TRIBUNAL DE CONTAS DA UNIÃO

Metodologia e ferramentas de suporte à auditoria de dados

Secretaria de Fiscalização de Tecnologia da Informação

Marcio Rodrigo Braz, Me

Maio de 2012

Objetivos do Minicurso

- ✓ Conhecer a atuação da Sefti em ATI
- ✓ Distinguir as diferentes abordagens em fiscalizações de tecnologia da informação (TI)
- ✓ Introduzir o conceito de CAATTs
- ✓ Apresentar a metodologia de auditoria de dados
- ✓ Demonstrar aplicações para uso da técnica

Agenda

- ✓ Introdução à Auditoria de TI
  - ✓ Por que fiscalização de TI e o papel do auditor
  - ✓ Atuação da Sefti/TCU
  - ✓ Abordagens de auditoria de TI
  - ✓ Normas e Padrões em ATI
- ✓ Introdução ao uso de CAATs
- ✓ Auditoria de Dados
  - ✓ Padrões de auditoria no TCU
  - ✓ Metodologia de auditoria de dados

Por que fiscalização em tecnologia da informação?

- ✓ Materialidade: a União programou gastar R$ **18 bilhões** em 2011 com TI
  - ✓ Altos investimentos e grandes riscos.

- ✓ Criticidade: todas as áreas críticas da administração pública **dependem** de TI
  - ✓ + sistemas => +complexidade e +interconectividade.
  - ✓ + interconectividade induz maior vulnerabilidade a ameaças externas.
  - ✓ Pequenos erros podem produzir grandes danos.

Por que fiscalização 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 fiscalização em tecnologia da informação?

- ✓ Necessária a incorporação de mecanismos de controle cada vez mais poderosos.
- ✓ Impactos na forma como os entes fiscalizadores exercem suas competências.
- ✓ Preparação dos entes fiscalizadores para enfrentar o desafio de auditar uma Administração Pública cada vez mais informatizada, sujeita a maiores riscos e com um sistema de controle interno mais complexo.
- ✓ Necessidade do auditor de conviver com novos conceitos e metodologias de trabalho.

Por que fiscalização em tecnologia da informação?

- ✓ Grande parte dos controles internos de uma organização está embutida em sistemas informatizados.
- ✓ O trabalho de auditoria baseia-se, na maior parte das vezes, em informações oriundas de sistemas informatizados, as quais servirão de evidências para os achados de auditoria.
- ✓ Uma auditoria de conformidade (financeira) ou operacional, frequentemente requer considerações sobre os controles gerais de TI e, a depender dos objetivos almejados, uma avaliação dos dados.

Papel do auditor

Avaliação do ambiente de controle:

- ✓ “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)

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."

(Internal Auditor Institute / 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."

(Internal Auditor Institute, *Global Technology Audit Guides*-GTAG).

E a auditoria de TI?

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 estrutura de governança de TI da organização
- ✓ 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 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

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)

Agenda

- ✓ Introdução à Auditoria de TI
  - ✓ Por que fiscalização de TI e o papel do auditor
  - ✓ **Atuação da Sefti/TCU**
  - ✓ Abordagens de auditoria de TI
  - ✓ Normas e Padrões em ATI
- ✓ Introdução ao uso de CAATs
- ✓ Auditoria de Dados
  - ✓ Padrões de auditoria no TCU
  - ✓ Metodologia de auditoria de dados

O que é a Secretaria de Fiscalização de TI (Sefti) do TCU?

SEFTI – Origem

1992 – 2006

- ✓ Criação de grupos específicos para auditoria de TI
- ✓ Elaboração de padrões, manuais, procedimentos de auditoria de sistemas
- ✓ Várias auditorias na área de TI
- ✓ Realização de cursos e capacitação

Agosto/2006

- ✓ Criação de uma secretaria especializada para o controle externo (Sefti) – Res. TCU 193/2006.

Mapa estratégico

Negócio
Controle externo da governança de tecnologia da informação na Administração Pública Federal.

Missão
Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Visão
Ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação.

A SEFTI hoje

Quantos somos

- ✓ 28 servidores: 26 auditores e 2 técnicos
- ✓ Formação em áreas de TI e Direito
- ✓ 12 CISA + 5 outras certificações (CGEIT, CISSP etc)
- ✓ 3 Mestres e 8 MBA

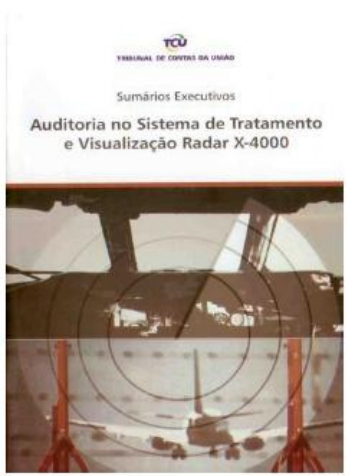
Estrutura

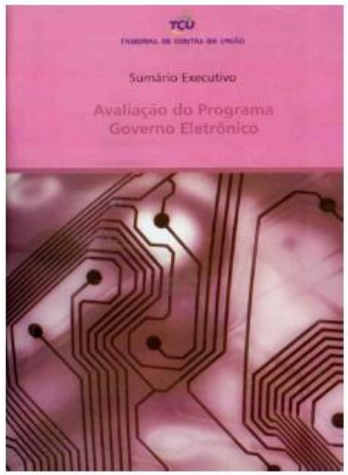
- ✓ 03 diretorias, 02 assessorias e 01 serviço de administração

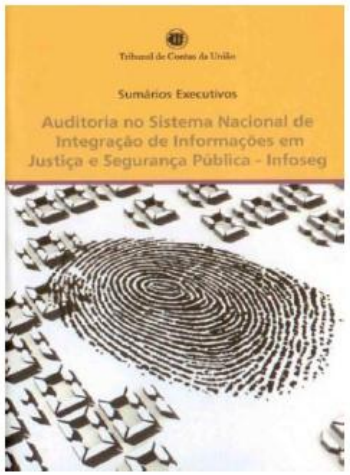
A SEFTI hoje

Ações estruturantes

- ✓ Cartilhas e manuais
- ✓ Levantamento de governança de TI
- ✓ Cursos
- ✓ Notas técnicas
- ✓ Orientações
- ✓ Eventos na área de controle e governança de TI
  - ✓ Controle externo em ação
  - ✓ Diálogos com gestores
  - ✓ Eventos para a alta administração
  - ✓ Conversa com a iniciativa privada







Acessíveis no portal:

http://www.tcu.gov.br/fiscalizacaoti

Agenda

- ✓ Introdução à Auditoria de TI
  - ✓ Por que fiscalização de TI e o papel do auditor
  - ✓ Atuação da Sefti/TCU
  - ✓ **Abordagens de auditoria de TI**
  - ✓ Normas e Padrões em ATI
- ✓ Introdução ao uso de CAATs
- ✓ Auditoria de Dados
  - ✓ Padrões de auditoria no TCU
  - ✓ Metodologia de auditoria de dados

