TRIBUNAL DE CONTAS DA UNIÃO

Auditoria em Contratos de Tecnologia da Informação

Secretaria de Fiscalização de Tecnologia da Informação
Sefti

Abril de 2012

Apresentação

- ✓ Apresentação rápida dos participantes e suas expectativas em relação ao curso
- ✓ Sobre o instrutor
- ✓ Sobre o horário do curso e seus intervalos
- ✓ Sobre o curso

Objetivos do Curso

- ✓ Conhecer formas de atuação da Sefti/TCU em trabalhos de fiscalização de TI
- ✓ Conhecer as principais normas e padrões utilizados pelo TCU na fiscalização de contratos de TI
- ✓ Compreender as técnicas utilizadas nas auditorias de contratos de TI com objetivo de verificar a legalidade e a eficiência das contratações de TI
- ✓ Conhecer questões de fiscalização de contratos de TI comumente utilizadas

Agenda do Curso

- ✓ Apresentação
- ✓ Controles Gerais de TI
- ✓ Introdução à Auditoria de TI
- ✓ Abordagens de Fiscalização de TI
- ✓ Método de Fiscalização de TI

3,5 hs.

- ✓ Auditoria de Contratos de TI – 24,5 hs.

Agenda do Curso

	Segunda	Terça	Quarta	Quinta	Sexta
	09.04	10.04	11.04	12.04	13.04
09h00 12h30		Abordagens e Método de Auditoria de TI	Auditoria de Contratações de TI	Auditoria de Contratações de TI	Auditoria de Contratações de TI
		André / Jezini	André / Jezini	André / Harley	Harley / Daud
	Almoço				
14h00 17h30	Abertura Governança de TI Estratégia e Riscos no Planejamento	Auditoria de Contratações de TI	Auditoria de Contratações de TI	Auditoria de Contratações de TI	Auditoria de Contratações de TI
		Daud / Wesley	Wesley / André	Clayton / Renato	Renato / André

Agenda

- ✓ **A importância da tecnologia da informação (TI) e o papel do auditor**
- ✓ **Conceitos e nomenclaturas**
- ✓ **Abordagens de Fiscalizações de TI**
- ✓ **Controles Gerais e de Aplicativo**
- ✓ **Método de Fiscalização de TI**
- ✓ **Normas de Auditoria de TI**

Materialidade da TI

Gastos do Governo Federal em TI:

- ✓ 2006: R$ 6 bilhões

  Fonte: Siafi

- ✓ 2010: estimados R$ 16 bilhões

  Fonte: LOA 2010

- ✓ 2011: programados **R$ 18 bilhões**

  Fonte: LOA 2011

Criticidade da TI

- ✓ TI é setor **estratégico** na Administração Pública e os problemas na área geram grandes vulnerabilidades para a organização
- ✓ Fiscalizações realizadas pelo TCU identificaram que há muitas deficiências nos controles sobre a **terceirização de TI** na Administração Pública

Por que auditoria em tecnologia da informação?

"Os consideráveis gastos investidos no processamento eletrônico de dados demandam por auditorias apropriadas. Tais auditorias devem ser baseadas em sistemas e abranger aspectos, tais como: planejamento; uso econômico dos equipamentos de processamento de dados; alocação de pessoal com habilidades apropriadas, preferencialmente dentro da administração da organização auditada; prevenção ao mau uso; e utilidade da informação produzida"

(Intosai, Declaração de Lima que contém os princípios da Auditoria, 1977)

Por que auditoria em tecnologia da informação?

- ✓ Uso cada vez mais intenso e amplo da TI.
- ✓ Crescente dependência da TI.
- ✓ Informação: recurso cada vez mais crítico e estratégico.
- ✓ Mudanças na forma em que as organizações conduzem seus negócios.
- ✓ Número cada vez maior de sistemas informatizados, com incremento da complexidade e da interconectividade.
- ✓ O incremento da interconectividade induz maior vulnerabilidade a ameaças externas.
- ✓ Pequenos erros podem produzir grandes danos.
- ✓ Altos investimentos e grandes riscos.

Atuação dos Auditores

Formação de equipes:

- ✓ Auditores (AUFCs)
- ✓ Auditores de TI (AUFCs - ATI):
  - ✓ O currículo de habilidades e técnicas da Intosai para o perfil de Auditor de TI baseia-se no universo de conhecimentos exigidos no programa de certificação CISA
  - ✓ ***Certified Information Systems Auditor*** (CISA): Criada e mantida pela Isaca. É referência mundial na área de Auditoria de TI, tendo mais de 85.000 profissionais certificados
  - ✓ A Sefti possui 10 auditores certificados CISA e o TCU possui 15
- ✓ Especialistas em TI (AUFCs - TI)

Papel do auditor

Avaliação dos Controles Internos:

- ✓ “O auditor, para determinar a extensão e o alcance da fiscalização, deve examinar e avaliar o grau de confiabilidade dos controles internos” (Normas de Auditoria da INTOSAI).
- ✓ “O papel do auditor é auditar as políticas, práticas e procedimentos de controle interno de uma organização, a fim de assegurar que os controles são adequados para se alcançar a missão institucional”. (Intosai, Controle Interno: estabelecendo uma base para prestação de contas no governo, 2001)
- ✓ “Conjunto de procedimentos adotados para avaliar o grau de confiança e de qualidade dos controles existentes, verificar a correta aplicação dos sistemas e procedimentos, e detectar as falhas que estejam ocorrendo” (Maria de Lourdes Deroza).

Papel do auditor

“Auditores internos devem ter conhecimento suficiente dos principais riscos e controles de TI e das técnicas de auditoria disponíveis, baseadas em tecnologia, para realizar seus trabalhos. Porém, não é esperado que todos auditores tenham as habilidades de um auditor interno com a responsabilidade primária de auditar TI.”

