TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Levantamento do referencial estratégico da Secretaria de Fiscalização de Tecnologia da Informação (Sefti)

República Federativa do Brasil

Tribunal de Contas da União

Ministros

Walton Alencar Rodrigues, Presidente
Ubiratan Aguiar, Vice-Presidente
Marcos Vinicios Vilaça
Valmir Campelo
Guilherme Palmeira
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz
Raimundo Carreiro

Auditores

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho

Ministério Público

Lucas Rocha Furtado, Procurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Maria Alzira Ferreira, Subprocuradora-Geral
Marinus Eduardo de Vries Marsico, Procurador
Cristina Machado da Costa e Silva, Procuradora
Júlio Marcelo de Oliveira, Procurador
Sérgio Ricardo Costa Caribé, Procurador

Negócio
Controle Externo da Administração Pública
e da gestão dos recursos públicos federais

Missão
Assegurar a efetiva e regular gestão dos
recursos públicos em benefício da sociedade

Visão
Ser instituição de excelência no controle e contribuir
para o aperfeiçoamento da Administração Pública

TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Levantamento do referencial Estratégico da Secretaria de Fiscalização de Tecnologia da Informação (Sefti)

Relator
Ministro Benjamin Zymler

Brasília, Brasil 2008

Impresso no Brasil / Printed in Brazil
<www.tcu.gov.br>

Para leitura deste Sumário Executivo, acesse o portal do TCU na Internet, no seguinte endereço: **<www.tcu.gov.br/fiscalizacaoti>**

Brasil. Tribunal de Contas da União.

Levantamento do referencial estratégico da Secretaria de Fiscalização de Tecnologia da Informação (Sefti) / Tribunal de Contas da União. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.

38 p. – (Sumários Executivos)

1. Auditoria. 2. Tecnologia da informação. I. Título. II. Série.

Catalogação na fonte: Biblioteca Ministro Ruben Rosa

SUMÁRIO

APRESENTAÇÃO

Devido à complexidade e à dimensão estratégica de que se reveste o tema *fiscalização de TI*, a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) do TCU, criada em 2006, necessitava obter informações acerca de boas práticas de fiscalização utilizadas por seus pares internos e externos para subsidiar a formulação de seu referencial estratégico. Com esse intuito, decidiu-se pela execução do levantamento objeto da presente publicação.

Os dados resultantes deste levantamento estão sendo utilizados na elaboração de indicadores da Sefti, na definição do seu referencial estratégico e na identificação, mapeamento e modelagem dos seus processos de trabalho.

Pretende-se, com a divulgação deste trabalho, oferecer às entidades pesquisadas e aos demais grupos interessados mais subsídios sobre o referido tema.

Esta publicação traz o resumo das principais informações coletadas em diversas entidades públicas e privadas, excluindo-se aquelas consideradas de caráter reservado, as quais permanecem constantes apenas no relatório original. O respectivo processo (TC-007.263/2007-0) foi apreciado em sessão do Plenário de 1º/8/2007, de caráter reservado, sob a relatoria do Ministro Benjamin Zymler, o qual autorizou a divulgação dos resultados dele decorrentes.

Walton Alencar Rodrigues
Ministro-Presidente

AGRADECIMENTOS

Os resultados deste levantamento decorrem da parceria que a equipe de auditoria estabeleceu com dirigentes e analistas de unidades técnicas do Tribunal de Contas da União (TCU) e com auditores das entidades externas pesquisadas. Ressalte-se que, desde a fase de planejamento deste trabalho, a equipe foi bem recebida nas unidades do Tribunal e nas entidades externas, e contou com a cordialidade e a colaboração dessas unidades durante as entrevistas, bem como na coleta de informações e documentos necessários ao desenvolvimento dos trabalhos do levantamento.

Agradece-se a colaboração dos dirigentes das unidades técnicas e dos chefes dos gabinetes do TCU participantes da pesquisa, e ainda dos funcionários das entidades externas visitadas, a seguir nominadas: Banco do Brasil, Banco Nacional de Desenvolvimento Econômico e Social, Bolsa de Mercadorias e Futuros, Bolsa de Valores de São Paulo, Bradesco, Caixa Econômica Federal, Câmara Interbancária de Pagamentos, Centrais Elétricas Brasileiras S.A., Comissão de Valores Mobiliários, Companhia de Processamento de Dados do Estado de São Paulo, Controladoria-Geral da União, Deloitte, Departamento de Auditoria Interna do Banco Central, Departamento de Polícia Federal, Departamento de Supervisão Direta do Banco Central, Empresa Brasileira de Correios e Telégrafos, Empresa de Tecnologia e Informações da Previdência Social, Ernest Young, Furnas Centrais Elétricas S.A., Instituto Nacional do Seguro Social, Itaú, Petróleo Brasileiro S.A., Serviço Federal de Processamento de Dados e Unibanco.

Também se agradece às Entidades de Fiscalização Superior (EFS) estrangeiras e aos Tribunais de Contas Estaduais (TCE) e Municipais (TCM) que colaboraram com a execução deste trabalho, respondendo tempestivamente aos questionários encaminhados.

RESUMO

Trata-se de levantamento de auditoria com objetivo de coletar informações para criação do referencial estratégico da Sefti, e identificar formas de atuação de entidades fiscalizadoras de TI. Com esse objetivo, foram definidas questões de auditoria que tivessem como resposta informações para criação de base de dados sobre fiscalização de TI, possíveis formas de atuação da Sefti e plano de divulgação das atividades da Sefti, consolidação do conteúdo e da estrutura da página da Sefti na Intranet/Internet, plano de desenvolvimento profissional para os servidores da Sefti, plano interno e externo de ação conjunta, conteúdo programático para concursos específicos para a Sefti, modelos de instrução, relatório e controle de qualidade, lista de ferramentas e de critérios aplicáveis a fiscalizações de TI.

Para levantar essas informações, foi necessário realizar entrevistas e enviar questionários a outras unidades do TCU e a algumas entidades externas. Assim, foram feitas entrevistas com representantes de 24 entidades externas e 46 unidades do TCU. Também foram recebidas respostas de 25 entidades internacionais de fiscalização superior e de 13 Tribunais de Contas Estaduais e Municipais.

Em todas as entrevistas e reuniões buscou-se registrar, de forma documental, as informações levantadas por meio do preenchimento de formulários pelos membros da equipe. Foram, ainda, encaminhados questionários para preenchimento pelos pesquisados e solicitadas informações complementares por meio de ofícios de requisição.

