Auditoria e Segurança de Sistemas de Informação

Auditoria de Sistemas

- A **auditoria** é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o intuito de verificar sua conformidade com certos objetivos e politicas institucionais, orçamentos, regras, normas e padrões.

10

Auditoria de Sistemas

- **Auditoria** é um exame sistemático e objetivo de um ou mais aspectos de uma organização que compara o que a organização faz, frente a um conjunto definido de critérios ou requisitos.

11

Auditoria de Sistemas

- As organizações usam a TI para apoiar as suas operações e na realização de sua missão e dos seus objetivos de negócios.
- Isso dá às organizações um grande interesse em assegurar que:
  - o uso da TI seja eficaz,
  - os sistemas de TI e processos operem da forma pretendida, e
  - os ativos de TI e outros recursos sejam eficientemente distribuídos e protegidos.

12

Auditoria de Sistemas

- O *Institute Of Company Secretaries Of India* em [2] define:
  - Sistema de informação não significa necessariamente o sistema de informação baseado em computador.
  - A Tecnologia da Informação (TI) é um componente importante do Sistema de Informação e não é em si a própria solução.
  - Com a ampla disponibilidade de microcomputadores e softwares poderosos, a TI é a espinha dorsal do sistema de informação.

13

Auditoria de Sistemas

- Como computadores desempenham um papel importante em ajudar-nos a processar os dados e tomar decisões, é importante que a sua utilização seja controlada.
- Seu uso descontrolado pode ter um amplo impacto sobre a sociedade.
  - informações imprecisas pode provocar má alocação de recursos na economia e
  - fraude pode ser perpetrada por causa de controles de sistemas inadequados.

14

Auditoria de Sistemas

- Assim ela define:
  - Auditoria de sistemas de informação ou auditoria de sistemas é o processo de coleta e avaliação de evidências para determinar se um sistema de computador:
    - salvaguarda ativos,
    - mantém a integridade dos dados,
    - permite que as metas organizacionais sejam alcançados de forma eficaz, e
    - usa recursos de forma eficiente

15

Auditoria de Sistemas

- Gantz em [1] define:
  - Auditoria de TI ajuda as organizações a compreender, avaliar e melhorar os seus controles para proteger os recursos de TI, medir e corrigir desempenho, e atingir os objetivos e os resultados pretendidos pela organização.

16

Auditoria de Sistemas

- Prof. Carlos Eduardo em [4] define:
  - A **auditoria de sistemas** é o ramo da auditoria que revisa e avalia o controles internos informatizados, visando:
    - proteger os ativos da organização;
    - manter a integridade e autenticidade dos dados;
    - atingir eficaz e eficientemente os objetivos da organização.

17

Auditoria de Sistemas

- E ainda...
  - **Auditoria de Sistema de Informação** é instrumento da direção, dos acionistas, do ambiente externo, do usuário para: opinar, avaliar, validar a qualidade dos dados, da informação e dos sistemas que a geram e mantêm, em termos de segurança, confiabilidade e eficiência.

18

Auditoria de Sistemas

- Consiste na utilização de metodologias de auditoria formais para examinar os processos específicos de TI, capacidades e ativos e seu papel em viabilizar os processos de negócios de uma organização [1].

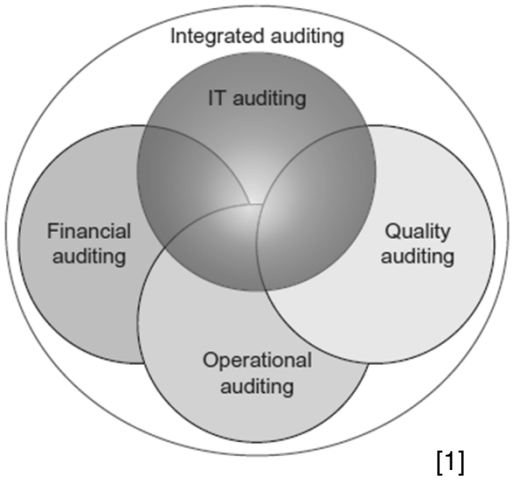
19

Auditoria de Sistemas

- Também aborda componentes de TI ou capacidades que dão suporte a outros domínios sujeitos a auditoria, tais como gestão financeira e contábil, desempenho operacional, garantia de qualidade e de governança, gerenciamento de risco e *compliance* (GRC) [1].

20

Auditoria de Sistemas



[1]

21

Auditoria de Sistemas

- Para ISO (a) e ITIL (b)
  - a) um processo sistemático, independente e documentado para obter evidências de auditoria e avaliá-la objetivamente para determinar a extensão em que são cumpridos os critérios de auditoria.
  - b) inspeção e verificação formal para verificar se uma norma ou conjunto de orientações estão sendo seguidas, que os registros são exatos ou que as metas de eficiência e eficácia estão sendo atendidas.