(IIA / IPPF - Padrão 1210.A3)

Papel do auditor

"Se os auditores internos terão que confiar no sistema de processamento de dados como base para determinar a validade de sua saída, eles devem ser capazes de analisar o sistema e seus controles ou requisitar pessoas que o façam. Dada à importância do sistema, mudanças em seu ambiente de operação e na forma em que o dado é processado são também críticas para o auditor."

(IIA, *Global Technology Audit Guides*-GTAG).

Agenda

- ✓ A importância da tecnologia da informação (TI) e o papel do auditor
- ✓ Conceitos e nomenclaturas
- ✓ Abordagens de Fiscalizações de TI
- ✓ Controles Gerais e de Aplicativo
- ✓ Método de Fiscalização de TI
- ✓ Normas de Auditoria de TI

Conceitos e nomenclatura

- ✓ Auditoria de Processamento Eletrônico de Dados (EDP Audit)
- ✓ Auditoria de Sistemas (IS Audit)
- ✓ Auditoria da Tecnologia da Informação (IT Audit)

Auditoria de Tecnologia da Informação

Processo que busca evidências para certificar-se de que os recursos de tecnologia da informação:

- ✓ possibilitam que os objetivos de negócio sejam alcançados;
- ✓ são usados com eficiência e em conformidade com as leis e normas aplicáveis; e
- ✓ são adequadamente protegidos para prover informação confiável sempre que requerida às pessoas autorizadas.

Exemplos de atividades

Verificar:

- ✓ a confiabilidade das informações processadas por sistemas.
- ✓ a segurança física e/ou lógica da área de TI de uma organização.
- ✓ o correto funcionamento de um sistema computadorizado.
- ✓ a adequação e o correto funcionamento da infraestrutura da área de TI (banco de dados, redes de computadores etc).
- ✓ o desempenho da área de TI (desenvolvimento, suporte técnico, produção etc), com vistas ao atendimento dos objetivos de negócio.
- ✓ a qualidade dos produtos, dos sistemas e dos serviços oferecidos pela área de TI ao negócio.
- ✓ a correta contratação de bens e serviços de TI (legalidade, eficácia, eficiência, economicidade e efetividade).

Agenda

- ✓ A importância da tecnologia da informação (TI) e o papel do auditor
- ✓ Conceitos e nomenclaturas
- ✓ Abordagens de Fiscalizações de TI
- ✓ Controles Gerais e de Aplicativo
- ✓ Método de Fiscalização de TI
- ✓ Normas de Auditoria de TI

Abordagens de ATI

- ✓ As abordagens de auditoria se complementam, existindo áreas de intersecção entre elas
- ✓ Isso ocorre devido os princípios que guiam cada uma dessas abordagens se encontrarem correlacionados dentro de uma estrutura de governança de TI
- ✓ Auditorias de TI normalmente mesclam aspectos de conformidade e operacionais

Utilização de diferentes abordagens

- Representam as possíveis formas de focalizar a TI
- Permitem que a TI seja examinada sob diferentes aspectos ou prismas
- Fornecem visões distintas e complementares da situação da TI na organização
- Decorre da necessidade de se estruturar a própria auditoria de TI com vistas a auxiliar a condução do trabalho pela equipe, durante as fases de planejamento e execução
- Cada abordagem pode se mostrar mais ou menos adequada para o alcance dos objetivos da auditoria, devendo ser definida na fase de planejamento