Após o recebimento das informações, a equipe analisou e consolidou os dados, gerando, como principais produtos, a base de dados sobre fiscalizações de TI e o levantamento das possíveis formas de atuação da Sefti, entre outros. Ressalte-se que este trabalho não gerou achados de auditoria e sim produtos, que serão detalhados nesta publicação. Da mesma forma, não houve volume de recursos fiscalizados e nem propostas de encaminhamento.

Os principais benefícios deste trabalho são a obtenção e a geração de conhecimento que permita a definição da forma de atuação da Sefti, condição essencial para que desempenhe sua missão de assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

OBJETIVOS DO LEVANTAMENTO

O objetivo deste levantamento foi levantar informações para criação do referencial estratégico da Sefti e identificar formas de atuação de entidades fiscalizadoras de Tecnologia da Informação (TI).

COMO SE DESENVOLVEU O TRABALHO

Durante a fase de planejamento, verificou-se que, para levantar todas as informações desejadas, seria necessário realizar entrevistas com pessoas de outras unidades do TCU e de algumas entidades externas, além de coletar informações via questionários.

Internamente, as entrevistas e questionários visaram buscar propostas de formas de atuação da Sefti, informações para construção do seu referencial estratégico e identificar as principais demandas de 46 unidades técnicas do Tribunal acerca de fiscalização de TI, dividindo-as em unidades finalísticas não especializadas, unidades finalísticas especializadas e unidades não finalísticas.

Além disso, foram feitas diversas reuniões internas na Sefti, envolvendo o secretário, os diretores, os analistas e os técnicos. Em todas as entrevistas e reuniões, buscou-se registrar, de forma documental, as informações levantadas por meio do preenchimento de formulários pelos membros da equipe, do encaminhamento de questionários para preenchimento pelos pesquisados e da solicitação formal de informações complementares por meio de ofícios de requisição.

Externamente, a meta da coleta de dados foi levantar boas práticas utilizadas por entidades que realizam fiscalização de TI, tanto do setor público quanto privado, visando aumentar a eficiência e eficácia da atuação da Sefti. Assim, para fazerem parte da pesquisa, foram relacionados órgãos, autarquias, empresas públicas, empresas privadas, entidades nacionais de fiscalização e entidades internacionais de fiscalização superior. Ao final,

foram entrevistados representantes de 24 entidades externas, e recebidas respostas a consultas de 25 entidades internacionais de fiscalização superior e 13 Tribunais de Contas Estaduais e Municipais, além da realização de reuniões com equipes de duas das principais empresas de auditoria do mercado.

Para selecionar as 24 entidades externas, buscaram-se informações e notícias sobre entidades que executam fiscalizações, fazem investimentos vultosos ou possuem grande dependência da área de TI para suporte e continuidade de seus negócios. Tal pesquisa resultou na seguinte relação: Banco do Brasil, Banco Nacional de Desenvolvimento Econômico e Social, Bolsa de Mercadorias e Futuros, Bolsa de Valores de São Paulo, Bradesco, Caixa Econômica Federal, Câmara Interbancária de Pagamentos, Centrais Elétricas Brasileiras S.A., Comissão de Valores Mobiliários, Companhia de Processamento de Dados do Estado de São Paulo, Controladoria-Geral da União, Deloitte, Departamento de Auditoria Interna do Banco Central, Departamento de Polícia Federal, Departamento de Supervisão Direta do Banco Central, Empresa Brasileira de Correios e Telégrafos, Empresa de Tecnologia e Informações da Previdência Social, Ernest Young, Furnas Centrais Elétricas S.A., Instituto Nacional do Seguro Social, Itaú, Petróleo Brasileiro S.A., Serviço Federal de Processamento de Dados e Unibanco.

Como limitação à execução dos trabalhos, citamos a impossibilidade física de entrevistar um número maior de entidades externas e de unidades técnicas do Tribunal, além do não-recebimento de todas as respostas em tempo hábil para análise.

PRODUTOS

Durante sua fase de planejamento, definiu-se que este levantamento deveria gerar os seguintes produtos:

1. Base de dados sobre fiscalização de TI;

2. Proposta de formas de atuação da Sefti;

3. Plano de divulgação permanente da Sefti;

4. Desenvolvimento profissional para os servidores da Sefti;

5. Oportunidades de atuação conjunta;

6. Proposta de seleção de novos servidores por meio de concurso público específico;

7. Levantamento de modelos e de procedimentos de fiscalização de outras unidades técnicas;

8. Lista de ferramentas de apoio a fiscalizações de TI;

9. Lista de critérios de auditoria de TI;

10. Controle de qualidade das fiscalizações da Sefti;

11. Proposta de conteúdo e de estrutura da página da Sefti no portal do TCU.

Devido ao caráter reservado de parte dessas informações, principalmente aquelas que se referem ao funcionamento interno das entidades entrevistadas e do próprio TCU, somente divulgamos nesta publicação informações relativas aos produtos 1, 4, 8 e 9, adaptando-os, conforme o caso.

BASE DE DADOS SOBRE FISCALIZAÇÃO DE TI

Seu objetivo é funcionar como um repositório de informações sobre normas, ferramentas, métodos, modelos e boas práticas utilizados pelas unidades técnicas do TCU e por entidades externas que executam trabalhos

de fiscalização interna ou externa. Após analisar os extratos das entrevistas e as respostas dos questionários, foram preparados produtos, alguns descritos a seguir, que servirão de base para o repositório.

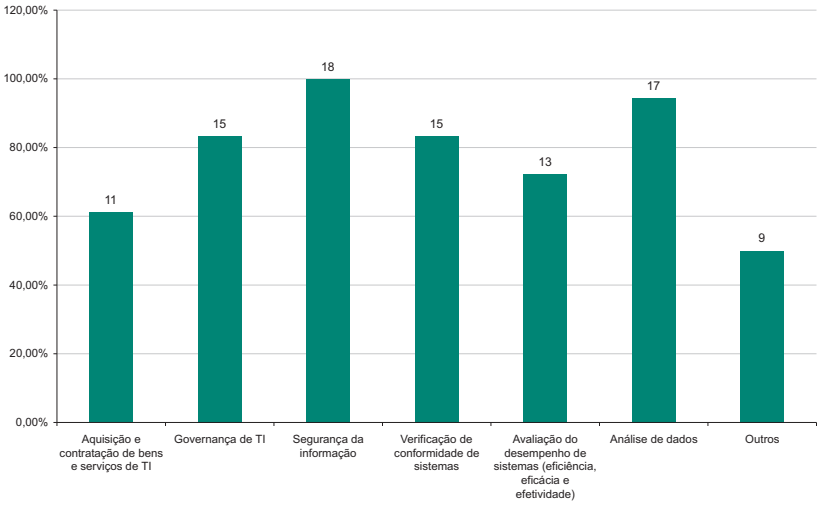
Relação das entidades fiscalizadoras de TI

Durante este trabalho, diversas entidades públicas e privadas que executam fiscalização de TI foram visitadas com intuito de criar uma rede de relacionamentos com seus auditores e abrir caminho para futuras trocas de informações e trabalhos conjuntos. A intenção do TCU de estreitar a cooperação técnica com outras entidades teve receptividade muito boa por parte dos entrevistados. Ao final, produziu-se uma lista de contatos externos, constante do relatório original, que servirá como base de consulta para futuras comunicações.