22

Auditoria de Sistemas

- Para uma auditoria externa, a linha base é geralmente definida nas regras e requisitos legais ou regulamentações relacionados com o propósito e objetivos da auditoria externa.
- Para auditorias internas, as organizações muitas vezes têm alguma flexibilidade para definir a sua própria linha base ou de adotar normas, estruturas ou requisitos especificados por outras organizações.

23

Auditoria de Sistemas

- **O que auditar** (1):
  - Como outros tipos de auditorias, a de TI compara processos organizacionais reais, práticas, capacidades, ou controles com uma linha base pré-definida.
  - podem ser executados em toda a estrutura ou em diferentes níveis dentro de uma organização
    - unidades de negócios individuais, missões, processos de negócios, serviços, sistemas, infra-estrutura, ou componentes de tecnologia).

24

Auditoria de Sistemas

- **O que auditar** (2):
  - Invariavelmente endereçam uma ou mais áreas relacionadas à tecnologia, incluindo controles relacionados com:
    - Centros de dados e outras instalações físicas
    - Infra-estrutura de rede
    - Telecomunicações
    - Sistemas operacionais
    - Databases
    - Armazenamento

25

Auditoria de Sistemas

- **O que auditar** (3):
  - Servidores e ambientes virtualizados
  - Serviços e operações terceirizadas
  - Servidores Web e de aplicativos
  - Aplicações e pacotes de software
  - Interfaces de usuário e aplicativo
  - Dispositivos móveis

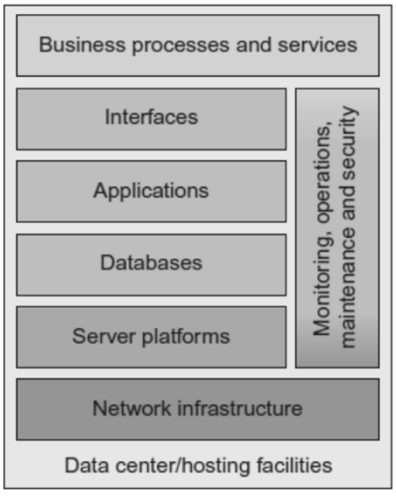
26

Auditoria de Sistemas

- **O que auditar** (4):
  - Elementos de TI podem ser auditados de forma isolada ou em conjunto,
  - Mesmo quando determinada auditoria se concentra estritamente em um aspecto de TI, os auditores precisam considerar os contextos mais amplos técnicos, operacionais e ambientais

27

Auditoria de Sistemas



[1]

28

Auditoria de Sistemas

- **O que auditar** (5):
  - Pode abordar também os processos de controle interno e funções, tais como:
    - operações e procedimentos de manutenção,
    - continuidade de negócios e recuperação de desastres,
    - resposta a incidentes,
    - de rede e monitoramento de segurança,
    - gerenciamento de configuração,
    - desenvolvimento de sistemas e
    - gerenciamento de projetos.

29

Auditoria de Sistemas

- **Características de auditoria de TI** (1)
  - Definições, normas, metodologias e orientações são as principais características associadas com as auditorias de TI
  - Derivados de normas de auditoria geralmente aceitas (GAAS - *Generally Accepted Auditing Standards*) e as normas e códigos de conduta internacionais.

30

Auditoria de Sistemas

- **Características de auditoria de TI** (2)
  - A complexidade e as características particulares dos controles de TI ou do ambiente operacional passando por uma auditoria, podem exigir dos auditores conhecimento especializado ou experiência para ser capaz de analisar corretamente e de forma eficaz os controles incluídos no escopo da auditoria de TI.

31

Auditoria de Sistemas

- **Características de auditoria de TI** (3)
  - Códigos de conduta, prática e comportamento ético são, como regra, comum em todos os domínios de auditoria,
  - Enfâse em princípios e objetivos, tais como integridade, objetividade, competência, confidencialidade e adesão a padrões e orientação apropriados.

32

Auditoria de Sistemas

- **Características de auditoria de TI** (4)
  - Independência do auditor - um princípio aplicável às auditorias e auditores internos e externos
    - os auditores e as organizações que representam não têm interesse financeiro específico sobre o que está sendo auditado e,
    - estão livres de conflitos de interesse em relação às organizações que auditam,
  - mantêm a objetividade e imparcialiadade.

33

Auditoria de Sistemas

- **Por que auditar** (1)
  - Muitas empresas de capital aberto e organizações estão sujeitas a requisitos legais e regulamentações, cujo cumprimento é muitas vezes determinado através de uma auditoria.
  - Organizações que buscam certificações para processo ou serviço de qualidade, maturidade, ou

34

Auditoria de Sistemas

- **Por que auditar** (2)
  - A implementação de controle e efetividade normalmente devem ser submetidas a auditorias de certificação por auditores independentes.
  - Auditorias muitas vezes fornecem informações que ajudam as organizações a gerenciar riscos, confirmar a alocação eficiente de recursos relacionados a TI, e atingir outros objetivos de TI e de negócios.

