ADVOCACIA-GERAL DA UNIÃO - AGU

ESCOLA DA AGU

CÂMARA DOS DEPUTADOS - CD

CENTRO DE FORMAÇÃO, TREINAMENTO E APERFEIÇOAMENTO - CEFOR

CONTROLADORIA-GERAL DA UNIÃO - CGU

SECRETARIA FEDERAL DE CONTROLE INTERNO - SFC

TRIBUNAL DE CONTAS DA UNIÃO - TCU

INSTITUTO SERZEDELLO CORRÊA - ISC

PROGRAMA DE PÓS-GRADUAÇÃO

Maíra Hanashiro

AUDITORIA DE TI NA CGU:

Proposta de Modelo de Implementação de Auditoria de Tecnologia da Informação no âmbito da Controladoria-Geral da União

Brasília

2009

Maíra Hanashiro

AUDITORIA DE TI NA CGU:

Proposta de Modelo de Implementação de Auditoria de Tecnologia da Informação no âmbito da Controladoria-Geral da União

Relatório técnico-científico apresentado para aprovação no curso de Especialização em Auditoria Interna e Controle Governamental do Instituto Serzedelo Corrêa do Tribunal de Contas da União.

Orientador: André Luiz Furtado Pacheco

Brasília

2009

Autorização

Autorizo a divulgação do texto completo no sítio da Câmara dos Deputados, da TCU, da AGU e da CGU a reprodução total ou parcial, exclusivamente, para fins acadêmicos e científicos.

Assinatura: _____

Data: ____/____/_____

Hanashiro, Maíra.
Auditoria de TI na CGU [manuscrito]: proposta de modelo de implementação de auditoria de tecnologia da informação no âmbito da Controladoria-Geral da União / Maíra Hanashiro. -- 2009.
95 f.

Orientador: André Luiz Furtado Pacheco.
Impresso por computador.
Trabalho de conclusão de curso – Relatório técnico-científico (especialização) -- Escola da AGU, da Advocacia-Geral da União, Centro de Formação, Treinamento e Aperfeiçoamento (Cefor), da Câmara dos Deputados, Secretaria Federal de Controle Interno (SFC), da Controladoria Geral da União e Instituto Serzedello Corrêa (ISC), do Tribunal de Contas da União, Curso de Especialização em Auditoria Interna e Controle Governamental, 2009.

1. Brasil. Controladoria-Geral da União (CGU). Secretaria Federal de Controle Interno (SFC). 2. Auditoria, Brasil. 3. Tecnologia da informação, Brasil. I. Título.

CDU 336.126.5:004(81)

Auditoria de TI na CGU: Proposta de Modelo de Implementação de Auditoria de Tecnologia da Informação no âmbito da Controladoria-Geral da União

Monografia – Curso de Especialização em Auditoria Interna e Controle Governamental do Instituto Serzedelo Corrêa do Tribunal de Contas da União – 2º Semestre de 2009.

Aluno: Maíra Hanashiro

Banca Examinadora:

André Luiz Furtado Pacheco

Francisco Eduardo de Holanda Bessa

Brasília, de 2009.

Esse trabalho é dedicado a
todos que combatem a corrupção no País
e lutam por uma administração
mais eficaz, eficiente e efetiva
dos recursos públicos.

Agradeço a Deus por tudo,
a minha mãe Vera pelo constante apoio,
a meu namorado Rafael pelo incentivo,
ao meu orientador André pelo direcionamento,
aos professores desse Curso pelas novas visões apresentadas,
aos colegas do Curso pelo apoio e companheirismo,
aos queridos amigos que participaram ativamente desse projeto,
a minha Coordenadora e a meus colegas de trabalhos pela compreensão
e aos Coordenadores-Gerais e servidores que contribuíram
tão prontamente com a coleta de informações.
Obrigada a todos vocês!

"Felicidade é quando
o que você pensa,
o que você diz
e o que você faz
estão em harmonia."
(Gandhi)

RESUMO

Diante dos altos investimentos em Tecnologia da Informação (TI) no contexto da Administração Pública e da importância da utilização eficiente e eficaz da Tecnologia da Informação para auxiliar no alcance dos objetivos das instituições públicas, é crescente a necessidade de Auditorias de TI. Por isso, esse trabalho tem como finalidade primária apresentar uma proposta para a implantação formal de um modelo de Auditoria de TI no âmbito da Controladoria-Geral da União (CGU), especificamente, dentro da Secretaria Federal de Controle (SFC). Antes disso, a fim de se identificar as fragilidades de Auditoria de TI dentro da SFC, é apresentado um diagnóstico realizado por meio de entrevistas e aplicação de questionários junto aos Coordenadores-Gerais e aos servidores de TI das áreas finalísticas. Tal diagnóstico detectou fragilidades no âmbito da SFC no que diz respeito a esse tipo de auditoria, tais como: subaproveitamento dos servidores de TI nas ações de controle de TI; baixo nível de maturidade do processo de Auditoria de TI dentro das Coordenações pesquisadas; falta de capacitação nessa área de atuação; ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI; e inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC. Após a detecção das fragilidades, são abordadas as características funcionais e organizacionais das Unidades temáticas da SFC a fim de verificar quais também poderiam ser aplicadas ao modelo proposto. Por fim, com o propósito de se eliminar ou mitigar as fragilidades da Auditoria de TI dentro da CGU e considerando os benefícios de se tratar cada auditoria como um novo projeto, foi apresentado um modelo de escritório de projetos de Auditoria de TI para a SFC, bem como suas características básicas e os requisitos iniciais para sua criação.