Relação das áreas de atuação das entidades fiscalizadoras de TI entrevistadas

Em relação ao universo de 24 entidades externas entrevistadas, foram identificadas 17 entidades que possuem 18 unidades especializadas em fiscalização de TI: Banco do Brasil, Banco Nacional de Desenvolvimento Econômico e Social, Bolsa de Mercadorias e Futuros, Bolsa de Valores de São Paulo, Bradesco, Caixa Econômica Federal, Centrais Elétricas Brasileiras S.A., Comissão de Valores Mobiliários, Departamento de Auditoria Interna do Banco Central, Departamento de Supervisão Direta do Banco Central, Empresa Brasileira de Correios e Telégrafos, Empresa de Tecnologia e Informações da Previdência Social, Furnas Centrais Elétricas S.A., Instituto Nacional do Seguro Social, Itaú, Petróleo Brasileiro S.A., Serviço Federal de Processamento de Dados e Unibanco. Essas unidades foram questionadas quanto a suas áreas de atuação e os resultados são apresentados no Gráfico 1.

Gráfico 1–Áreas de atuação das unidades de auditoria



O Quadro 1 apresenta o detalhamento das áreas de atuação das 18 unidades entrevistadas, por atividades específicas. Como cada unidade podia indicar mais de uma opção, o somatório dos percentuais em cada área pode ultrapassar 100%.

Quadro 1–Detalhamento das áreas de atuação

Áreas de atuação	Detalhamento	Quantidade	Percentual
Aquisição e contratação de bens e serviços de TI	Verificação de processos licitatórios	2	11,1%
	Verificação de sobrepreço e superfaturamento	3	16,7%
	Verificação de cláusulas contratuais (definição do objeto, níveis de serviço etc.)	11	61,1%
	Verificação do processo de execução e acompanhamento dos contratos	8	44,4%

Áreas de atuação	Detalhamento	Quantidade	Percentual
Governança de TI	Verificação e validação do planejamento de TI	11	61,1%
	Verificação do alinhamento das atividades de TI com o Plano Estratégico da Organização	9	50,0%
	Verificação do nível de terceirização de atividades críticas de negócio	10	55,6%
	Verificação do planejamento dos investimentos de TI	11	61,1%
	Verificação do retorno sobre investimentos feitos em TI	0	0,0%
	Outros	1	5,6%
Segurança da informação	Verificação de normas internas de segurança	14	77,8%
	Verificação de aderência da segurança da informação aos normativos padrão (NBR ISO/IEC 17799, ISO 27001, etc.)	16	88,9%
	Verificação dos processos de tratamento de incidentes de segurança	13	72,2%
	Testes de invasão	1	5,6%
	Testes de plano de continuidade de negócio	1	5,6%
	Testes de contingência	4	22,2%
	Verificação do funcionamento da gerência de mudanças	11	61,1%
	Outros	2	11,1%
Verificação de conformidade de sistemas	Aderência dos sistemas à legislação aplicável	14	77,8%
	Aderência à Metodologia de Desenvolvimento de Sistemas	13	72,2%
Avaliação do desempenho de sistemas (eficiência, eficácia e efetividade)	Verificação do atendimento das necessidades da organização	12	66,7%
	Verificação da satisfação dos usuários (usabilidade, navegabilidade, disponibilidade etc.)	10	55,6%
	Verificação de incidentes operacionais de sistemas	8	44,4%
Análise de dados	Verificação da consistência e confiabilidade dos dados	17	94,4%

Sobre os dados do Quadro 1, cabem alguns esclarecimentos:

- Os baixos percentuais de verificação de processos licitatórios, sobrepreço e superfaturamento se devem ao fato dessas atividades geralmente serem feitas por equipes da auditoria geral das entidades entrevistadas;

- O percentual de 0% (0) para verificação do retorno sobre investimentos feitos em TI (ROI) é decorrente do fato de, apesar de terem interesse pelo assunto, as equipes de auditoria entrevistadas encontrarem dificuldade para quantificar o ROI de TI, pois entendem que os benefícios gerados são muitas vezes intangíveis;

- A respeito dos testes de invasão, muitas equipes alegaram que é difícil e oneroso manter profissionais especializados nessa área e, por isso, preferem terceirizar esses testes;

- Quanto aos testes de plano de continuidade do negócio e de contingência, várias equipes se limitam a analisar os relatórios produzidos pelas unidades de TI, sem supervisionar a execução dos testes.

Também foram informadas outras áreas de atuação que não constavam do roteiro de entrevista:

- Verificação do processo de contratação e de treinamento do pessoal de TI;

- Verificação da realização de auditorias de sistemas;

- Verificação de documentos com informações sobre a arquitetura da informação;

- Verificação de aderência ao *Information Technology Infrastructure Library* (ITIL);

- Atuação em sindicâncias;
- Mapeamento dos controles de governança corporativa;
- Verificação do registro dos sistemas no Instituto Nacional de Propriedade Intelectual (INPI);
- Segurança de comércio eletrônico;
- Participação no Comitê de Segurança da Informação;
- Auditoria em parceiros de negócio;
- Acompanhamento do desenvolvimento de soluções tecnológicas.

Normas, ferramentas e manuais de fiscalização de TI

As normas aplicadas à fiscalização de TI mais citadas pelas entidades pesquisadas foram a NBR ISO/IEC 17799[1] em fiscalizações de segurança da informação, e o *Control Objectives for Information and Related Technology*[2] (Cobit) em trabalhos sobre governança de TI, enquanto que as ferramentas mais citadas foram o programa *Audit Command Language*[3] (ACL) para análise de dados e as ferramentas desenvolvidas pelas próprias entidades para suportar suas auditorias. Foram recebidos manuais de fiscalização de TI de algumas entidades, os quais serão analisados à época da revisão do manual de auditoria de sistemas, produzido pela Diretoria de Auditoria de Tecnologia da Informação (Dati) em 1998, citado como referência por órgãos da Administração Pública Federal, que aguardam sua atualização.