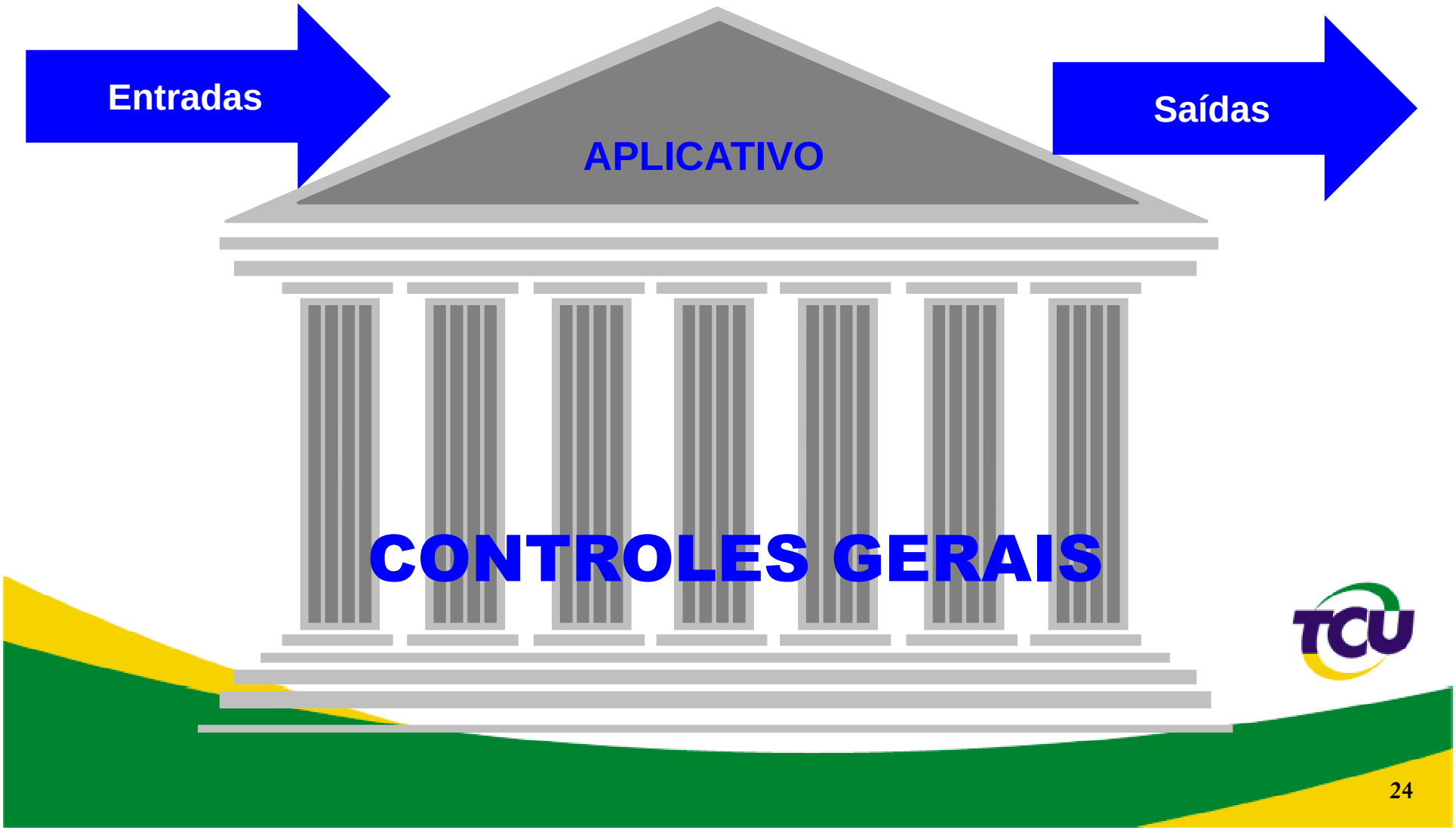
Abordagens

- ✓ Auditoria de Governança de TI
- ✓ Auditoria de Sistemas
- ✓ Auditoria de Dados
- ✓ Auditoria de Segurança da Informação
- ✓ Auditoria de Contratações de TI

Agenda

- ✓ A importância da tecnologia da informação (TI) e o papel do auditor
- ✓ Conceitos e nomenclaturas
- ✓ Abordagens de Fiscalizações de TI
- ✓ Controles Gerais e de Aplicativo
- ✓ Método de Fiscalização de TI
- ✓ Normas de Auditoria de TI

Controles gerais e de aplicativo



Controles gerais e de aplicativos

Objetivo dos Controles:

- ✓ Prevenir fraudes, erros, desperdícios, abusos.
- ✓ Proteger o ativo.
- ✓ Assegurar a obediência às diretrizes, planos, normas e procedimentos.
- ✓ Assegurar a validade e integridade dos dados para tomada de decisão.
- ✓ Caráter preventivo.
- ✓ Voltados para a correção de desvios.
- ✓ Instrumentos auxiliares de gestão em todos os níveis hierárquicos.

Controles e o papel do gestor

“Auditores são parte do modelo governamental de controle interno, mas eles não são responsáveis pela implementação dos procedimentos de controle numa organização. Este trabalho é específico do gestor.”

*(*Intosai, Padrões de Controle Interno)

“Controle interno é uma ferramenta do gestor usada para prover razoável certeza de que os objetivos da administração estão sendo alcançados.”

(Intosai, Orientações para Padrões de Controle Interno)

Controles e o papel do gestor

"3.4.6 Normalmente a gerência é responsável por implantar um efetivo sistema de controle interno que garanta a conformidade com as leis e regulamentos. Ao desenhar as ações e os procedimentos para examinar essa conformidade, o auditor deve avaliar os controles internos da organização e mensurar o risco de que a estrutura de controle não previna ou detecte os casos de não-conformidade."

(Intosai, Código de Ética e Padrões de Auditoria, 1998)

Controles e o papel do gestor

"... a gerência deve fazer avaliação de risco para descobrir quais são seus riscos e quão sérios eles são. A auditoria interna deveria auxiliá-los nessa avaliação. Então, a gerência deve decidir quais riscos são aceitáveis e quais devem ser mitigados, e realizar a análise custo-benefício para decidir que controles são mais efetivos para mitigá-los . Controles já existentes devem ser examinados a fim de verificar se são efetivos ou se necessitam de controles compensatórios."

(IIA, *Global Technology Audit Guides*-GTAG).

"O gestor e a alta administração são responsáveis pelos processos de gestão de risco e controles da organização."

(IIA / IPPF - Padrão 2120-1)

Controles gerais e de aplicativos

- ✓ O auditor, ao cumprir seu papel de auditar controles e, com intuito de buscar indícios sobre a confiabilidade dos dados processados por sistemas, deve realizar uma avaliação limitada dos controles gerais e dos controles de aplicativos de TI.
- ✓ Ao certificar-se da efetividade dos controles gerais, o auditor possui algumas informações sobre os sistemas e os dados processados no ambiente estudado que lhe permitem decidir pelo nível de confiança a ser-lhes concedido e ações ou propostas de ações a serem executadas ainda no decorrer da auditoria ou posteriormente.

Controles gerais e de aplicativos

Avaliação limitada: avaliação menos profunda dos controles gerais e de aplicativos, que pode ser realizada por equipes compostas somente por auditores que não detenham conhecimentos específicos de TI. Os controles pertinentes são examinados na extensão necessária para atendimento dos objetivos da auditoria.

Controles gerais e de aplicativo

Controles Gerais de TI

- ✓ Estão relacionados ao ambiente onde os sistemas são processados e são implementados para assegurar que a estrutura de controle é estável e bem gerenciada (IIA, *Global Technology Audit Guides*-GTAG).

- ✓ Se aplicam a todos os processamentos executados em um ambiente informatizado, visando garantir que o ambiente computacional como um todo seja seguro e confiável. (TCU, Manual de Auditoria de Sistemas, 1998)

Controles gerais e de aplicativo

Controles Gerais de TI

- ✓ Políticas e padrões organizacionais, especialmente relacionados à TI.
- ✓ Organização e administração da TI.
- ✓ Segregação de funções.
- ✓ Controles físicos (de acesso e de ambiente).
- ✓ Controles lógicos de acesso.
- ✓ Desenvolvimento de sistema e alterações de programas.
- ✓ Plano de Continuidade de Negócios.
- ✓ Computação de usuário final.