35

Auditoria de Sistemas

- **Por que auditar** (3)
  - Razões para justificar auditorias internas de TI podem incluir:
    - conformidade com as regras de Valores Mobiliários que as empresas têm uma função de auditoria interna;
    - avaliar a eficácia dos controles implementados;
    - confirmar a aderência às políticas internas, processos e procedimentos;
    - verificar a conformidade com governança de TI ou de controle de estruturas e padrões;

36

Auditoria de Sistemas

- **Por que auditar** (3)
  - Razões para justificar auditorias internas de TI podem incluir:
    - análise de vulnerabilidades e definições de configuração para apoiar a monitorização contínua;
    - identificar fragilidades e deficiências, como parte da gestão inicial ou contínua de riscos;
    - medir o desempenho em relação aos parâmetros de qualidade ou acordos de nível de serviço;

37

Auditoria de Sistemas

- **Por que auditar** (4)
  - Razões para justificar auditorias internas de TI podem incluir:
    - verificação e validação dos sistemas de engenharia ou práticas de gerenciamento de projetos de TI; e
    - auto-avaliação da organização, de frorma antecipada, em relação a padrões ou critérios que serão utilizados em auditorias externas.

38

Auditoria de Sistemas

- **Por que auditar** (5) *resumindo...*
  - Auditoria de TI interna são muitas vezes impulsionadas por:
    - requisitos organizacionais para a governança de TI,
    - gestão de riscos, ou
    - de garantia da qualidade,
  - qualquer um deles pode ser usado para determinar o que precisa ser auditado e como priorizar as atividades de auditoria.

39

Auditoria de Sistemas

- **Por que auditar** (6) *resumindo...*
  - Auditoria de TI externa é mais frequentemente impulsionada por uma necessidade ou desejo de demonstrar o cumprimento de normas externamente impostas, regulamentos ou requisitos aplicáveis ao tipo de organização, indústria ou ambiente operacional.

40

Auditoria de Sistemas

- **Objetivos** (1)
  - Auditoria de sistemas apoia os objetivos da auditoria tradicionais [2];
    - objetivos de certificação que incidem sobre a segurança de ativos e integridade de dados e,
    - objetivos de gestão que englobam não só objetivos de certificação, mas também os objetivos de eficácia e eficiência.
    - Às vezes, os sistemas de informação de auditoria tem outro objetivo, ou seja, garantir que uma organização cumpra com algum regulamento, regra ou condição.

41

Auditoria de Sistemas

- **Objetivos** (2)
  - Segurança de ativos
    - Os ativos do sistema de informação de uma organização incluem hardware, software, instalações, pessoas (conhecimento), arquivos de dados, documentação do sistema e suprimentos.
    - Como todos os ativos, eles devem ser protegidos por um sistema de controle interno.
      - Hardware pode ser danificado de forma maliciosa.
      - Software proprietário e o conteúdo dos arquivos de dados podem ser roubados ou destruídos.

42

Auditoria de Sistemas

- **Objetivos** (3)
  - Integridade dos dados
    - É um estado implicando que os dados tem certos atributos: completude, integridade, pureza e veracidade.
    - Se a integridade dos dados não é mantida, uma organização não tem uma verdadeira representação de si mesmo ou de eventos.
    - Se a integridade dos dados de uma organização é baixo, ela poderia sofrer uma perda de vantagem competitiva.

43

Auditoria de Sistemas

- **Objetivos** (4)
  - Eficácia do sistema
    - Um sistema de informação eficaz realiza os seus objetivos.
    - Avaliação da eficácia implica o conhecimento das necessidades dos usuários.
    - Para avaliar se um sistema de relatórios de informações facilita a tomada de decisão por seus usuários, auditores devem conhecer as características dos usuários e do ambiente de tomada de decisão.

44

Auditoria de Sistemas

- **Objetivos** (5)
  - Eficiência do sistema
    - Um sistema de informação eficiente utiliza recursos mínimos para atingir os seus objetivos necessários.
    - Sistemas de informação consome, vários recursos: tempo de máquina, periféricos, software de sistema e de trabalho.
      - Estes recursos são escassos, e diferentes sistemas de aplicação normalmente concorrem para a sua utilização.

45

Auditoria de Sistemas

- **Objetivos** (6)
  - A administração deve se interessar principalmente em impedir:
    - O tempo excessivo de desenvolvimento.
    - O custo alto de desenvolvimento.
    - Objetivos irrealistas ou impossíveis de cumprir.
    - Sistemas rígidos quando se tornarem operacionais.
    - Não agregação de valor.
    - Métodos e sistemas dispendiosos.