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 Contratações de TI
- ✓ Auditoria de Segurança da Informação
- ✓ Auditoria de Dados
- ✓ Auditoria de Sistemas
- ✓ Outras variações: Políticas de TI, ERP, infraestrutura e tecnologia etc

Auditoria de Governança de TI

- ✓ Envolvimento da alta administração com aspectos de TI: orientar e dirigir
- ✓ iGovTi (criticidade x materialidade)
- ✓ Avalia também aspectos de gestão
  - ✓ Gestão dos serviços
  - ✓ Políticas
  - ✓ Processo de controle
  - ✓ Investimentos
  - ✓ Recursos
- ✓ ISO 38.500 e Cobit

Auditoria de Contratações de TI

- ✓ Avaliação incidental de contratos
- ✓ Conformidade
- ✓ Processo de planejamento e execução de aquisições de TI
- ✓ Gestão contratual
- ✓ Remuneração por resultados
- ✓ Efetividade (objetivos de negócio)

Auditoria de Segurança da Informação

- ✓ Gestão da segurança da informação
- ✓ Aderências às boas práticas
- ✓ Controles em SI
  - ✓ Confidencialidade, integridade e disponibilidade
  - ✓ Políticas e planos
  - ✓ Controle de acesso lógico e físico
- ✓ Normas GSI, NBR 27.002/2005, jurisprudência

Auditoria de Dados

- ✓ Avaliar integridade e confiabilidade dos dados, bem como sua conformidade para com as regras de negócio
- ✓ Cruzamentos de bases de dados
- ✓ Pode apoiar avaliação de risco
- ✓ Pode complementar outra abordagem
- ✓ Uso de CAATT

Auditoria de Sistemas

- ✓ Pode abordar aspectos de:
  - ✓ integridade, disponibilidade, confiabilidade, conformidade, controles internos
  - ✓ Entrada, processamento e saídas.
  - ✓ Usabilidade, satisfação
  - ✓ Objetivos do sistema frente aos objetivos de negócio
- ✓ Acompanhamento de sistemas em desenvolvimento
- ✓ Pode demandar conhecimento especializado

- ✓ Ex: matéria - módulo de consignações Siape

Outras variações...

- Políticas e programas governamentais na área de TI
  - A TI agrega valor ao negócio da administração pública?
  - A sociedade está sendo devidamente beneficiada?
- ERP
  - Ramo especializado da auditoria de sistemas
  - Grandes sistemas, interconexão, orientado a processos, dependência, grandes projetos
- Infraestrutura
  - Avaliação de ambiente de rede, banco de dados etc

Agenda

- ✓ Introdução à Auditoria de TI
  - ✓ Por que fiscalização de TI e o papel do auditor
  - ✓ Atuação da Sefti/TCU
  - ✓ Abordagens de auditoria de TI
  - ✓ **Normas e Padrões em ATI**
- ✓ Introdução ao uso de CAATs
- ✓ Auditoria de Dados
  - ✓ Padrões de auditoria no TCU
  - ✓ Metodologia de auditoria de dados

Normas e Padrões em ATI

- Constituição Federal
  - em especial, art. 37 (princípios da adm. pública)
- Legislação brasileira e demais normativos
- Cobit e ITIL (Governança, gestão, operação)
- Normas ISO/IEC:
  - 20000 (serviços de TI)
  - 27000 (segurança da informação)
  - 38500 (governança de TI)
- Outros Padrões
  - *Normas ISACA*

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
- ✓ LC 123/2006 – Direito de preferência

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

Outros normativos

- ✓ 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
- ✓ Tribunal de Contas da União (TCU)
  - Jurisprudência
- ✓ Órgãos governantes: CNJ, CNMP, CJF, DEST
- ✓ Associação Brasileira de Normas Técnicas (ABNT)
  - NBR ISO/IEC série 27000 e outras internalizadas no País
  - Padrões suplementares em áreas específicas

Lacunas na Legislação Brasileira

- ✓ Acesso não autorizado aos sistemas
- ✓ Interceptação não autorizada de informações
- ✓ Uso não autorizado de sistemas de informática
- ✓ Alteração de dado ou programa de computador
- ✓ Difusão de vírus eletrônico
- ✓ Quebra de privacidade de banco de dados
- ✓ PL-84/1999 (2793/2011) – Crimes na área de informática (aprovado CD)

Cobit

Cobit (*Control Objectives for Information and related Technology*) é conjunto de boas práticas em gestão de TI:

- ✓ 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 – (implantação e implementação de sistema de controles internos nas instituições financeiras)
- ✓ Lei americana Sarbanes-Oxley (SOX) de 2002 – *Section 404: Assessment of internal control*
- ✓ Jurisprudência TCU
  - ✓ Adoção de boas práticas do Cobit como critério de auditoria

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

Outras Normas Internacionais

- ✓ **ISO 12207** – Processo de Desenvolvimento de Software
- ✓ **ISO 15408** – Segurança de Aplicação (desenvolvimento)
- ✓ **ISO 15504** – Processo de Desenvolvimento de Software

Outras normas

Intosai (*International Organization of Supreme Audit Institutions*)

- ✓ aplicação não obrigatória
- ✓ representam consenso de boas práticas

Isaca (Information Systems Audit and Control Association)

- ✓ Aplicáveis a membros da associação

Outros institutos e organizações

Agenda

- ✓ Introdução à Auditoria de TI
  - ✓ Por que fiscalização de TI e o papel do auditor
  - ✓ Atuação da Sefti/TCU
  - ✓ Abordagens de auditoria de TI
  - ✓ Normas e Padrões em ATI
- ✓ **Introdução ao uso de CAATs**
- ✓ Auditoria de Dados
  - ✓ Padrões de auditoria no TCU
  - ✓ Metodologia de auditoria de dados

Técnicas e ferramentas de auditoria auxiliadas por computador

- ✓ Computer-Assisted Audit Techniques and Tools (CAATTs)
- ✓ Uso combinado de ferramentas e técnicas para automatizar o processo de auditoria

Motivação

- ✓ Automatização de tarefas repetitivas
- ✓ Sistemas com milhões de transações
- ✓ Amostras normalmente muito reduzidas
  - ✓ Uso de CAATs permite aplicação de testes de auditoria em até 100% das transações
- ✓ Maior tempestividade na realização de testes
  - ✓ Auditoria contínua
- ✓ Complexidade de fraudes e processos