Controles Gerais de TI

- ✓ Consistem na estrutura, políticas e procedimentos que se aplicam aos sistemas aplicativos e bases de dados de uma organização.
- ✓ Influem no ambiente em que os sistemas aplicativos e os controles irão operar.
- ✓ Buscam garantir a integridade dos sistemas como um todo, incluindo todos os aplicativos, dados e arquivos.
- ✓ Durante uma auditoria em que seja necessário avaliar algum sistema ou base de dados em particular, é preciso inicialmente avaliar os controles gerais que atuam sobre o estrutura computacional da organização.
- ✓ Um ambiente de controle estável e bem gerenciado reforça a efetividade dos controles de aplicativos.

Controles Gerais de TI

Políticas e padrões organizacionais, especialmente relacionados à TI:

- ✓ Políticas, procedimentos e estrutura organizacional estabelecidos para organizar as responsabilidades de todos os envolvidos nas atividades relacionadas à área de informática.

Ex.: Política de Segurança da Informação (PSI),
Política de Controle de Acesso (PCA),
Política de Senhas (qualidade, revisão periódica),
Processo de Contratação de Soluções de TI

Controles Gerais de TI

Objetivo de controle: ter garantia de que políticas e normas são estabelecidas, divulgadas e seguidas na organização

Possíveis questões de auditoria:

- ✓ Existem políticas e normas de TI formalmente estabelecidas?
- ✓ Existe um processo formal para estabelecimento e manutenção das políticas e normas de TI?
- ✓ As políticas e normas são efetivamente conhecidas, seguidas e aplicadas?
- ✓ As políticas estabelecidas concorrem para uma boa gestão de segurança da informação ?
- ✓ As políticas estabelecidas concorrem para aquisições de TI adequadas às necessidades da organização e de acordo com a legislação vigente ?

Controles Gerais de TI

Critérios:

- ✓ NBR ISO/IEC 27002:2005, item15.2.1 Conformidade com as políticas e normas de Segurança da Informação
- ✓ Cobit 4.1
  - PO6.1 Ambiente de controle e políticas de TI;
  - PO6.3 Gerência de políticas de TI;
  - PO6.4 Divulgação de políticas;
- ✓ IN-4/2010 – Processo de Contratação de Soluções de TI

Possíveis achados:

- ✓ Inexistem políticas de TI

  Ex.: Política de Segurança da Informação (PSI),
  Política de Controle de Acesso (PCA),
  Processo de Contratação de Soluções de TI formalizado.
- ✓ Inexiste processo de criação/revisão das políticas de TI
- ✓ As políticas de TI são desconhecidas ou ineficazes

Controles Gerais de TI

Segregação de funções:

- ✓ Tem como objetivo evitar que um indivíduo venha a controlar todos as etapas críticas de um processo (por exemplo, um programador com permissão para independentemente escrever, testar e aprovar alterações de programa).
- ✓ A segregação de funções é alcançada pela divisão de responsabilidades entre dois ou mais grupos organizacionais.
- ✓ Verificação da separação dos ambientes de desenvolvimento, teste e produção.
- ✓ O controle organizacional e de operação da área de TI mais importante é a **segregação de funções**.

Controles Gerais de TI

Objetivo de controle: assegurar que estão definidos os papéis e responsabilidades, em termos quantitativos e qualitativos, de cargos, funções e ambientes de TI e de negócio, com respeito ao princípio da segregação

Possíveis questões de auditoria:

- ✓ Há definição formal de responsabilidades para as áreas, cargos e funções de TI?
- ✓ As funções são devidamente segregadas?
- ✓ Os papéis sensíveis ou áreas críticas de TI (planejamento, coordenação, supervisão, controle, administração de banco de dados e de rede, segurança da informação) possuem tratamento diferenciado?
- ✓ Os ambientes são devidamente segregados (produção, homologação, teste, desenvolvimento)?

Controles Gerais de TI

Critérios:

- ✓ Decreto nº 2.271/1998, art. 6º
- ✓ Acórdãos nºs 2.023/2005, item 9.3.2.2 e 71/2007, itens 9.2.5 e 9.2.23, todos do Plenário-TCU
- ✓ NBR ISO/IEC 27002:2005, item10.1.3 Segregação de funções
- ✓ Cobit 4.1

  PO4.6 Estabelecimento de papéis e responsabilidades; PO4.13 Pessoal chave de TI; PO4.11 Segregação de funções