Plano de divulgação dos resultados das fiscalizações de TI

A equipe levantou de que forma a Controladoria-Geral da União (CGU), o Departamento de Polícia Federal (DPF), o TCU e as 18 unidades relacionadas anteriormente (p. 12) fazem essa atividade. Nenhuma das 18 unidades de auditoria entrevistadas faz divulgação externa de seus trabalhos. A divulgação de seus resultados se restringe aos auditados e às diretorias das respectivas entidades.

Quanto à CGU e ao DPF, que são órgãos que executam fiscalização externa, ambos possuem assessoria de comunicação e vêm alcançando bons resultados, utilizando linguagem não-jurídica de fácil entendimento para o público externo. Foi ressaltado que, para a mídia, especificamente em relação a aquisições de TI, importam quatro fatores: 1) O que foi comprado é necessário?; 2) O preço foi justo?; 3) O produto foi entregue?; 4) O produto foi utilizado?

Em relação às entidades que atuam na área financeira e de investimentos, por sua vez, alegaram que não têm interesse em divulgar os resultados de seus trabalhos, pois isso geraria especulações que afetariam negativamente os mercados.

Expectativas e sugestões das entidades quanto à forma de atuação da Sefti

A respeito da forma de atuação da Sefti, as 24 entidades externas entrevistadas (p. 10) fizeram algumas observações e sugestões, resumidas a seguir:

- O auditor de TI deve buscar a compreensão de todo o negócio antes da execução dos trabalhos de auditoria, sendo necessário fazer um pré-planejamento para mapear e descrever as funções de negócio que serão auditadas, delimitando a complexidade dos trabalhos. Somente depois deve ocorrer o planejamento e o detalhamento dos trabalhos de auditoria;

- O auditor de TI deve ser capaz não apenas de analisar os dados, mas também de fazer uma correta identificação dos fatos que podem gerar impacto. Isso visa impedir que sejam feitos trabalhos de auditoria desnecessários, somente de TI, que não agreguem valor ao negócio;

- A atuação da auditoria de TI deve ser multidisciplinar, pois envolve várias áreas de conhecimento. Concentrar esforços para manter uma equipe interna especializada para executar somente uma atividade específica, como testes de invasão, é muito caro e não garante bons resultados;

- A Sefti deve exigir que as entidades auditadas façam validação dos dados de entrada dos sistemas da Administração Pública Federal (APF), pois existem evidências de inconsistências nessas informações. A realização de fiscalizações nessa área pode gerar melhorias nesses sistemas e evitar fraudes;

- A Sefti deve implementar, com uso de ferramentas automatizadas, auditorias contínuas nas bases de dados da APF, centralizando, processando e cruzando informações em busca de fraudes;

- A Sefti deve estar atenta para a existência de despesas com serviços de informática prestados por terceiros que não estão discriminadas adequadamente no Sistema Integrado de Administração Financeira do Governo Federal (Siafi) e devem ser objeto de fiscalização;

- A Sefti deve promover o treinamento de auditores de TI de outros órgãos, divulgar suas técnicas de auditoria e os resultados de suas fiscalizações de TI. Além disso, deve criar fóruns e listas de discussão para que as equipes de auditoria de TI troquem experiências;

- A Sefti deve ter uma visão geral da situação da TI na APF, dando atenção especial para a análise de custo/benefício de suas recomendações/determinações, atuando na melhoria dos processos da APF e não apenas no controle dos gastos;

- A Sefti deve atuar na proposta de criação de um arcabouço legal, visando padronizar os trabalhos de auditoria de TI nos órgãos;

- A Sefti deve alavancar a governança de TI na APF, verificando se os dirigentes das entidades estão sensibilizados e comprometidos com as questões de segurança e governança de TI. As entidades devem ter uma missão bem definida e seus departamentos de TI devem estar alinhados a ela;

- O uso somente do Cobit não é solução para implantação da governança de TI, pois ele falha por não entrar em detalhes. Existem alternativas, como *o Systems Auditability and Control* (SAC) do *Institute of Internal Auditors* (IIA), que podem ser utilizadas para minimizar o problema;

- A Sefti deve manter contato com outras entidades de fiscalização de TI para execução de trabalhos conjuntos, troca de informações de interesse mútuo e para evitar a prescrição de fraudes e crimes. Para isso, deve formalizar essas parcerias para evitar que essas iniciativas se percam quando houver troca dos gestores;

- Para divulgar melhor os seus resultados, a Sefti deve interagir com outros órgãos, como o Ministério Público e a Polícia Federal, que possuem boa interação com a mídia e grande poder de divulgação.

Boas práticas sobre fiscalização de TI

Durante as entrevistas, foram identificadas as seguintes boas práticas sobre fiscalizações de TI:

- **Compreensão do negócio a ser auditado**: As equipes entrevistadas ressaltaram a importância de o auditor de TI compreender previamente os processos de negócio que serão auditados. Essa compreensão é fundamental para garantir que a auditoria aborde os aspectos mais importantes e agregue valor ao negócio suportado pela TI.

  Nesse sentido, identificou-se uma entidade que capacita seus auditores para, num único trabalho, fiscalizar vários aspectos relacionados a um mesmo processo de negócio (contábil, financeiro, operacional e TI). Em outros casos, há a formação de equipes multidisciplinares, compostas por auditores especialistas em TI e no negócio.

- **Auditoria de governança de TI**: Uma das principais áreas de atuação apontadas pelas unidades entrevistadas foi a governança de TI, auditada por 83,33% (15) das equipes por meio do Cobit, citado por 88,89% (16) das unidades. Esse percentual é bastante significativo, pois a governança de TI contribui para que as estruturas organizacionais e processos de tecnologia da informação das empresas sustentem e expandam os objetivos e estratégias corporativos.

- **Identificação do nível de maturidade das áreas de TI**: Essa identificação é feita por meio do mapeamento da situação da governança de TI das entidades com base no índice de maturidade do Cobit. Algumas entidades estão iniciando trabalhos nesse sentido para que possam conhecer a situação da área de TI, estabelecer metas futuras e traçar estratégias para alcançá-las.

- **Coleta prévia de informações para mapeamento de riscos de TI**: Uma das formas utilizadas para levantar informações sobre os

riscos de TI existentes nas entidades a serem auditadas é o envio de questionários, baseados no Cobit, a essas entidades. Ao responder os questionários, seguindo um roteiro para atribuição de notas, as entidades fazem uma auto-avaliação das suas áreas de TI. Com os resultados, mapeiam-se os riscos de TI existentes nas auditadas e cria-se o plano anual de auditoria.

