesión y promoverán un acercamiento ético a la práctica de la misma.

-30-

Situación 1

Desacuerdo con las políticas de la empresa o dirección

-31-

Situación 2

Empleado que actúa en una forma no ética, por ejemplo, no realizando adecuadamente el testeo de un sistema crítico.

-32-

Situación 3

Le ofrecen participar en un proyecto del gobierno de un país para desarrollar armas de uso militar.

-33-

Situación 4

Un profesional que trabaja en una institución determinada (por ejemplo una universidad X) ofrece sus servicios a una empresa Y para realizar trabajos dentro de la universidad X.

-34-

Situación 5

Un ing. de SW desarrolla un programa para mensajería que al instalarse envía información de la computadora del usuario a un determinado servidor.

-35-

Situación 6

Debe recomendar a un cliente que maneja una pequeña empresa que SW usar para su PC recién adquirida. Sabe que el costo del SW comercial que se usa actualmente es prohibitivo. Que haría?

-36-

El código de ética de ISACA

- Ahora veremos un código específico para auditores de sistemas de información

-37-

ISACA principles

- Favorecer la implementación de, y apoyar que se cumpla con:
  - estándares,
  - procedimiento y
  - controles apropiados para los SI.
- Realizar sus deberes con diligencia y cuidado profesional en acuerdo con los estándares y mejores prácticas.

-38-

ISACA principles

- Servir al interés de los stakeholders en forma legal y honesta manteniendo altos estándares con conducta y carácter
- Mantener la privacidad y confidencialidad de la información obtenida durante el trabajo a menos que sea requerido por una autoridad legal revelar información. La información no puede ser usada para beneficio personal.

-39-

ISACA principles

- Ser competentes en los campos de trabajo y sólo acceder a realizar aquellas actividades que pertenezcan a las áreas de competencia.

-40-

ISACA principles

- Informar a las partes apropiadas sobre los resultados del trabajo realizado revelando todos los hechos significativos que conozcamos.
- Promover la educación profesional de los participantes para mejorar su entendimiento de la seguridad y el control de los SI.

-41-

Estándares ISACA

- Hacer que los auditores de SI tengan un nivel mínimo de performance
- Garantizar que se cumplan las expectativas de la gerencia en cuanto a la calidad del trabajo
- Definen requerimientos obligatorios para las auditorías

-42-

1001: Audit Charter

- El propósito responsabilidad y autoridad de la función de auditar SI debe estar documentada en un audit charter o engagement letter (Carta de compromiso)
- Se debe aprobar en un nivel adecuado de la organización

-43-

1002 y 1003: Independencia

- **Independencia profesional:** entre el auditor y el que está siendo auditado
- **Independencia organizacional:** el área de auditoría en SI debe ser independiente del área o actividad que está siendo revisada

-44-

1006: Competencia

- Debe tener la habilidad y el conocimiento para realizar la tarea asignada
- Debe someterse a una educación continua

-45-

1201 y 1202: Planificación

- Planificar para cumplir los objetivos y respetar las leyes aplicables y los estándares de auditoría
- Desarrollar y documentar un acercamiento basado en riesgos
- Desarrollar y documentar un plan de auditoría detallando la naturaleza y objetivos, tiempos, alcance y recursos requeridos.

-46-

1203: Performance

- Se debe supervisar el staff
- Se debe recolectar suficiente evidencia
- Se debe documentar el trabajo realizado

-47-

1401: Reporte

- Establece cómo debe reportarse el trabajo del auditor
- Es muy importante que las conclusiones estén sustentadas en evidencia adecuada y suficiente

-48-

1402: Seguimiento

- Evaluar si se han tomado las acciones apropiadas de acuerdo a lo recomendado

-49-

1207: Irregularidades

- Concierne a como lidiar con irregularidades y actos ilegales
- Ver 1207 ITAF

-50-

1202: Riesgos

- Usar un acercamiento basado en riesgos para la planificación a fin de determinar prioridades para el uso de los recursos disponibles
- Al planificar revisiones individuales se debe identificar y abordar riesgos relevantes al área