Controles Gerais de TI

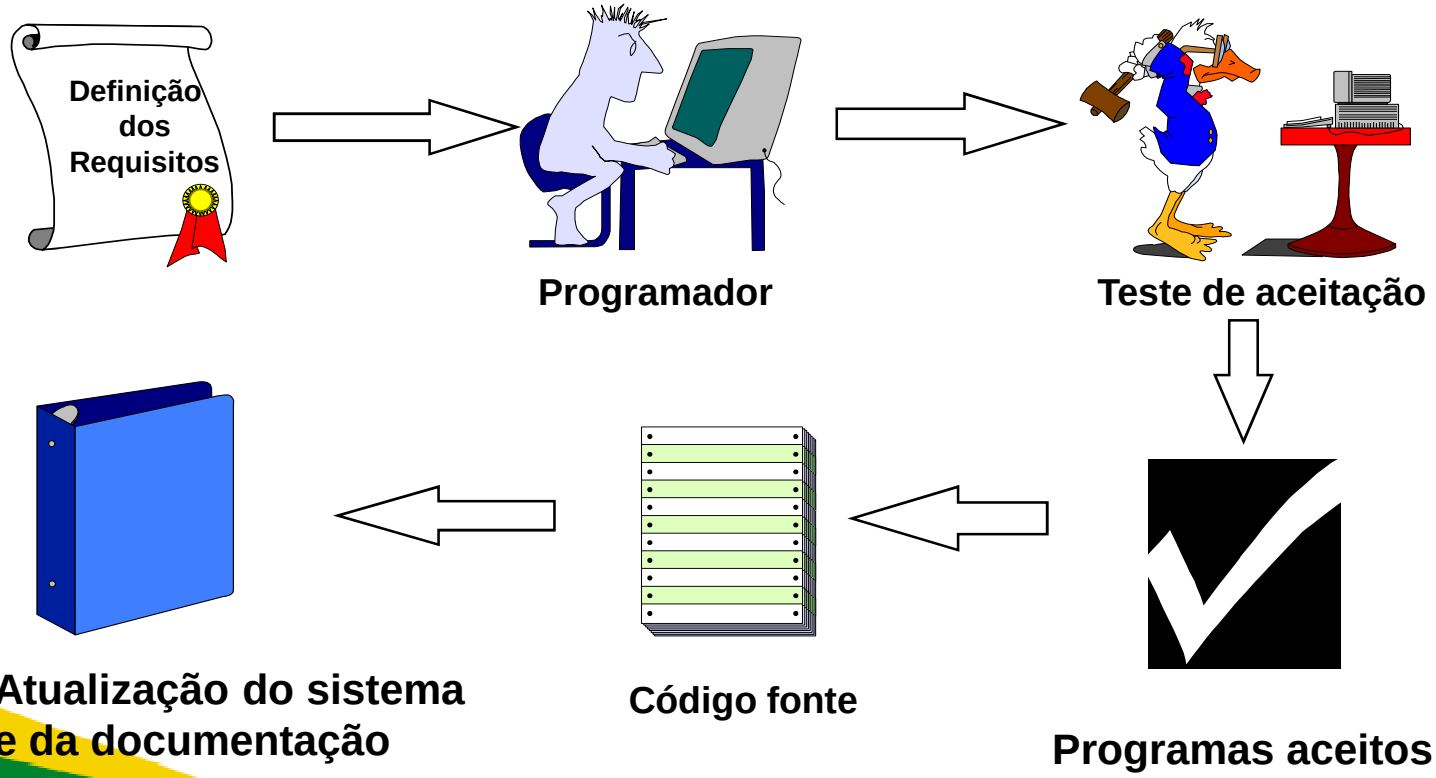
Possíveis achados:

- ✓ Não há definição formal de responsabilidades (o gestor do sistema não está formalmente definido)
- ✓ As áreas críticas de TI estão sem responsável ou são exercidas por terceirizados
- ✓ O princípio da segregação de funções não é respeitado, pois não há divisão de papéis e responsabilidades
- ✓ Funcionários do Serpro com acesso não controlado ao ambiente de produção (Acórdão nº 1.505/2007 – TCU – Plenário)
- ✓ Confusão dos papéis do gestor e da área de TI (Acórdão nº 2.023/2005 – TCU – Plenário)

Controles Gerais de TI

Desenvolvimento de sistema:

- ✓ Utilização de um Processo de Desenvolvimento de *Software* formalmente aprovado, que contemple padrões de desenvolvimento, artefatos, documentações, casos e planos de testes, aceites etc. durante o ciclo de vida dos sistemas.



Controles Gerais de TI

Alterações de programas:

- ✓ Devem existir políticas e procedimentos específicos, padronizados e formalizados para instalar e modificar o software de sistemas, bem como documentar e solucionar problemas com esse software (Controle de Mudanças).
- ✓ Alterações no sistema devem ser aprovadas pelo proprietário do sistema e não apenas pela área de TI.
- ✓ Alterações de programas também se sujeitam ao Processo de Desenvolvimento de Software institucional.
- ✓ Todos os softwares novos ou alterados devem ser testados e aprovados em ambiente específico de testes/homologação.

Controles Gerais de TI

Objetivo de controle: assegurar que o processo de desenvolvimento e manutenção de sistemas existe e é formalizado e seguido em todas as aquisições

Possíveis questões de auditoria:

- ✓ Há padrões para o desenvolvimento de sistemas?
- ✓ Estão previstos os artefatos a serem gerados para documentação dos sistemas?
- ✓ Há regras para implementação de mudanças em sistemas?
- ✓ Há área específica para lidar com as mudanças no ambiente de TI?

Controles Gerais de TI

Critérios:

- ✓ IN-4/2010 SLTI/MP, art. 13, II
- ✓ Acórdão nº 1.603/2008-TCU-Plenário, item 9.1.4;
- ✓ Acórdão nº 2.023/2005-TCU-Plenário, item 9.1.5;
- ✓ Acórdão nº 71/2007-TCU-Plenário, item 9.2.9;
- ✓ Cobit 4.1
  - PO8.3 Padrões de desenvolvimento e de aquisições

Possíveis achados:

- ✓ Inexiste processo sistematizado para desenvolvimento de sistemas
- ✓ Inexiste ou é precária a documentação dos sistemas
- ✓ As mudanças promovidas em sistemas não são testadas ou não são homologadas em ambientes específicos antes de entrarem em produção

Controles gerais e de aplicativo

Controles de Aplicativos

- ✓ são específicos dos sistemas e são implementados para prevenir, detectar e corrigir erros e irregularidades em transações durante a entrada, processamento e saída de dados. (CIA, Análise de Negócio e Tecnologia da Informação, Volume 2: Seções C-E, pag.301)
- ✓ possui como objetivo garantir um processamento confiável e exato, a partir de controles incorporados diretamente em programas aplicativos, nas três áreas de operação: entrada, processamento e saída de dados. (TCU, Manual de Auditoria de Sistemas, 1998)

Controles gerais e de aplicativo

Controles de Aplicativos

- ✓ Controles e procedimentos que garantem que apenas as transações válidas são processadas e registradas.
- ✓ Controles na(o):
  - Entrada de dados;
  - Processamento de dados;
  - Saída de dados.