- **Criação de ranking das entidades auditadas:** Uma das unidades entrevistadas utiliza os níveis de maturidade do Cobit para avaliar os riscos de TI das entidades sob sua jurisdição construindo, a partir daí, um ranking que evidencia as entidades que se encontram em situação mais vulnerável e que devem ser fiscalizadas com prioridade.

- **Certificação com selo de qualidade de TI**: Outra boa prática encontrada foi a identificação de uma unidade que fornece selos de qualidade para auditadas cuja área de TI se apresente em conformidade com os normativos pertinentes e siga um conjunto de boas práticas detalhadas pela certificadora por meio de roteiros. Trata-se de abordagem estrutural e operacional que busca conferir foco gerencial às principais atividades de TI e estabelecer atribuições essenciais para a infra-estrutura de suporte à operação do negócio. A obtenção desses selos não é obrigatória.

- **Auditoria contínua por meio do uso de rotinas automatizadas**: Foi identificado o uso de rotinas automatizadas de verificação de dados (rotinas *batch*), gerando relatórios diários para as áreas de controle, como, por exemplo, rotinas para verificação de catracas eletrônicas, folhas de pagamento e outros processos, centralizando e cruzando informações em busca de fraudes.

- **Utilização de sistemas de auxílio às fiscalizações de TI:** Foi observado que algumas unidades entrevistadas utilizam sistemas para auxiliá-las no planejamento, execução, elaboração de relatórios e acompanhamento das recomendações, sendo alguns adquiridos no

mercado e outros desenvolvidos pelas próprias entidades. Seu uso permite o armazenamento de programas de trabalho que podem ser reutilizados em outras auditorias. Além disso, muitos aplicam um *check-list* para verificação do preenchimento de itens obrigatórios dos relatórios, contribuindo para o controle de qualidade.

- **Utilização de sistema para gestão de riscos:** Foi identificada a utilização de um sistema de gestão de riscos que registra e acompanha controles implementados pelas áreas finalísticas, delegando as responsabilidades de controle, registrando as medidas adotadas e dando alertas sobre seu descumprimento. Esse sistema permite que a organização gerencie seus riscos, controles e objetivos de controle de forma organizada, sendo acessível via página *web*, possibilitando que todos os interessados no processo de gerenciamento de risco recebam comunicados ou acessem informações pertinentes.

- **Produção de *releases***: Os relatórios das fiscalizações de TI tendem a ser muito técnicos e de difícil entendimento para pessoas que não trabalham nessa área. Uma forma encontrada para facilitar a divulgação dos resultados dos trabalhos é a produção de *releases* em linguagem menos técnica e acessível ao público não especialista em TI.

- **Aplicar questionários de satisfação**: Com o objetivo de aprimorar a qualidade dos trabalhos de auditoria de TI, bem como fortalecer o relacionamento com os auditados, foram identificadas unidades que aplicam questionários com essa finalidade, junto aos auditados.

- **Acompanhamento *in loco* dos testes de contingência**[4]: Foram registrados casos em que as equipes de auditoria interna participam de acompanhamento *in loco* dos testes de contingência. Em contrapartida, foi observado que outras unidades fazem apenas controle indireto dos testes de contingência, por meio da análise de relatórios gerados pelas áreas de TI.

O fato de acompanhar diretamente os testes é importante, pois garante, ao auditor, que todas as etapas do teste foram efetuadas, que os participantes do processo conhecem bem seus papéis e que o resultado desejado foi alcançado.

- **Busca de certificações**: Identificou-se uma forte tendência das unidades buscarem certificações para melhorar a qualidade, a aceitação e o respaldo de seus trabalhos de auditoria interna.

- **Incentivo à pós-graduação**: De forma análoga às certificações, as unidades entrevistadas incentivam seus auditores a buscarem pós-graduação em auditoria de TI. Como não há muitos cursos desse tipo disponíveis, algumas unidades montaram uma grade própria e fecharam turmas exclusivas, alcançando resultado positivo.

DESENVOLVIMENTO PROFISSIONAL

Nesta etapa do levantamento, a equipe avaliou as habilidades e competências necessárias para o desenvolvimento de trabalhos na área de fiscalização de TI, recomendando as formas mais adequadas para alcançar essas competências.

Habilidades e competências para realizar fiscalizações de TI

Como referência para a definição das habilidades necessárias ao auditores de TI, a equipe utilizou as recomendações da *International Organization of Supreme Audit Institutions* (Intosai) publicadas no documento *IT Audit Curriculum – 2007* e na definição de competências realizada pelos dirigentes da Sefti.

O currículo de habilidades e técnicas de TI proposto pela Intosai baseia-se no universo de conhecimentos exigidos no programa de

certificação *Certified Information Systems Auditor* (CISA), promovido pela *Information Systems Audit and Control Association* (Isaca). O currículo, porém, não aponta explicitamente quais os treinamentos necessários para a aquisição dessas competências.

A Intosai define três perfis de auditores para atuação em TI. O primeiro perfil refere-se aos auditores generalistas, que têm conhecimento do negócio e estão também capacitados a utilizar técnicas e procedimentos mais simples de auditoria de TI e a solicitar objetivamente informações de um especialista em TI.

Os dois outros perfis tratados pela Intosai referem-se à especialização das atividades de auditoria de TI. Basicamente, as competências dos dois níveis referenciados, Auditor de TI e Auditor de TI Especialista, são as mesmas, diferenciando-se pela maior profundidade e amplitude de conhecimentos do Auditor Especialista. O Auditor de TI Especialista conhece, por exemplo, em maior profundidade e quantidade, os sistemas operacionais disponíveis no mercado. Dessa forma, esses dois perfis são indicados para os servidores da Sefti.

A Intosai agrupa as competências e habilidades dos auditores para atuação em TI em sete áreas:

- planejamento de auditoria de TI;
- avaliação de controles em sistemas de TI;
- técnicas de auditoria assistidas por computador (CAAT);
- auditoria em desenvolvimento ou aquisição de sistemas de TI;
- auditoria operacional em sistemas e atividades de TI;
- revisão e elaboração de relatórios em auditorias de TI;

- pesquisa, capacitação e assessoria.

A partir de trabalhos e estudos do próprio TCU, foram identificadas as seguintes competências como necessárias aos auditores no âmbito do Governo:

- análise e instrução de processos;
- auditoria de conformidade;
- auditoria de natureza operacional;
- análise de contratações em TI;
- análise sobre a utilização da tecnologia da informação;
- análise de bases de dados;
- análise de riscos de TI;
- gestão do conhecimento;
- gestão de projetos.