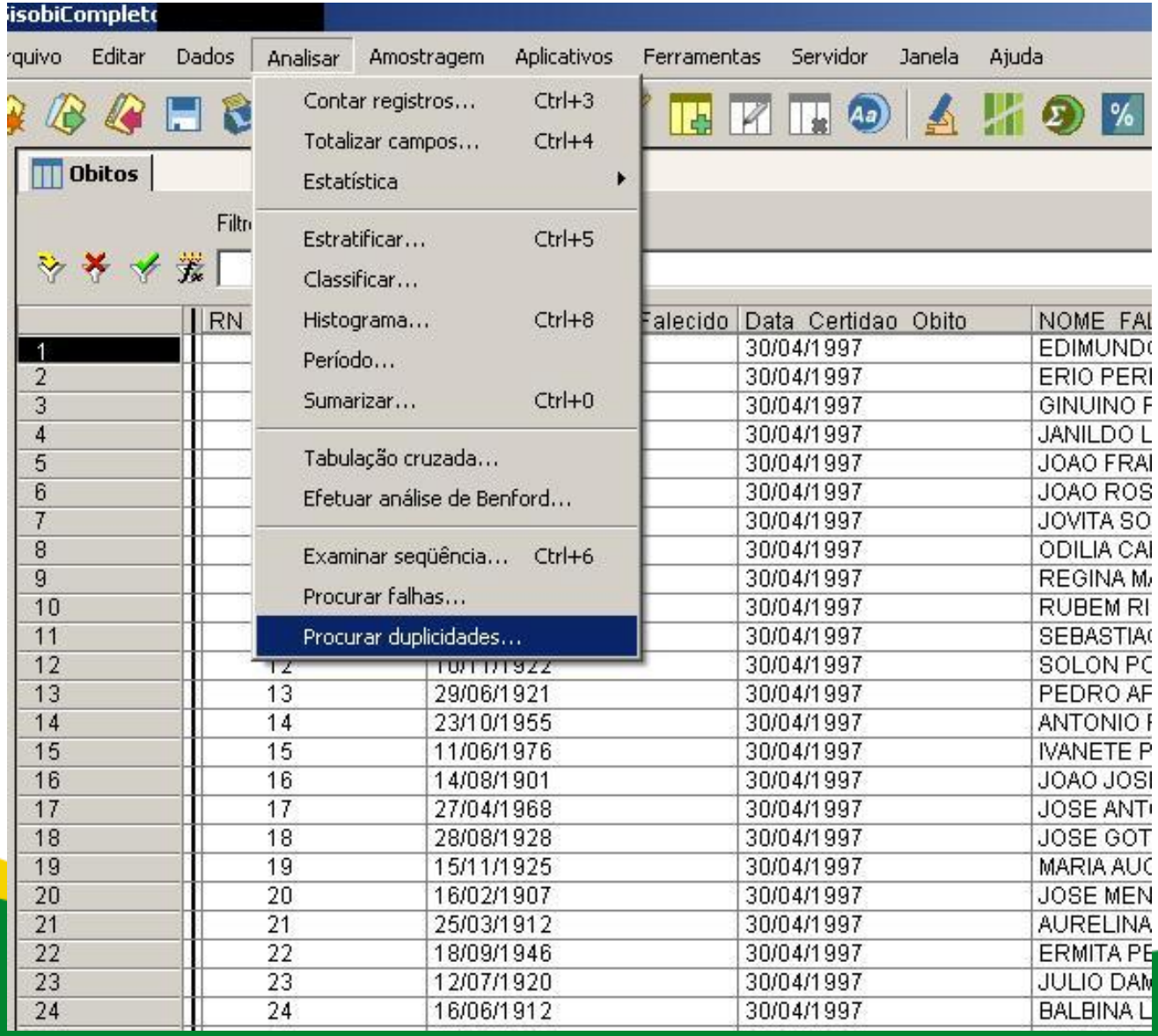
Exemplos: ferramentas de ...

- ✓ Escritório: processadores de texto, planilhas e de banco de dados (excel, access, openoffice)
- ✓ Análise estatística (SAS)
- ✓ Business Intelligence (BO)
- ✓ Análise e cruzamento de dados (ACL, Idea, Picalo)
- ✓ Testes de controles de segurança (ERP, infraestrutura)
- ✓ Testes de invasão
- ✓ Outras finalidades específicas

Funcionalidades e aplicações

- ✓ Permite teste de grande volume de transações
- ✓ Amostragem
- ✓ Análises estatísticas
- ✓ Cruzamento de arquivos
- ✓ Apóiam a documentação dos procedimentos
- ✓ Análise de sequências
- ✓ Simulação de cálculos
- ✓ Independência dos sistemas auditados
- ✓ Detecção de fraudes
- ✓ Testes analíticos

Exemplo de CAAT



IS Auditing Guideline: G3 Use of Computer-Assisted Audit Techniques

- ✓ Norma de auditoria de TI do ISACA
- ✓ Descreve aspectos específicos no uso de CAATs
  - ✓ Fatores de decisão para uso de CAATs
  - ✓ Planejamento
  - ✓ Considerações sobre a execução da auditoria
  - ✓ Documentação necessária
  - ✓ Elementos necessários no relatório

IS Auditing Guideline: G3 Use of Computer-Assisted Audit Techniques

Fatores de decisão para uso de CAATs

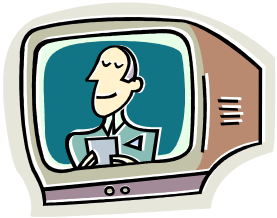
- ✓ Expertise
- ✓ Disponibilidade de ferramentas
- ✓ Eficiência das CAATs sobre técnicas manuais
- ✓ Limitações de prazo
- ✓ Nível de risco

IS Auditing Guideline: G3 Use of Computer-Assisted Audit Techniques

- ✓ Requisitos do planejamento
  - ✓ Definir objetivos no uso das CAATs
  - ✓ Avaliar disponibilidade de programas e dados
  - ✓ Definir os procedimentos que se deseja
  - ✓ Definir os requisitos de saída
  - ✓ Recursos necessários
  - ✓ Documentar
  - ✓ Negociação com o auditado
  - ✓ Testar as CAATs
  - ✓ Garantir segurança

Pausa para um vídeo!

- ✓ Exemplo de auditoria com uso de CAATTS
- ✓ Auditoria de dados
- ✓ Auditoria no MDS – Cadastro único
- ✓ Acórdão 906/2009-P
- ✓ Informativo
- ✓ Matéria TV:



Agenda

- ✓ Introdução à Auditoria de TI
  - ✓ Por que fiscalização de TI e o papel do auditor
  - ✓ Atuação da Sefti/TCU
  - ✓ Abordagens de auditoria de TI
  - ✓ Normas e Padrões em ATI
- ✓ Introdução ao uso de CAATs
- ✓ Auditoria de Dados
  - ✓ **Padrões de auditoria no TCU**
  - ✓ Metodologia de auditoria de dados

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.