Agenda

- ✓ A importância da tecnologia da informação (TI) e o papel do auditor
- ✓ Conceitos e nomenclaturas
- ✓ Abordagens de Fiscalizações de TI
- ✓ Controles Gerais e de Aplicativo
- ✓ Método de Fiscalização de TI
- ✓ Normas de Auditoria de TI

Levantamento

Informações Iniciais → Avaliação dos Controles Internos → Relatório do Levantamento

Planejamento

Visão Geral → Avaliação dos Controles Internos (*) → Elaboração Matriz de Planejamento

Execução

Aplicação dos Procedimentos → Acumulação de Evidências → Desenvolvimento dos Achados (Matriz de Achados)

Elaboração do Relatório

Elaboração do Relatório → Revisão do Relatório

Monitoramento

Verificação das Ações Tomadas → Aplicação dos Procedimentos → Acumulação de Evidências → Matriz de Achados → Elaboração do Relatório

(*) caso a fase de levantamento não tenha sido realizada.

Método de Auditoria de TI

- ✓ Fases (Levantamento, Planejamento, Execução, Elaboração do Relatório e Monitoramento)
- ✓ Matrizes (Planejamento e Achados)
- ✓ Técnicas de Auditoria de Conformidade
- ✓ Técnicas de Auditoria Operacional

Levantamento

- ✓ Informações Iniciais:
  - Objetivos institucionais.
  - Legislação aplicável.
  - Estrutura organizacional.
- ✓ Avaliação dos Controles Internos:
  - "*o auditor, para determinar a extensão e o alcance da fiscalização, deve examinar e avaliar o grau de confiabilidade dos controles internos*" (Normas de Auditoria da INTOSAI).
  - *"Conjunto de procedimentos adotados para avaliar o grau de confiança e de qualidade dos controles existentes, verificar a correta aplicação dos sistemas e procedimentos, e detectar as falhas que estejam ocorrendo"* (Maria de Lourdes Deroza).

Levantamento

- ✓ Procedimentos de Avaliação:
  - Identificação e documentação dos sistemas informatizados da organização.
  - Identificação e análise de riscos.
  - Identificação dos principais controles a serem avaliados.
  - Aplicação de ferramentas de auditoria (*Computer Assisted Audit Tools* – CAATs).

Levantamento

- ✓ Controles Gerais
- ✓ Controles de Aplicativos
- ✓ Análise de dados

Levantamento

- ✓ Análise de Dados:
  - Testes de Aderência:
    - Seu objetivo é proporcionar ao auditor razoável segurança quanto à efetiva utilização dos procedimentos previstos como controles internos.
  - Testes Substantivos:
    - Seu objetivo é obter evidências que corroborem a validade e propriedade dos atos e fatos administrativos, assegurando razoável grau de certeza quanto à inexistência de erros e irregularidades materiais.
  - Testes de Aderência X Testes Substantivos:
    - Segundo princípios geralmente aceitos de auditoria, quanto menor a confiabilidade dos controles gerais ou de aplicativo (ou se esses não forem avaliados), maior a extensão do teste necessário para determinar a confiabilidade dos dados.

Determinação da extensão da avaliação dos controles de TI

- ✓ Conhecimento prévio sobre o ambiente de TI, sobre os controles do sistema ou sobre os dados.
- ✓ Papel da evidência:
  - única evidência para fundamentar um achado;
  - evidência auxiliar, ou de ratificação;
  - informação geral (histórico, descrições etc.)
- ✓ Quanto menor a confiabilidade dos controles gerais ou de aplicativo (ou se esses não forem avaliados), maior a extensão do teste necessário para determinar a confiabilidade dos dados.

Planejamento

- ✓ Nesta fase, deve ser definido:
  - Objetivo da auditoria.
  - Objeto da auditoria.
  - Universo a ser auditado (escopo).
  - Técnicas e procedimentos a serem utilizados.
  - Critérios de auditoria.
  - Etapas e cronogramas.
  - Recursos humanos e materiais.

Planejamento

- ✓ Atividades da fase de planejamento:
  - Visão Geral
  - Avaliação dos Controles Internos (*)
  - Escolha da(s) Abordagem(ns) da Auditoria de TI
  - Elaboração da Matriz de Planejamento
  - Definição do envolvimento dos especialistas
  - Documentação do planejamento da auditoria

(*) Caso a fase de Levantamento não tenha sido realizada.

Planejamento

- ✓ Visão Geral:
  - Objetivos institucionais.
  - Estrutura organizacional.
  - Legislação aplicável.
  - Práticas administrativas.
  - Planos Estratégicos.
  - Descrição do objeto da fiscalização.

Conhecendo o auditado

- ✓ Compreender o negócio é essencial para identificar os riscos e controles;
- ✓ Direcionar os esforços da auditoria de forma mais eficiente;
- ✓ Entender o negócio:
  - Processos
  - Pessoas
  - Tecnologia
- ✓ Algumas questões a serem respondidas:
  - Existem problemas que o auditor deveria conhecer melhor?
  - Há alguma previsão de mudança na organização?
  - Quais são os principais sistemas e bases de dados?
  - Quem o auditor deve entrevistar para obter as informações de que necessita?

Planejamento

- ✓ Escolha da(s) abordagem(ns) da ATI:
  - Cada abordagem pode se mostrar mais ou menos adequada para o alcance dos objetivos da auditoria.
  - As abordagens escolhidas fornecerão suporte para a definição e elaboração das matrizes de planejamento e procedimentos que serão utilizadas para avaliar os controles dos sistemas e processos de TI.
  - Mudanças de abordagens trazem grandes alterações e impactos no planejamento da auditoria.
  - Por exemplo, uma fiscalização que inicialmente se vislumbrava ser uma auditoria somente de dados pode se transformar em uma auditoria de sistemas, ou vice-versa, impactando o escopo do trabalho, os recursos envolvidos e prazos para sua execução.

Planejamento

- ✓ Matriz de Planejamento:
  - Instrumento para organizar as informações relevantes do planejamento de uma auditoria.
  - Homogeneização do entendimento da equipe, e demais envolvidos, quanto:
    - ao objetivo do trabalho;
    - aos passos a serem seguidos;
    - à estratégia metodológica a ser adotada.
  - Orienta os integrantes da equipe nas fases de execução e de elaboração do relatório.