-51-

Ejercicio

- Investigar en qué consisten los estándares restantes

-52-

Guías

- Las guías proveen información más detallada sobre cómo cumplir con los estándares
- Se debe usar el juicio profesional para aplicarlas o no a una auditoría particular

-53-

Algunos ejemplos

- 2001: como debe ser la estructura del audit charter y como elaborarla
- Se debe justificar una desviación de lo que dice la guia
- 2002: Independencia organizacional, como debe ser la estructura de la empresa para asegurarla

-54-

Algunos ejemplos

- 2005: Cuidado profesional requerido
- Está relacionado con el código de ética ISACA
- Ver la guia

-55-

Procedimientos

.Provee ejemplos de procedimientos que el Auditor de Sistemas puede utilizar en una revisión. Los procedimientos ofrecen información de cómo cumplir con los estándares al realizar una auditoría de sistemas pero no especifican requerimientos.

-56-

Procedimientos

- P1: IS risk assessment
- P2: Digital signatures
- P3: Intrusion detection
- P4: Viruses
- P5: Control risk self assessment
- P6: Firewalls

-57-

Procedimientos

- P7: Irregularities and ilegal acts
- P8: Security assessment
- P9: Evaluation of management controls over encryption methodologies
- P10: Bussines aplications change controls
- P11: Electronic Funds Transference

-58-

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.

-59-

Comunicación entre auditor y auditado

- La persona que está siendo auditada aprecia que se le explique el propósito. Se siente en desventaja. Explicar de forma simple.
- Se puede evaluar la performance de acuerdo a la actitud hacia el auditor en el sitio a auditar.
- Si se está realizando un buen trabajo el cliente muestra interés y es proactivo brindando buenas respuestas e información.

-60-

Planificación

- Cómo planificar una auditoría
- A corto plazo: lo que puede realizarse en un año como máximo
- A largo plazo: objetivos a largo plazo que toman en cuenta elementos relacionados con el riesgo con respecto a cambios estratégicos en la organización con respecto a IT

-61-

Planificación

- Se debe replantear al menos una vez al año
- Hay que considerar cambios en los riesgos, tecnologías, etc
- Los cambios deben ser aprobados por la gerencia
- También debe actualizarse si cambia el marco regulatorio

-62-

Planificación

- Entender los objetivos de negocio, procesos, etc
- Esto incluye la disponibilidad necesaria, la seguridad, la confidencialidad, etc
- Identificar contenidos clave: políticas, estándares y guidelines. Procedimientos y estructura organizativa.

-63-

Planificación

- Realizar un análisis de riesgos para ayudar a diseñar el plan
- Especificar el alcance y los objetivos de la auditoría
- Desarrollar una estrategia de auditoría.
- Asignar personal para realizar la auditoría
- Organizar la logística necesaria

-64-

Planificación

- Se debe considerar el panorama tecnológico actual y la dirección futura
- Leer publicaciones industriales, planes estratégicos, reportes anuales, memorias
- Leer informes de auditorías anteriores
- Entrevistar gerentes
- Asignar recursos disponibles a las tareas del plan

-65-

Algunas reflexiones…

- Ser auditor es una posición ejecutiva
- La confidencialidad del auditor es sumamente importante
- Usar sólo la información mínima necesaria para completar una tarea
- En casos comprometidos buscar consejo legal

-66-

Algunas reflexiones…

- El auditor debe usar controles para proteger sus activos
- Un grupo de auditores debe tener sólo un líder y una estructura bien definida de responsabilidades.

-67-

Bibliografía

- Auditors guide to information systems auditing, R. Cascarino, Wiley, 2007. Capítulo 3, 4.
- CISA Study guide, Cannon, Bergman y Pamplin, Wiley, 2013.
- CISA Review Manual. ISACA, 2011.

-68-