Padrões de auditoria do TCU

- ✓ NAT – Normas de auditoria do TCU (2011)
- ✓ Manual de auditoria operacional
- ✓ Normas específicas (obras)
- ✓ Orientações Segecex
  - ✓ Levantamento, monitoramento, proposição de determinações
- ✓ Orientações FOC
- ✓ Outras disposições específicas

Padrões de auditoria do TCU

- ✓ Classificação
  - ✓ Conformidade
  - ✓ Operacional
- ✓ Modalidade
  - ✓ Levantamento
  - ✓ Inspeção
  - ✓ Auditoria
  - ✓ Monitoramento
  - ✓ Acompanhamento

Estrutura básica das auditorias

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

Levantamento

- ✓ Informações Iniciais:
  - Objetivos institucionais.
  - Legislação aplicável.
  - Avaliação do ambiente de controle
    - Falhas e riscos conhecidos
    - Estrutura organizacional.
    - Histórico de fiscalizações
  - Demanda apresentada
    - Comando de acórdão
    - TMS
    - Denúncia a ser apurada

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**

Matriz de planejamento (resumida)

Questões de Auditoria	Informações requeridas	Fontes de informação	Detalhamento do Procedimento	Possíveis Achados
Q 2. O controle de acesso do Sistema Sisobi dificulta o acesso não autorizado às informações de óbitos?	-Critérios para concessão e revogação de acessos e privilégios - Listas de usuários e respectivas permissões -Relação de cartórios existentes no Brasil	-Gestores -Normas de controle de acesso -Base de dados do Sisobi e de cartórios do CNJ	P2.2 – Verificar os procedimentos de concessão e revogação de acessos (usuários de cartórios e do INSS). P2.2.3 – Verificar como é feito o registro dos direitos de acesso concedidos e revogados. P2.2.7 – Verificar os usuários que possuam acesso vigente a mais de um cartório. Consultar os cartórios para identificar se tais pessoas ainda trabalham nos respectivos cartórios.	-Falta de procedimentos formalizados para concessão e revogação de acessos. -Pessoas que não trabalham mais nos cartórios continuam com acesso ao sistema

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;
  - Prudência ao relatar situações
  - Bom senso ao colocar achados de baixa relevância;
  - 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

- ✓ Linguagem mais técnica
- ✓ Evidências
- ✓ Relatório deve ser útil
- ✓ Detalhamento dos achados, riscos associados e recomendações
- ✓ Inclusão de gráficos e tabelas bem apresentados e contextualizados
- ✓ Equilíbrio entre concisão e a clareza no corpo principal do relatório (uso de apêndices se necessário, evitar o exagero de informações)

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.

Auditoria de Dados

Agenda

- ✓ **Objetivos.**
- ✓ Atuação do TCU
- ✓ Conceitos Básicos.
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento.
- ✓ Execução e relatório.
- ✓ Estudo de caso: Sisobi

Objetivos

- ✓ Compreender os principais conceitos, o enfoque e a aplicabilidade da auditoria de dados.
- ✓ Compreender como deve ser conduzida e que aspectos devem ser abordados numa auditoria de dados.
- ✓ Conhecer formas de atuação da Sefti/TCU em trabalhos de auditoria de dados.
- ✓ Discutir algumas questões de auditoria relacionadas à auditoria de dados.
- ✓ Conhecer alguns exemplos práticos de uso de CAATTs

A auditoria de dados

- Aborda os dados contidos em meios de armazenamento eletrônico a fim de se certificar se são íntegros, confiáveis e em conformidade com as leis que regem o negócio.
- Pode ser executado isoladamente ou de forma a complementar outra auditoria (ex.: auditoria de sistemas).
- Possibilita a verificação de até 100% das transações auditadas
- Permite o cruzamento de informações com outras bases de dados a fim de verificar os registros auditados.

Agenda

- ✓ Objetivos.
- ✓ Atuação do TCU
- ✓ Conceitos Básicos
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento.
- ✓ Execução e relatório.
- ✓ Estudo de caso: Sisobi

Alguns trabalhos do TCU...

- ✓ Sisobi/INSS (Ac. 2812/2009-P)
- ✓ Cadastro Único para programas sociais do governo federal no MDS (Ac. 906/2009-P)
- ✓ Avaliação do controle do trânsito de produtos florestais realizado por meio de sistema do Ibama (Ac. 309/2009-P)
- ✓ Incompatibilidade entre a jornada de trabalho de servidores e respectiva remuneração (Ac. 89/2008–P)
- ✓ Auditoria operacional em hospitais universitários do RJ (Ac. 473/2007-P);
- ✓ Sistema de Controle da Dívida Ativa da União (PGFN) (Ac. 3382/2010-P e 2994/2011-P)
- ✓ SIASG/ComprasNet (Acórdão 1.793/2011-P, em sede de recurso)

Agenda

- ✓ Objetivos.
- ✓ Atuação do TCU
- ✓ Conceitos Básicos
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento.
- ✓ Execução e relatório.
- ✓ Estudo de caso: Sisobi

Agenda

- ✓ Objetivos.
- ✓ Atuação do TCU
- ✓ Conceitos Básicos
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento.
- ✓ Execução e relatório.
- ✓ Estudo de caso: Sisobi

Campos de aplicação

- ✓ Análise exploratória
- ✓ Teste e avaliação de controles
- ✓ Detecção de fraudes
- ✓ Análise de trilhas de auditoria
- ✓ Auditoria contínua

Análise exploratória

- ✓ Auditoria de escopo ainda não delimitado
- ✓ Apoiar planejamento
- ✓ Avaliar criticidade e materialidade
- ✓ Estratificar os dados
- ✓ Identificar anomalias
- ✓ Percepção de risco e experiência do auditor
- ✓ Exemplos
  - ✓ Valores máximos e mínimos de contratos
  - ✓ Distribuição por tipos de licitação
  - ✓ Controles sobre datas
  - ✓ Estratificação por licitante, por modalidade

Teste e avaliação de controles

- Avaliar a eficácia dos controles internos
- Testar a conformidade para com as regras de negócio
- Análise de 100% das transações
- Pode ajudar na identificação das causas de falhas nos controles por meio da análise das transações não conformes
- Exemplos:
  - Modalidade de licitação x valor licitado
  - Número CPF válidos
  - Segurados da previdência estão vivos
  - Se as placas de automóveis indicadas nas multas se referem a automóveis válidos

Detecção de fraudes

- ✓ Possibilidade verificar indícios de fraudes
- ✓ Verificações dependem da área de negócio
- ✓ Estratificação de transações (por usuário, por departamento, por hórário etc)
- ✓ Uso de circularização (outras bases de dados)
- ✓ Incompatibilidade entre cargo e transações
- ✓ Análise de desvios e comportamento não esperado
- ✓ Transações mais vultosas
- ✓ Dependem de testes complementares, pois os dados são uma mera representação

Análise de trilhas de auditoria

- ✓ pode facilitar a análise de milhões de registros
- ✓ verificar autoria
- ✓ verificar ordem e sequência de transações
- ✓ verificar coerência entre arquivos de dados e log

Exemplo de uso

- ✓ Análise exploratória
- ✓ Aplicação de testes
- ✓ Uso de ferramenta

Dificuldades

- ✓ Delimitação de escopo
- ✓ Falta de qualidade dos dados armazenados
- ✓ Complexidade de processos de negócio e estruturas de dados (modelos com centenas de tabelas)
- ✓ Carência de documentação
- ✓ Estruturas de dados complexas ou mal organizadas
- ✓ Volume de transações (demanda por processamento)

Compreender o negócio é essencial!