Matriz de Planejamento

Objetivo: Enunciar de forma clara e resumida o aspecto a ser enfocado pela auditoria, de acordo com o levantamento de auditoria previamente realizado.

Questões de Auditoria	Informações Requeridas	Fontes de Informação	Detalhamento do Procedimento	Objetos	Membro Responsável	Período	Possíveis Achados
Apresentar, em forma de perguntas, os diferentes aspectos que compõem o escopo da fiscalização e que devem ser investigados com vistas à satisfação do objetivo	**Identificar as informações necessárias para responder a questão de auditoria**	**Identificar as fontes de cada item de informação requerida da coluna anterior. Estas fontes estão relacionadas com as técnicas empregadas**	**Descrever as tarefas que serão realizadas, de forma clara, esclarecendo os aspectos a serem abordados (itens de verificação ou *check list*)**	**Indicar o documento, o projeto, o programa, o processo, ou o sistema no qual o procedimento será aplicado. Exemplos: contrato, folha de pagamento, base de dados, ata, edital, ficha financeira, processo licitatório, orçamento**	**Pessoa(s) da equipe encarregada(s) da execução de cada procedimento**	**Dia(s) em que o procedi-mento será execu-tado**	**Esclarecer com precisão que conclusões ou resultados podem ser alcançados**

Execução

- ✓Aplicação dos procedimentos definidos
- ✓Acumulação de evidências
- ✓Desenvolvimento dos achados:
  - Consiste no acúmulo organizado de informações (ou evidências) apropriadas e necessárias para esclarecê-los e sustentá-los.
- ✓ Elaboração da Matriz de Achados:
  - Deve ser preenchida à medida que os achados sejam identificados durante a execução dos procedimentos de auditoria.
  - Permite uniformizar o entendimento dos membros da equipe de auditoria, preparando-os para a escrita do relatório.

Execução

Matriz de Achados:

Achado	Situação Encontrada	Critério	Evidência	Causas	Efeitos	Encaminha-mento
Corres-pondência com o Achado (An) constante da Matriz de Procedi-mentos	Situação existente, identificada e documentada durante a fase de execução da auditoria	Legislação, norma, jurisprudência, entendimento doutrinário ou padrão adotado	Informações obtidas durante a auditoria no intuito de documentar os achados e de respaldar as opiniões e conclusões da equipe	O que motivou a ocorrência do achado	Conse-qüências do achado	Propostas da equipe de auditoria. Deve conter identificação do(s) responsável (is)
A1						
A2						
An						

Execução

- ✓ Matriz de Achados:
  - Os achados da auditoria devem levar em conta o nível de risco associado;
  - Bom senso em colocar achados de baixo risco;
  - Devemos ser realistas, usar a empatia;
  - Cada falha apontada deve estar suportada por evidências e papéis de trabalho.

Elaboração do Relatório

O Relatório de Auditoria é o instrumento formal e técnico por intermédio do qual a equipe de auditoria comunica:

- ✓ o objetivo do trabalho.
- ✓ a metodologia (como foi executado).
- ✓ os achados (resultado obtido).
- ✓ as conclusões (avaliações e opiniões).
- ✓ a proposta (recomendações e determinações).

Elaboração do Relatório

Requisitos do Relatório de Auditoria:

- ✓ **C**lareza
- ✓ **C**onvicção
- ✓ **C**oncisão
- ✓ **E**xatidão
- ✓ **R**elevância
- ✓ **T**empestividade
- ✓ **O**bjetividade

Elaboração do Relatório

Estrutura do Relatório de Auditoria:

- ✓ Resumo
- ✓ Sumário
- ✓ Introdução (Visão Geral)
- ✓ Achados de Auditoria
  - Situação encontrada
  - Critérios
  - Evidências
  - Causas
  - Efeitos
  - Encaminhamentos
- ✓ Outros Fatos Relevantes
- ✓ Conclusão
- ✓ Proposta de Encaminhamento
- ✓ Apêndices/Anexos

Elaboração do Relatório

Relatório Final:

- ✓ Linguagem mais técnica
- ✓ Relatório deve ser útil
- ✓ Detalhamento dos achados, riscos associados e recomendações
- ✓ Inclusão de gráficos e tabelas bem apresentados e contextualizados
- ✓ O excesso de informação ou detalhe deve ser evitado, procurando-se manter um equilíbrio entre a concisão e a clareza no corpo principal do relatório (uso de apêndices se necessário)

Elaboração do Relatório

Cuidados com o público:

- ✓ Durante a escrita dos achados de auditoria, a equipe deve tomar cuidados especiais com o uso de termos técnicos ou de difícil entendimento, levando em conta que o relatório será lido por pessoas que, na sua maioria, não trabalham ou se encontram diretamente envolvidas com TI (público leigo)
- ✓ Essas pessoas (gestores, autoridades, auditores, jornalistas etc) estarão mais interessadas em compreender como os achados levantados afetam as áreas de negócio do órgão/entidade auditado
- ✓ Glossário de termos técnicos (se necessário)

Elaboração do Relatório

Propostas de Encaminhamento:

- ✓ Conjunto de medidas a serem adotadas pela entidade visando corrigir as falhas ou irregularidades apontadas.
- ✓ Recomendações devem ser realistas, exequíveis e racionais, ou seja, aceitáveis e passíveis de implementação.
- ✓ Para cada achado deverá haver pelo menos uma recomendação.

Monitoramento

O que é?

- ✓ Instrumento para verificar o cumprimento das deliberações do TCU e os resultados delas advindos.
- ✓ É composto pelas mesmas fases de uma auditoria (Planejamento, Execução e Elaboração do Relatório).