Certificados profissionais e cursos relacionados à área de Auditoria de TI e Segurança da Informação no âmbito governamental

Os certificados profissionais na área de Auditoria de TI e Segurança da Informação são uma forma prática de aquisição dos conhecimentos necessários ao desempenho das atividades dos auditores de TI. A obtenção de certificações reflete-se em maior credibilidade e aceitação dos trabalhos produzidos pela equipe, além de proporcionar o aprimoramento do conhecimento técnico dos seus membros.

Ressalta-se, porém, que as certificações de maior referência no mercado nacional e internacional não apresentam conteúdo em tecnologias específicas, mas sim asseguram que o profissional está apto na aplicação de determinadas habilidades. Dessa forma, faz-se necessário aos profissionais, além de adquirir os conhecimentos referenciados nos programas das principais certificações, também desenvolver os conhecimentos relacionados às diversas tecnologias aplicadas na Administração Pública Federal.

Apresentam-se, a seguir, as principais certificações e treinamentos recomendados:

- **Certificação *Certified Information Systems Auditor* (CISA)**: criada e mantida pela Isaca e tomada como referência no currículo da Intosai para o perfil de Auditor de TI. É referência mundial na área de Auditoria de TI, tendo, à época deste levantamento, mais de 50.000 profissionais certificados.

  O programa do CISA abrange as melhores práticas e conhecimentos necessários à eficiência no processo de auditoria de sistemas independentemente da tecnologia aplicada. Vem, dessa forma, ao encontro das necessidades de qualificação dos analistas lotados na Sefti, devendo ser a certificação prioritária a ser buscada.

- **Certificação *Certified Information Systems Security Professional* (CISSP):** considerada a mais respeitada certificação para profissionais em segurança da informação. Oferecida pelo *International Information Systems Security Certification Consortium* – (ISC), pode ser considerada como complementar ao CISA, ao abordar, de forma mais detalhada, temas específicos de segurança da informação, buscando, do profissional, uma forte base teórica nessa área de conhecimento.

- **Outras certificações:** Embora consideradas não prioritárias, certificações *Certified Information Security Manager* (CISM), da Isaca, e *Certified Internal Auditor* (CIA), do *Institute of Internal Auditors* (IIA). A primeira é voltada para profissionais com experiência em segurança da informação que atuam na área gerencial; a segunda, para atividades de auditoria interna, abordando, entre outros aspectos, os sistemas de informação.

- **Treinamento em *Control Objectives for Information and related Technology* (Cobit):** O Cobit é um guia dirigido para a governança de TI que independe das plataformas de TI adotadas nas organizações, do tipo de negócio, do valor e da participação que a tecnologia da informação tem na cadeia produtiva.

  Recomendado pela Isaca, também possui uma série de recursos que podem servir como modelo de referência para a auditoria da gestão da TI na APF. Especialistas em gestão e institutos independentes recomendam o uso do Cobit como meio para otimizar os investimentos de TI, melhorando o retorno sobre o investimento (ROI) percebido, fornecendo métricas para avaliação dos resultados.

- **Treinamento em *Information Technology Infrastructure Library* (ITIL):** Também um modelo que começa a ser adotado na APF, o ITIL é a referência para gerenciamento de processos de TI mais aceito mundialmente. Sua metodologia foi criada pela Secretaria de Comércio do governo inglês, a partir de pesquisas realizadas por consultores, especialistas e doutores, para desenvolver as melhores práticas para a gestão da área de TI nas empresas privadas e públicas. O foco desse modelo é descrever os processos necessários para gerenciar a infra-estrutura de TI de forma eficiente e eficaz.

- **Treinamento em ferramentas para análise de dados**: treinamento específico direcionado a uma ferramenta específica para análise e auditoria de bases de dados.

- **Treinamento em normas:** As normas da *International Organization for Standardization* (ISO) e da *Associação Brasileira de Normas Técnicas* (ABNT) constituem-se num dos principais critérios de auditorias. Dessa forma, é primordial que o conhecimento das características essenciais das normas mais relevantes, notadamente a NBR ISO/IEC 17799, que define um código de prática para a gestão da segurança da informação; a ISO 20000, que estabelece melhores práticas para o gerenciamento de TI, e a família de normas ISO 27000, que abordam os aspectos relevantes para a construção de sistemas de gestão de segurança da informação.

- **Treinamento em análise de contratos de TI:** treinamento para dotar os auditores com as habilidades necessárias para avaliar a legalidade e a legitimidade dos procedimentos de aquisição de bens e serviços de TI na APF, assim como a regularidade da celebração e da execução dos contratos firmados pelos diversos órgãos e entidades governamentais.

FERRAMENTAS DE APOIO A FISCALIZAÇÕES DE TI

As entidades estão cada vez mais dependentes dos sistemas de informação e das redes de computadores, utilizando ambientes heterogêneos e difíceis de serem mantidos, protegidos e controlados, tornando a auditoria de TI uma atividade complexa. Assim, com o constante aumento do volume de informações que devem ser analisadas, o auditor pode recorrer a Técnicas de Auditoria Assistida por Computador (CAAT) para aumentar a eficácia e eficiência de sua análise.

A seguir, será feita uma breve descrição das ferramentas citadas pelas entidades entrevistadas, divididas por finalidade.

Ferramentas de extração, manipulação e análise de dados

- **Audit Command Language (ACL)**: ferramenta que permite, de acordo com critérios estabelecidos pelos auditores, analisar dados de modo rápido e eficiente, apontando erros e fraudes potenciais;

- **Interactive Data Extraction and Analysis (Idea)**: ferramenta de análise de dados similar ao ACL;

- **Sql Query Analyser**: ferramenta administrativa utilizada para definição e manipulação de dados, usando a linguagem SQL;

- **Easytrieve**: linguagem de programação utilizada para confecção de programas que não requerem muito processamento, se caracterizando por possuir facilidade para manipulação de arquivos e emissão de relatórios;

- **Access**: software gerenciador de banco de dados;

- **Excel**: planilha eletrônica;

- **Python**: linguagem de programação interpretada utilizada para execução e automação de trabalhos e processamento de informação não estruturadas.

Sistemas de acompanhamento de recomendações

- **Sistema de Acompanhamento (follow-up)**: ferramenta desenvolvida pela própria entidade para acompanhamento do atendimento das recomendações de auditoria;

- **Sistema de Controle da Auditoria Interna (Sisaud)**: sistema interno desenvolvido por uma das entidades entrevistadas para

planejamento, monitoração e acompanhamento das recomendações de auditoria.