Dificuldades

- ✓ Insuficiência de conhecimento a respeito da base de dados por parte da equipe responsável pela manutenção
- ✓ Sistemas de bancos de dados antigos
- ✓ Sigilo dos dados
- ✓ Oposição à extração dos dados (caso sistema de solicitações)
- ✓ Carência de recursos humanos para processar a extração
- ✓ Ausência de chaves comuns entre arquivos ou bases de dados

Indícios de problemas na confiabilidade dos dados

- documentação ausente ou precária;
- sistemas antigos, que exigem muita manutenção;
- estruturas de dados complexas e desorganizadas;
- alta rotatividade de pessoal e treinamento inadequado ou em escala insuficiente;
- falta de padrões para o processamento de dados, especialmente quanto à segurança, acesso e controle de mudança de programas.
  - (TCU, Manual de Auditoria de Sistemas, 1998)

Confiabilidade dos dados

"3.5.2 ... Quando os dados obtidos mediante sistemas informatizados forem parte importante da auditoria e a confiabilidade dos dados seja decisiva para o alcance do objetivo da fiscalização, os auditores devem certificar-se de que os dados são confiáveis e pertinentes".

(Intosai, Código de Ética e Padrões de Auditoria, 2001)

Confiabilidade dos dados (riscos)

- Os princípios de auditoria exigem que qualquer evidência (independentemente de sua fonte ou formato) seja confiável, relevante e suficiente.
- O risco de confiabilidade dos dados é definido como sendo *o "risco de que os dados utilizados não sejam suficientemente confiáveis para o fim a que se destinam"*, ou seja, o risco de que esses não sejam exatos e completos o suficiente para servir de fundamento para achados de auditoria.

  (TCU, Manual de Auditoria de Sistemas, 1998)

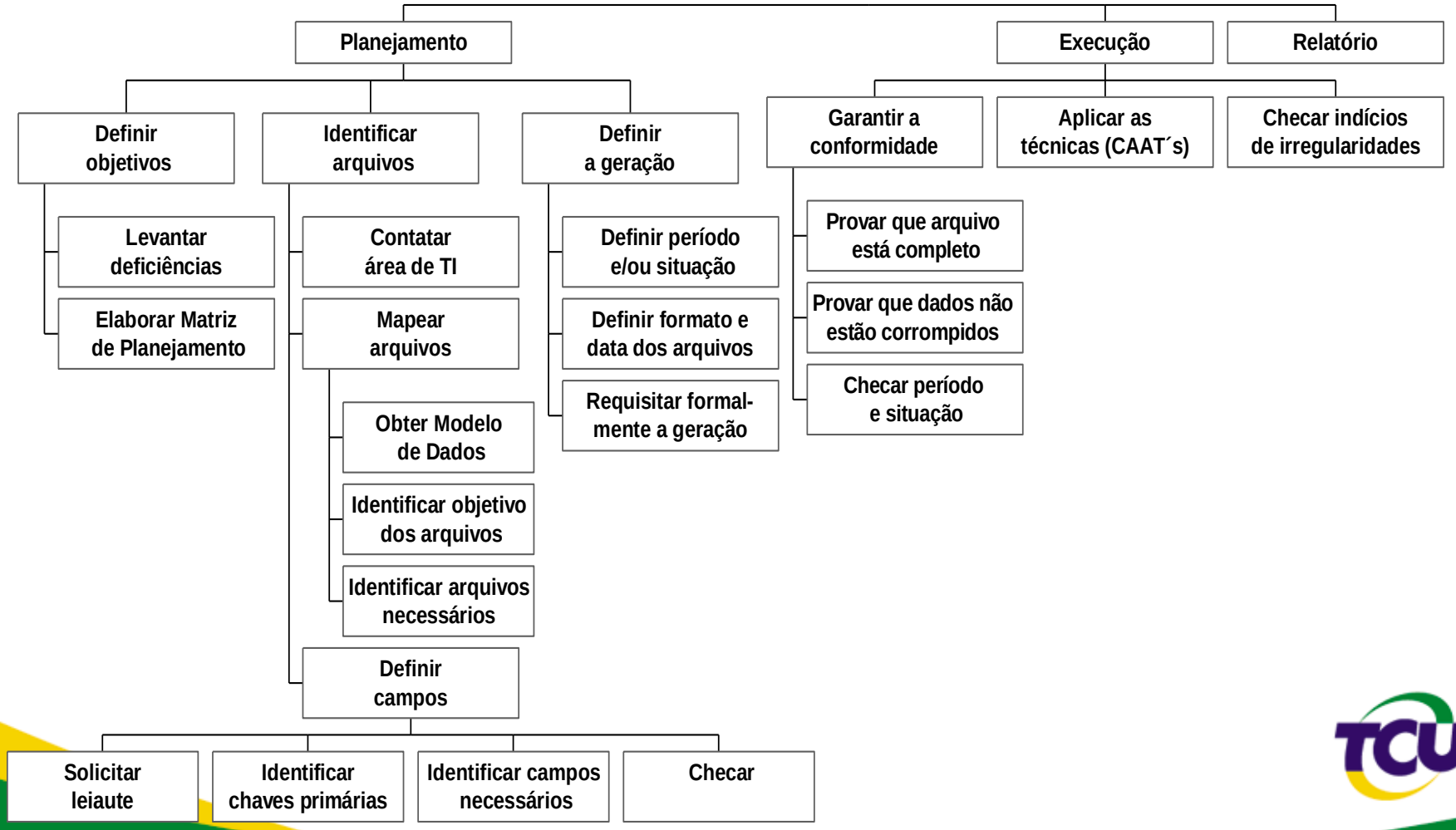
Benefícios

- ✓ Auditoria mais:
  - ✓ Eficiente
  - ✓ Eficaz
  - ✓ Abrangente
- ✓ Pode produzir uma redução do tempo para execução de auditoria posterior
- ✓ Pareceres mais conclusivos
- ✓ Resultados mais expressivos

Agenda

- ✓ Objetivos.
- ✓ Atuação do TCU
- ✓ Conceitos Básicos
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento
- ✓ Execução e relatório
- ✓ Estudo de caso: Sisobi

Escopo e Planejamento



Planejamento

Definir objetivos

- ✓ Definir questões de auditoria
- ✓ Definir procedimentos
- ✓ Identificar bases de dados e órgãos envolvidos
- ✓ Buscar definir os órgãos envolvidos e envolvê-los formalmente na fiscalização (portaria)