Objetivos:

- ✓ Acompanhar as providências tomadas no âmbito do órgão ou programa auditado em resposta às recomendações exaradas pelo Tribunal, interagindo com os gestores responsáveis, de forma a maximizar a probabilidade de que essas recomendações sejam adequadamente adotadas (Follow-Up).
- ✓ Permite a retroalimentação do trabalho de auditoria, na medida em que fornece aos gestores o *feedback* de que necessitam para verificar se as ações que vêm adotando têm contribuído para o alcance dos resultados desejados.

Agenda

- ✓ O papel do auditor e a importância da auditoria de tecnologia da informação (ATI)
- ✓ Conceitos e nomenclaturas
- ✓ Abordagens de Fiscalizações de TI
- ✓ Controles Gerais e de Aplicativo
- ✓ Método de Fiscalização de TI
- ✓ Normas de Auditoria de TI

Normas e Padrões em ATI

- ✓ Constituição Federal
- ✓ Legislação Brasileira
- ✓ Cobit – *Control Objectives for Information and related Technology* – Governança de TI
- ✓ NBR ISO/IEC 38500 – Governança de TI
- ✓ ITIL – *Information Technology Infrastructure Library* – Serviços de TI
- ✓ NBR ISO/IEC 20000 – Serviços de TI
- ✓ Série NBR ISO/IEC 27000 – Segurança da Informação
- ✓ Outros Padrões

Constituição Federal

- ✓ Direitos e Deveres Individuais e Coletivos (Art. 5º)
  - Liberdade de expressão e crenças
  - Direito de resposta
  - Intimidade, vida privada, honra e imagem
  - Sigilo correspondência e comunicação de dados
- ✓ Princípios da Administração Pública (Art. 37)
  - Legalidade, impessoalidade, moralidade, publicidade e eficiência
  - Contratações mediante licitação

Legislação Brasileira

- ✓ Lei 8.112 de 1990 – Regime Jurídico dos Servidores Públicos Civis da União
- ✓ Lei 8.666 de 1993 – Licitações e Contratos da Administração Pública Federal
- ✓ Lei 9.609 de 1998 – Proteção da propriedade intelectual de software
- ✓ Lei 9.983 de 2000 – Crimes contra a Previdência (altera o Código Penal)
- ✓ Lei 10.520 de 2002 – Institui a modalidade de licitação Pregão
- ✓ Lei 12.527 de 2011 – Acesso às Informações

Decretos

- ✓ Decreto 3.505 (2000) – PSI da Administração Pública Federal
- ✓ Decreto 4.553 (2002) – Segurança das Informações e Documentos Sigilosos da Administração Pública Federal
- ✓ Decreto 5.450 (2005) – Regulamenta o Pregão na forma eletrônica
- ✓ Decreto 7.174 (2010) – Regulamenta a Contratação de Bens e Serviços de Informática pela Administração Federal

Cobit 4.1

Cobit (*Control OBjectives for Information and related Technology*) é um processo estruturado com objetivo de possibilitar a governança em TI, ou seja:

- ✓ gerenciar e controlar as iniciativas de TI nas organizações;
- ✓ garantir o retorno de investimentos;
- ✓ garantir a adoção de melhorias nos processos organizacionais; e
- ✓ minimizar riscos.

Disseminação do Cobit

- ✓ Resolução nº 2.554 do Banco Central de 1998 – dispõe sobre a implantação e implementação de sistema de controles internos
- ✓ Lei americana Sarbanes-Oxley (SOX) de 2002 – *Section 404: Assessment of internal control*
- ✓ Acordo do Comitê da Basiléia II (2004)
- ✓ Circular nº 249 da Susep de 2004 – dispõe sobre a implantação e implementação de sistema de controles internos nas sociedades seguradoras, nas sociedades de capitalização e nas entidades abertas de previdência complementar

ITIL v3

- ✓ *Information Technology Infrastructure Library*
- ✓ biblioteca de boas práticas nos serviços de TI
- ✓ desenvolvida no final dos anos 80 pela CCTA (*Central Computer and Telecommunications Agency*)
- ✓ atualmente sob custódia da OGC (*Office for Government Commerce*) do Reino Unido

ITIL v3

- ✓ promover a gestão com foco no cliente e na qualidade dos serviços de TI
- ✓ estruturas de processos para a gestão de TI da organização
- ✓ conjunto abrangente de processos e procedimentos gerenciais, organizados em disciplinas
- ✓ gestão tática e operacional
- ✓ alcançar o alinhamento estratégico com os negócios

Série NBR ISO/IEC 27000

- ✓ 27001 – Especificação de Sistema de Gestão de Segurança da Informação (2006)
- ✓ 27002 – Código de Prática para Gestão da Segurança da Informação (2005)
- ✓ 27003 – Implantação de Sistema de Gestão de Segurança da Informação (ainda em estudos)
- ✓ 27004 – Medição da Eficácia do Sistema de Gestão de Segurança da Informação (2010)
- ✓ 27005 – Gestão de Riscos de Segurança da Informação (2008)
- ✓ 27006 – Normas para Certificadores de SI (2007)

Outros Padrões

- ✓ Outras Normas internacionais
- ✓ Entidades de Fiscalização Superior - EFS
- ✓ Associações profissionais
- ✓ Padrões nacionais
- ✓ Padrões internos das organizações

Padrões Nacionais

- ✓ Associação Brasileira de Normas Técnicas (ABNT)
  - NBR ISO/IEC série 27000 e outras internalizadas no País
  - Padrões suplementares em áreas específicas
- ✓ Gabinete de Segurança Institucional (GSI/PR)
  - IN-01/2008 – Gestão da Segurança da Informação
  - NC-1 a NC-14 – Segurança da Informação
- ✓ Secretaria de Logística e TI (SLTI/MP)
  - IN-4/2010 – Processo de Contratação de TI
  - IN-2/2008 – Contratação de Serviços
- ✓ Tribunal de Contas da União (TCU)
  - Manual de Auditoria de Sistemas (1998)
  - Manual de Fiscalização de TI (previsto para 2012)
  - Guia de Contratações de TI (previsto para 2012)

Obrigado!

sefti@tcu.gov.br