46

Auditoria de Sistemas

- **Objetivos** (7)
  - A falta de controle envolve muitos riscos.
  - Muitos sistemas falham por causa de algum dos seguintes motivos:
    - Falta de gestão de capacidade técnica.
    - Falta de apoio à gestão no desenvolvimento do sistema.
    - A inexperiência dos funcionários ou falta de treinamento.
    - Expectativas irrealistas com orientações erradas.

47

Auditoria de Sistemas

- **Quem é auditado** (1)
  - Dada a utilização generalizada da TI em organizações de todos os tamanhos e tipos, e os benefícios para organizações que estabelecem e mantêm programas de auditoria interna de TI com sucesso, a auditoria é algo valioso.

48

Auditoria de Sistemas

- **Quem é auditado** (2)
  - No que diz respeito à auditoria de TI externa, as organizações podem não estar em posição de determinar se, como, nem quando se submeter a auditorias de TI, vez que muitas auditorias externas são legalmente obrigatórias e não facultativas.

49

Auditoria de Sistemas

- **Quem é auditado** (3)
  - Para muitas organizações a decisão de estabelecer e manter a gestão de risco ou de programas de governança de TI é uma escolha, não uma exigência, mas tais abordagens são comumente vistos como melhores práticas.

50

Auditoria de Sistemas

- **Quem faz a auditoria** (1)
  - Auditar os controles internos de TI exige:
    - amplo conhecimento de TI,
    - habilidades, capacidades e conhecimentos especializados em princípios gerais e específicos, práticas e processos de auditoria de TI.

51

Auditoria de Sistemas

- **Quem faz a auditoria** (2)
  - As organizações precisam desenvolver ou contratar pessoal com o entendimento especializado de objetivos de controle e experiência em operações de TI necessários para a condução de auditorias de TI de forma eficaz.

52

Auditoria de Sistemas

- **Quem faz a auditoria** (3)
  - Os tipos de organizações e indivíduos que realizam auditorias de TI incluem:
    - Os auditores internos – empregados que realizam auditoria interna de TI;
    - auditores de TI independentes ou como empregados de empresas de serviços profissionais que prestam serviços de auditoria de TI externos ou internos;

53

Auditoria de Sistemas

- **Quem faz a auditoria** (4)
  - Os tipos de organizações e indivíduos que realizam auditorias de TI incluem:
    - organizações de certificação - avaliam as práticas e controles organizacionais e conferem certificação para organizações cujos processos, sistemas, serviços ou ambientes operacionais internos aderem aos padrões aplicáveis ou outros critérios de certificação;

54

Auditoria de Sistemas

- **Quem faz a auditoria** (5)
  - Os tipos de organizações e indivíduos que realizam auditorias de TI incluem:
    - Organizações com a autoridade para supervisionar a implementação dos controles necessários ou fazer cumprir os regulamentos, como o Government Accountability Office (GAO), Federal Deposit Insurance Corporation (FDIC), e do Departamento de Saúde e Serviços Humanos (HHS) Escritório de Direitos Civis (OCR) dentro do governo federal dos EUA;

55

Auditoria de Sistemas

- **Auditor de TI** (1)

[1]

56

Auditoria de Sistemas

- **Auditor de TI** (2)
  - Educação e relevantes experiência profissionais como pré-requisitos associados a certificações relacionados à auditoria são alguma indicação,
  - os auditores precisam de treinamento extensivo, conhecimento, e experiência prática antes que eles possam ser eficazes na realização de auditorias.

57

Auditoria de Sistemas

- **Auditor de TI** (3)
  - Requer conhecimento relevante e habilidades não apenas relacionados a TI, mas experiência em muitas facetas de operações de negócios, gestão organizacional e de governança, gerenciamento de risco e execução de processos e prestação de serviços, também contribuem como base de conhecimento para que auditores de TI sejam bem sucedidos no seu trabalho.

58

Auditoria de Sistemas

- **Auditor de TI** (3)
  - Auditoria de TI requer amplo conhecimento técnico e funcional e toca domínios empresariais e de TI em vários níveis dentro de uma organização.
  - Auditores de TI eficazes podem potencialmente vir de muitas disciplinas diferentes ou áreas iniciais de especialização.

59

Bibliografia

1. *The Basics of IT Audit - Purposes, Processes, And Practical Information*, Stephen D. Gantz – Elsevier
2. *Professional Programme – Information Technology And Systems Audit - Module 2 - Paper 4* - ICSI
3. *Boas Práticas em Segurança da Informação*, TCU, 4ª. Edição
4. *Auditoria em Sistemas de Informação*, Prof. Carlos Eduardo Gertners de Magalhães, UGF – Apostila

60