Planejamento

Identificar arquivos

- ✓ Obter modelos de dados e documentação
- ✓ Estudar arquivos
  - ✓ Compreender objetivo dos arquivos
  - ✓ Identificar chaves primárias
  - ✓ Selecionar campos de interesse
  - ✓ Compreender estrutura dos campos
- ✓ Definir campos de dados necessários
- ✓ Estimar tamanho da base gerada

Planejamento

Avaliar requisitos para custódia das informações

- ✓ Verificar disponibilidade de espaço em disco
- ✓ Consultar aspectos de sigilo e segurança das informações
- ✓ Providenciar ambiente seguro e adequado para processamento dos dados

Planejamento

Definir a geração

- ✓ Definir leiaute desejado
- ✓ Definir período dos dados
- ✓ Avaliar tamanho da base gerada
- ✓ Definir meio seguro para transmissão das informações (uso de criptografia, se necessário)
- ✓ Negociar e discutir demanda com o jurisdicionado (layout, prazos, entendimento)
- ✓ **Formalizar!**
  - ✓ **EXEMPLO DE OFÍCIO**

Escopo e Planejamento

- Observações na definição dos campos a serem obtidos
  - Verificar se estão faltando informações que seriam úteis.
  - Chaves primárias sempre devem ser recuperadas.
  - Campos calculados devem ser evitados. Deve-se dar preferência aos campos atômicos.
  - Os dados não obrigatoriamente estão armazenados na forma que aparecem nas telas e relatórios de sistemas informatizados.

Escopo e Planejamento

- Observações na definição da geração dos dados
  - ✓ O arquivo não deve, preferencialmente, ser um *back-up*.
  - ✓ Necessidade de fornecimento de layout dos arquivos junto aos dados.
  - ✓ Necessidade de recebimento de "*jobs*" de execução de geração de dados.
  - ✓ Considerar possibilidade de acompanhamento do processo de geração.

Escopo e Planejamento

Formatos de arquivos mais comuns

- ✓ ASCII de comprimento fixo
- ✓ Arquivos de escritório: Excel, Access, Openoffice
- ✓ Texto com campos separados por caracteres especiais, como vírgula, ponto e vírgula
- ✓ Formato natural gerado pelo SGBD (requer uma etapa adicional de importação para um SBGD compatível);
- ✓ Como última alternativa, relatório padrão ou elaborado para fins da auditoria, em meio magnético.

Escopo e Planejamento

- Observações finais da Fase de Planejamento
  - ✓ Maior duração do que outras abordagens de auditoria TI

    => Tempo para conhecer as bases de dados

  - ✓ Contatos, negociação e pedido de geração de bases pertencentes a órgãos não abrangidos pela auditoria devem ser feitos nesta fase, quando for o caso.

  - ✓ Considerar a interrupção da auditoria nesta fase

Requisição

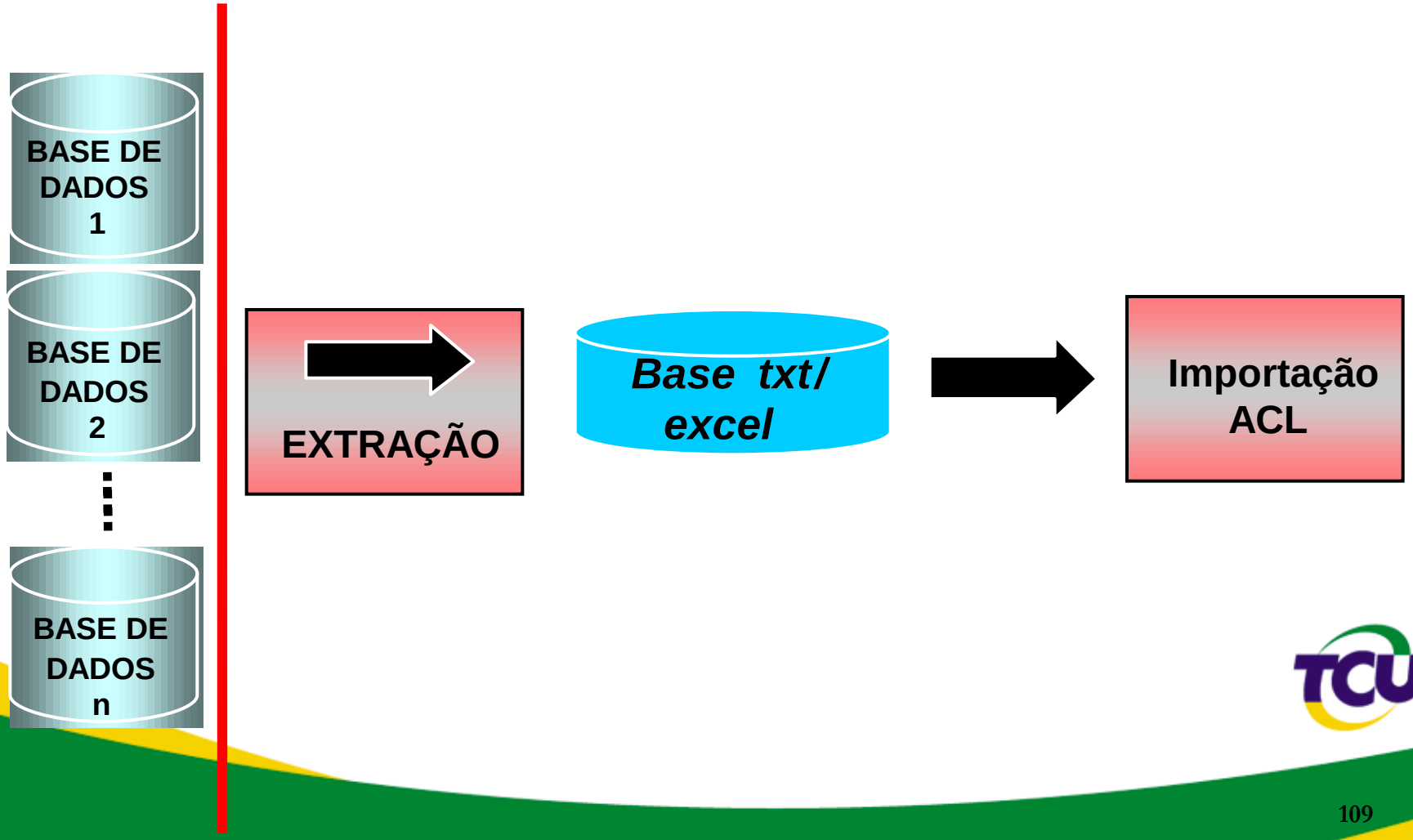
- Observações finais da Fase de Planejamento
  - ✓ Maior duração do que outras abordagens de auditoria TI

    => Tempo para conhecer as bases de dados

  - ✓ Contatos, negociação e pedido de geração de bases pertencentes a órgãos não abrangidos pela auditoria devem ser feitos nesta fase, quando for o caso.