Ferramentas de análise de vulnerabilidades

- **GroupTools**: ferramenta para análise de e-mails;
- **Languard**: ferramenta para análise de segurança de redes;
- **Check-up tools (Risk Manager)**: ferramenta para análise de riscos de ativos tecnológicos;
- **Nessus Vulnerability**: ferramenta utilizada para testes de invasão que investiga as máquinas de uma rede à procura de vulnerabilidades, alertando para falhas de segurança.

Aplicativos de análise estatística

- **Statistical Package for the Social Sciences (SPSS)**: aplicativo de análise estatística avançada que, a partir de dados em forma de planilha, permite avaliações econométricas, regressões múltiplas e vários tipos de testes estatísticos com possibilidade de apresentação em gráficos diversos;
- **Statistical Analytics Software (SAS)**: aplicativo de análise estatística similar ao SPSS.

Sistemas de apoio a auditorias

- **Audit Automation Facility (AAF)**: ferramenta utilizada para auxílio na execução das auditorias, que possibilita o cadastro e execução de programas de auditoria;

- **Sistema de Auditoria (Siaud)**: solução interna desenvolvida por uma das entidades entrevistadas para auxiliar na execução das auditorias. Uma de suas características é que utiliza o Cobit como base e os objetivos de controle são cadastrados no sistema à medida que os programas de auditoria são executados. Além disso, funciona como um *check-list* de controle de qualidade.

CRITÉRIOS DE AUDITORIA DE TI

No Quadro 2, são apresentados os critérios de auditoria de TI citados pelas entidades entrevistadas, classificados de acordo com sua área de aplicação, em governança de TI, segurança da informação, engenharia de *software* e auditoria de TI.

Quadro 2–Critérios de auditoria de TI

Governança de TI		
Critério	Assunto	Onde encontrar
Cobit 4.1 – *Control Objectives for Information and Related Technology*	Modelo de referência para governança de TI	http://www.isaca.org/cobit
ITIL – *Information Technology Infrastructure Library*	Biblioteca de boas práticas em gerenciamento de serviços de TI	http://www.itil.co.uk/
ISO/IEC 20000-1:2005	Especificação para a gestão de serviço (ITIL)	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
ISO/IEC 20000-2:2005	Código de boas práticas para gestão de serviço (ITIL)	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
NBR ISO/IEC Guia 73:2005	Recomendações para uso em normas de gestão de riscos	http://www.abntnet.com.br/
Coso – *Committee of Sponsoring Organizations*	Estrutura de gerenciamento de riscos	http://www.coso.org/

Governança de TI		
Critério	Assunto	Onde encontrar
SOX – Lei Sarbanes-Oxley	Certificação da conformidade dos controles de TI com a SOX	http://www.pcaob.org/
BSC–*Balanced Scorecard*	Sistema de gestão estratégica de empresas	http://www.balancedscorecard.org/
ValIT	Estrutura para gerenciamento de investimentos em TI	http://www.isaca.org/valit
SAS70 – *Reports on the Processing of Transactions by Service Organizations*	Diretrizes para organização de serviços	https://www.cpa2biz.com/
e-SCM – *eSourcing Capability Model*	Modelo de gestão de terceirização de TI	http://itsqc.cs.cmu.edu/downloads/
Decreto nº 6.021, de 22 de jan. 2007	Cria a Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR), e dá outras providências.	http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Decreto/_decretos2007.htm
Segurança da Informação		
Critério	Assunto	Onde encontrar
NBR ISO/IEC 17799:2005	Código de boas práticas para gestão da segurança da informação	http://www.abntnet.com.br/
NBR ISO/IEC 27001:2005	Modelo de gestão da segurança da informação	http://www.abntnet.com.br/
ISO/IEC TR 13335-3:1998	Diretrizes para gestão da segurança em TI Parte 3: Padrão para análise de riscos	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
ISO/IEC TR 13335-4:2000	Diretrizes para gestão da segurança em TI Parte 4: Seleção de controles	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html

Segurança da Informação		
ISO/IEC TR 13335-5:2001	Diretrizes para Gestão da Segurança em TI Parte 5: Guia de gestão em segurança de redes	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
ISO/IEC 15408	Avaliação de requerimentos de segurança	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
BS 25999-1:2006	Código de boas práticas para gestão da continuidade do negócio	http://www.itgovernance.co.uk/products/632
Decreto nº 3.505, de 13 de jun. de 2000	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.	http://www.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm
Decreto nº 4.553, de 27 de dez. de 2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.	http://www.planalto.gov.br/ccivil_03/decreto/2002/Quadro_2002.htm
Engenharia de Software		
Critério	Assunto	Onde encontrar
MPS.BR – Melhoria do Processo de Software Brasileiro	Modelo de melhoria e avaliação de processo de software	http://www.softex.br/portal/mpsbr/_guias/default.asp
NBR ISO/IEC 12207	Processo de ciclo de vida de software	http://www.abntnet.com.br/
ISO/IEC 15504 – SPICE : *Software Process Improvement and Capability Determination*	Avaliação de processo de desenvolvimento de software	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
CMM – *Capability Maturity Model for Software*	Modelo de maturidade da capacitação para software	http://www.sei.cmu.edu/cmm/

Engenharia de Software		
CMMI – *Capability Maturity Model Integration*	Modelo de maturidade da capacitação para software Integrado	http://www.sei.cmu.edu/cmmi/
ISO/IEC TR 9126	Qualidade do produto	http://www.iso.org/iso/en/prodsservices/ISOstore/store.html
PMBOK – *Project Management Body of Knowledge*	Conjunto de boas práticas em gerência de projetos	http://www.pmi.org/
E-ping – Padrões de Interoperabilidade de Governo Eletrônico	Conjunto de especificações técnicas para interoperabilidade de serviços de governo eletrônico	http://www.governoeletronico.pr.gov.br/governoeletronico/arquivos/File/e-ping.pdf
Auditoria de TI		
Critério	Assunto	Onde encontrar
SAC–*Systems Auditability and Control*	Modelo para gerenciamento de riscos de TI complementar ao Cobit	http://www.theiia.org/guidance/technology/it-resources/it-security/
GTAG–*Global Technology Audit Guide*	Conjunto de publicações direcionadas a auditores internos	http://www.theiia.org/guidance/technology/gtag
Base de documentos da Isaca	Conjunto de padrões, guias e procedimentos da Isaca	http://www.isaca.org/Template.cfm?Section=Standards&Template=/TaggedPage/TaggedPageDisplay. cfm&TPLID=29&ContentID=8529
NBR ISO 19011:2002	Diretrizes para auditorias de sistemas de gestão da qualidade e/ou ambiental	http://www.abntnet.com.br/

No âmbito governamental, destacamos como relevante para auditoria de TI a análise das aquisições de bens e serviços de informática, que envolve desde o planejamento da contratação até a análise da execução dos contratos. Parte dessa legislação se aplica a todo tipo de contratação, como a Lei

nº 8.666/1993, e parte se aplica especificamente a contratações de TI, como o Decreto nº 1.070/1994, que dispõe sobre contratações de bens e serviços de informática e automação pela Administração Pública Federal.

Sobre esse assunto, apresentamos o Quadro 3 com as principais normas federais aplicadas às contratações de TI.

Quadro 3 – Normas federais aplicadas às contratações de TI

Norma	Data	Descrição	Onde encontrar
Lei nº 8.248/1991	23/10/1991	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.	http://www.planalto.gov.br/ccivil/Leis/L8248.htm
Lei nº 8.666/1993	21/06/1993	Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.	http://www.planalto.gov.br/ccivil/Leis/L8666cons.htm
Dec. nº 1.070/1994	02/03/1994	Regulamenta o art. 3° da Lei n° 8.248, de 23 de outubro de 1991, que dispõe sobre contratações de bens e serviços de informática e automação pela Administração Federal, nas condições que especifica e dá outras providencias.	http://www.planalto.gov.br/Ccivil_03/decreto/D1070.htm
Dec. nº 2.271/1997	07/07/1997	Dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.	http://www.planalto.gov.br/ccivil_03/decreto/D2271.htm
Dec. nº 3.555/2000	08/08/2000	Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.	http://www.planalto.gov.br/ccivil/decreto/D3555.htm

Norma	Data	Descrição	Onde encontrar
Dec. nº 3697/2000	21/12/2000	Regulamenta o parágrafo único do art. 2º da Medida Provisória nº 2.026-7, de 23 de novembro de 2000, que trata do pregão por meio da utilização de recursos de tecnologia da informação.	http://www.planalto.gov.br/ccivil/decreto/D3697.htm
Dec. nº 3931/2001	19/09/2001	Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e dá outras providências.	http://www.planalto.gov.br/CCIVIL/decreto/2001/D3931htm.htm
Lei nº 10.520/2002	17/07/2002	Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.	http://www.planalto.gov.br/ccivil/leis/2002/L10520.htm
Lei nº 11.077/2004	30/12/2004	Altera a Lei nº 8.248, de 23 de outubro de 1991, a Lei nº 8.387, de 30 de dezembro de 1991, e a Lei nº 10.176, de 11 de janeiro de 2001, dispondo sobre a capacitação e competitividade do setor de informática e automação e dá outras providências.	https://www.planalto.gov.br/ccivil/_Ato2004-2006/2004/Lei/L11077.htm
Dec. nº 5.450/2005	31/05/2005	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.	http://www.planalto.gov.br/ccivil/_Ato2004-2006/2005/Decreto/D5450.htm

Norma	Data	Descrição	Onde encontrar
Dec. nº 5.504/2005	05/08/2005	Estabelece a exigência de utilização do pregão, preferencialmente na forma eletrônica, para entes públicos ou privados, nas contratações de bens e serviços comuns, realizadas em decorrência de transferências voluntárias de recursos públicos da União, decorrentes de convênios ou instrumentos congêneres, ou consórcios públicos.	http://www.planalto.gov.br/CCIVIL_03/_Ato2004-2006/2005/Decreto/D5504.htm
LC nº 123/2006	14/12/2006	Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; (...) (...)Estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios.	http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp123.htm

BENEFÍCIOS DESTE LEVANTAMENTO

Espera-se que as informações coletadas neste levantamento sejam utilizadas na elaboração de indicadores da Sefti, na definição do seu referencial estratégico, na identificação, no mapeamento e na modelagem de seus processos de trabalho. O principal resultado da utilização do conhecimento gerado será a definição da forma e do conteúdo das atividades a serem desenvolvidas pela Secretaria para alcançar com efetividade a finalidade para a qual foi criada. Considera-se, também, que muitas das informações e boas práticas levantadas podem ser aproveitadas no âmbito de outras unidades do TCU, assim como por outras entidades fiscalizadoras de TI. A partir dos produtos deste levantamento, foi proposta uma estrutura de conteúdo da Sefti para o portal do TCU (http://www.tcu.gov.br/fiscalizacaoti), acessível aos públicos interno e externo do tribunal.

Os manuais e documentos recebidos durante as entrevistas subsidiarão a revisão do manual de auditoria de sistemas, produzido pela Dati em 1998, e no desenvolvimento de novas sistemáticas de auditoria no âmbito do Tribunal.

A Sefti tem como objetivo melhorar o controle externo da gestão e do uso de recursos de Tecnologia da Informação pela Administração Pública Federal, com vistas a assegurar a sua efetiva e regular aplicação em benefício da sociedade, e somente logrará esse êxito com a sustentabilidade de suas ações amparadas nos conhecimentos necessários à sua finalidade.

NOTAS

[1] Norma técnica da Associação Brasileira de Normas Técnicas sobre boas práticas de segurança da informação.

[2] Guia para a gestão de TI que inclui sumário executivo, framework, objetivos de controle, mapas de auditoria, conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.

[3] Programa de computador que auxilia auditores na realização de testes em arquivos de dados.

[4] Um plano de contingência tem o objetivo de descrever as medidas a serem tomadas por uma entidade, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos. Os testes de contingência têm como objetivo verificar a adequação do plano.

TRIBUNAL DE CONTAS DA UNIÃO
SAFS Quadra 4 lote 1
70042-900 Brasília-DF
<http://www.tcu.gov.br>

Responsabilidade Editorial

Secretário-Geral de Controle Externo
Jorge Pereira de Macedo

Secretário de Fiscalização de Tecnologia da Informação
Cláudio Souza Castello Branco

Equipe do Levantamento
Cláudia Augusto Dias (supervisora)
Harley Alves Ferreira
Rodrigo Machado Benevides (coordenador)
Tibério Cesar Jocundo Loureiro

Capa e Editoração

Secretaria-Geral da Presidência
Instituto Serzedello Corrêa
Centro de Documentação
Editora do TCU

Revisão de Texto
Focalize Eventos e Serviços Ltda.

Impresso pela Sesap/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

Endereço para contato e solicitação de exemplares

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Fiscalização de
Tecnologia da Informação (Sefti)
SAFS, Quadra 4, Lote 1
Anexo II, Sala 311
70042-900 – Brasília-DF
Fone: (61) 3316.5371/7396
Fax: (61) 3316.5372
sefti@tcu.gov.br

Secretaria de Fiscalização de Tecnologia da Informação

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.