  - ✓ Considerar a interrupção da auditoria nesta fase

Fluxo de geração de dados



Escopo e Planejamento

- Exemplo de layout de um arquivo

IT-IN-ATIVO	A 0001	
IT-CO-UNIDADE-GESTORA	N 0006	
IT-NO-UNIDADE-GESTORA	A 0045	
IT-NO-MNEMONICO-UNIDADE-GESTORA	A 0019	
IT-CO-UF		A 0002
GR-ORGAO	N 0005	

```
 020012SUBSECRETARIA DE EXPEDIENTE                    SSEXP                DF02000
 020024SUBSECRETARIA DE DIVULGACAO                    SSDIV                DF02000
 030014SECRETARIA CONTROLE EXTERNO EM MATO G DO SUL   TCU - SECEX/MS       MS03000
 030104TCU - 4A SECRETARIA DE CONTROLE EXTERNO        TCU - 4A SECEX       DF03000
 060006AUDITORIA DA 4A. CJM                           AUD. 4A. CJM         MG13000
 060029DIRETORIA DO FORO - 2A. CJM                    DIRET.FORO-2A CJM    SP13000
 070046COORDENADORIA DE CONTROLE INTERNO - TRE/PE     CCI-TRE/PE           PE14000
 110015SUBEX                                          SUBEX                DF20101
 110030DEPARTAMENTO DE SAUDE                          DEP.DE SAUDE         DF20101
 110055SUBCHEFIA PARA ACOMP.DA ACAO GOVERNAMENTAL     SUBCHEFIA P/A.A.GOVDF20101
 110073PROCURADORIA DA UNIAO NO ESTADO DA BAHIA/AGU   PU/BA                BA20114
 110090PROCUR. DA UNIAO NO ESTADO DE PERNAMBUCO/AGU   PU/PE                PE20114
I110204DIVISAO DE RECURSOS HUMANOS                    DIDAR                DF30201
I110238SUCURSAL SAO PAULO                             SUPAL                DF30201
 113205CENTRO DE DESENV.DA TECNOLOGIA NUCLEAR         CNEN/CDTN            MG20301
 114601FUNDACAO IBGE-ADMINISTRACAO CENTRAL/RJ         IBGE/ADM.CENTRAL/RJRJ25205
 114617UNIDADE ESTADUAL DO IBGE NA BAHIA              IBGE/UE/BA           BA25205
 114637COMPLEXO DA TIJUCA - CDDI-RIO DE JANEIRO       IBGE/TIJUCA/RJ       RJ25205
I118052RADIOBRAS-DIFERENCA DA INTEGRACAO              RADIOBRAS- D.I.      DF30201
```

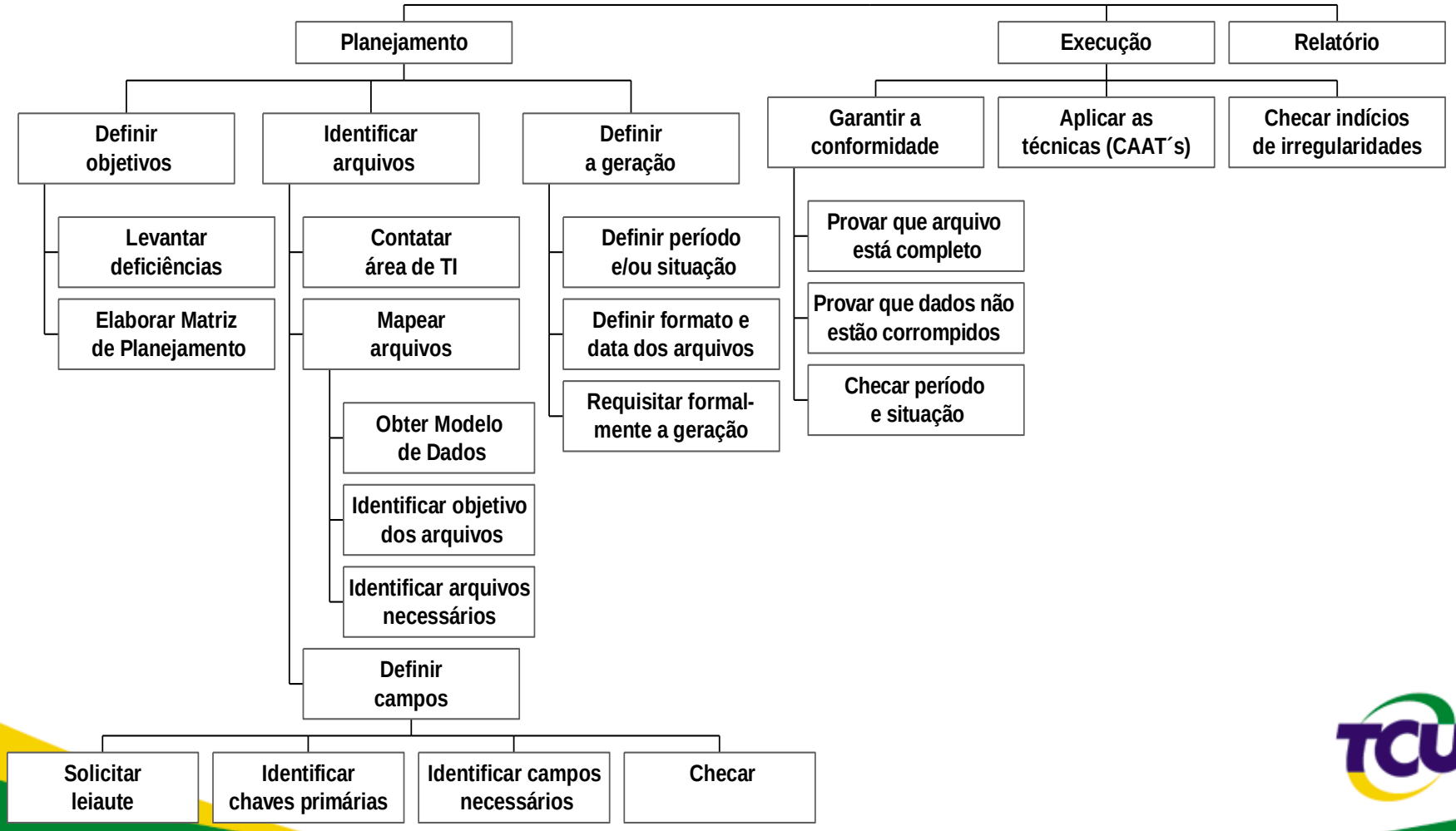
Agenda

- ✓ Objetivos.
- ✓ Atuação do TCU
- ✓ Conceitos Básicos
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento.
- ✓ Execução e relatório.
- ✓ Estudo de caso: Sisobi

Execução e relatório

- Observações sobre essas fases
  - ✓ Em geral, execução “in-house”
  - ✓ Uso de Caatts
  - ✓ Maior número de achados (relevância)
  - ✓ Irregularidades nos dados podem não necessariamente significar irregularidades na vida real. Devem ser interpretados como indícios!
  - ✓ Comprovação documental e confirmação dos indícios por outras fontes
    - ✓ Nova auditoria
    - ✓ Amostragem estatística
    - ✓ Amostragem por criticidade e materialidade
  - ✓ Fase de relatório da auditoria de dados não difere de outras auditorias.
    - ✓ Adicionar-se anexo de metodologia com detalhes dos cruzamentos

Execução e relatório



Execução

- Receber os arquivos e verificar integridade
  - Checar se o arquivo está completo
  - Verificar se não há dados corrompidos
  - Verificar período desejado
  - Efetuar checagens adicionais de acordo com os filtros aplicados
- Armazenar os arquivos de acordo com os requisitos de custódia
  - “As informações recebidas de pessoa física ou jurídica externa ao Tribunal devem ser classificadas de acordo com os requisitos de segurança da informação pactuados com quem as forneceu”. (Art. 2º, 3º, Resolução-TCU nº 229/2009 – Classificação da Informação)

Execução

- Efetuar procedimentos preparatórios
  - Efetuar “limpeza” nos dados
  - Efetuar normalização de arquivos
  - Criar índices e arquivos de resumo para aumento de performance
  - Criar identificadores únicos de registro
  - Documentar todos os procedimentos aplicados sobre os dados

Execução

- Executar os procedimentos (cíclicos)
  - Documentar os procedimentos aplicados (com uso de scripts, se disponível)
  - Executar os procedimentos
  - Avaliar os resultados

- Checar indícios de irregularidades

Execução (tipos de testes)

Tipos de testes

- Testes da **integridade** dos dados: determinam se o universo contém **todos** os elementos de dados e **registros relevantes** para o **objetivo de auditoria**, no período abrangido (exemplo, todos os pagamentos efetuados a um mesmo fornecedor).
- Testes de autenticidade dos dados: verificam se os dados computadorizados refletem com **exatidão sua fonte** (os registros de entrada de dados devem reproduzir fielmente os **documentos-fonte**).
- Testes de **exatidão do processamento**: informam se todos os registros relevantes foram processados de forma completa e se todos os **processamentos atenderam aos objetivos** pré-estabelecidos.

Relatório

- Documentar a metodologia aplicada:
  - Descrever bases utilizadas
  - Procedimentos de seleção dos arquivos e períodos
  - Procedimentos preparatórios
  - Cruzamentos e procedimentos realizados
  - Exemplos (script e metodologia)
- Escrever relatório
- Proteger anexos contendo dados e informações com uso de criptografia

Boas práticas

- Documentar a metodologia aplicada:
  - Descrever bases utilizadas
  - Procedimentos de seleção dos arquivos e períodos
  - Procedimentos preparatórios
  - Cruzamentos e procedimentos realizados
- Escrever relatório
- Proteger anexos contendo dados e informações com uso de criptografia

Possíveis questões

Objetivo de controle: assegurar que os dados contidos nas bases de dados são confiáveis

- ✓ As informações do Índice Nacional – IN – refletem as informações das bases de dados dos agentes de segurança pública? (Auditoria no Infoseg - Acórdão nº 71/2007-TCU-Plenário)
- ✓ Os cruzamentos do sistema do Cadastro Único com outros sistemas são efetivos para detectar a ocorrência de erros e fraudes no sistema? (Auditoria no CadÚnico - Acórdão nº 906/2009-TCU-Plenário)
- ✓ O sistema do Cadastro Único cumpre a legislação a ele aplicável? (Auditoria no CadÚnico)

Possíveis achados

- Inconsistências entre as bases de dados criminais e o Índice Nacional (Auditoria no Infoseg).
- Dados que evidenciam o não cumprimento à legislação (duas aposentadorias em cargos inacumuláveis na atividade – Auditoria no Siape)
- Divergência nas datas de óbitos entre bases pertencentes a diferentes instituições (auditoria no Sisobi)

Agenda

- ✓ Objetivos.
- ✓ Atuação do TCU
- ✓ Conceitos Básicos
- ✓ Oportunidades e dificuldades
- ✓ Escopo e Planejamento.
- ✓ Execução e relatório.
- ✓ Estudo de caso: Sisobi

Case Sisobi –Aspectos técnicos

- Auditoria de dados (apoiar a correção de deficiências na base de dados do Sisobi)
- Várias bases de dados: Sisobi, SIM, SUB, CPF, IBGE
- SUB: avaliar efetividade do Sisobi em seu objetivo maior
- Uso intensivo de cruzamento de dados entre as bases
- Diversas entrevistas para compreender organização das bases de dados (significado de campos)
- Amostragem (risco e materialidade) para pesquisas adicionais

Case Sisobi – Aspectos técnicos

- Plataforma alta (SUB) x Plataforma baixa (Sisobi)
  - diferenças nas estruturas de dados
  - diferenças na formatação de caracteres especiais (acentuação etc): joão x joao x jo#o
  - Diferenças na documentação
- Outro órgão gestor (SIM)
  - mais diferenças
- Tamanhos das bases de dados: vários arquivos com mais de 20, 30 milhões de registros
  - Produto cartesiano??

Case Sisobi – Aspectos técnicos

- Cruzamentos Sisobi x SUB x SIM
  - *Verificar problemas na concessão e manutenção de benefícios em decorrência de falhas nos registros de óbitos*
- Qual a chave adequada?
  - *Ausência de identificador comum de pessoas confiável (projeto RIC em curso)*
  - *Nome + ????*
  - *Equilíbrio entre risco de falsos-positivos e falsos-negativos*

Case Sisobi – Aspectos técnicos

- Grande esforço de documentação de scripts
- Documentação da metodologia em nível mais alto
- Testes adicionais (requisições ao INSS)
  - Prova de vida
  - Trecho do relatório Min. Augusto Nardes, Acórdão 2.812/2009-P

> *Pesquisa de vida do INSS indicou que a beneficiária faleceu há mais de 1 ano. Havia representante legal que era sua tia. Segundo a pesquisa, 'o cartão de recebimento ficou com seu sobrinho [...] que o sobrinho pegou o cartão dela [da representante legal] e o da segurada, para ajudar nas despesas de casa, pois as duas estavam na casa dele (pois a [...] [tia] tinha quebrado a perna) e depois que a sobrinha faleceu e ela melhorou e voltou para Unaí-MG, o sobrinho não quis devolver o cartão da segurada' (fls. 81 e 82, anexo 1)*

TRIBUNAL DE CONTAS DA UNIÃO

Obrigado!

Marcio Rodrigo Braz, Me.

brazmr@tcu.gov.br