Palavras-chave: Controladoria-Geral da União, Secretaria Federal de Controle Interno, Tecnologia da Informação, Auditoria de TI, escritório de projetos.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
AFC	Analista de Finanças e Controle
APF	Administração Pública Federal
CF88	Constituição Federal de 1988
CGU	Controladoria-Geral da União
COBIT	*Control Objectives for Information and Related Technology*
CRG	Corregedoria-Geral da União
DC	Diretoria de Planejamento e Coordenação das Ações de Controle
DCOPE	Coordenação-Geral de Operações Especiais
DCPLA	Coordenação-Geral de Planejamento e Avaliação
DCREX	Coordenação-Geral de Recursos Externos
DCTEQ	Coordenação-Geral de Técnicas, Procedimentos e Qualidade
DE	Diretoria da Auditoria da Área Econômica
DEDIC	Coordenação-Geral de Auditoria das Áreas de Desenvolvimento, Indústria e Comércio Exterior
DEFAZ I	Coordenação-Geral de Auditoria da Área Fazendária I
DEFAZ II	Coordenação-Geral de Auditoria da Área Fazendária II
DEPOG	Coordenação-Geral de Auditoria dos Programas das Áreas de Planejamento, Orçamento e Gestão
DI	Diretoria de Auditoria da Área de Infra-Estrutura
DIAMB	Coordenação-Geral de Auditoria da Área do Meio Ambiente
DICIT	Coordenação-Geral de Auditoria das Áreas de Ciência e Tecnologia
DIENE	Coordenação-Geral de Auditoria da Área de Minas e Energia
DIINT	Coordenação-Geral de Auditoria da Área de Integração Nacional
DITRA	Coordenação-Geral de Auditoria da Área de Transportes
DIURB	Coordenação-Geral de Auditoria da Área de Cidades
DP	Diretoria de Auditoria de Pessoal, Previdência e Trabalho
DPPAS	Coordenação-Geral de Auditoria da Área de Previdência Social
DPPCE	Coordenação-Geral de Auditoria da Área de Pessoal e Benefícios e de Tomada de Contas Especial
DPSES	Coordenação-Geral de Auditoria da Área de Serviços Sociais
DPTEM	Coordenação-Geral de Auditoria das Áreas de Trabalho e Emprego
DR	Diretoria de Auditoria da Área de Produção e Tecnologia
DRAGR	Coordenação-Geral de Auditoria das Áreas de Agricultura, Pecuária e Abastecimento
DRCOM	Coordenação-Geral de Auditoria da Área de Comunicações
DRCULT	Coordenação-Geral de Auditoria da Área de Cultura
DRDAG	Coordenação-Geral de Auditoria da Área de Desenvolvimento Agrário
DRTES	Coordenação-Geral de Auditoria das Áreas de Turismo e Esportes
DS	Diretoria de Auditoria da Área Social

DSDES	Coordenação-Geral de Auditoria da Área de Desenvolvimento Social
DSEDU I	Coordenação-Geral de Auditoria da Área de Educação I
DSEDU II	Coordenação-Geral de Auditoria da Área de Educação II
DSI	Diretoria de Sistemas e Informação
DSSAU	Coordenação-Geral de Auditoria da Área de Saúde
DSSEG	Coordenação-Geral de Auditoria das Áreas de Justiça e Segurança Pública
GSTI-DR	Grupo de Soluções em Tecnologia da Informação da Diretoria de Auditoria da Área de Produção e Tecnologia
GSTIN	Coordenação-Geral de Auditoria de Tecnologia da Informação
INTOSAI	*International Organization of Supreme Audit Institutions*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
LDO	Lei de Diretrizes Orçamentárias
NBR	Norma Brasileira
ODP	Observatório da Despesa Pública
OGU	Orçamento Geral da União
PDG	Programa de Dispêndios Globais
PL	Projeto de Lei
PLC	Projeto de Lei da Câmara
PLS	Projeto de Lei do Senado
PMBOK	*Project Management Body Of Knowledge*
PMI	*Project Management Institute*
PMO	*Project Management Office*
SEFTI	Secretaria Fiscalização de Tecnologia da Informação
SFC	Secretaria Federal de Controle
SIAFI	Sistema Integrado de Administração Financeira do Governo Federal
SLTI/MP	Secretaria de Logística de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão
SOF/MP	Secretaria de Orçamento Federal do Ministério do Planejamento, Orçamento e Gestão
SPCI	Secretaria de Prevenção da Corrupção e Informações Estratégicas
TCU	Tribunal de Contas da União
TFC	Técnico de Finanças e Controle
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, a exemplo do que ocorre no setor privado, as atividades do setor público têm se tornado cada vez mais dependentes de processos de Tecnologia da Informação (TI) e das informações geradas por eles.

Dentro da Administração Pública Federal (APF) brasileira, há investimentos na ordem de bilhões de reais para capacitação e modernização tecnológica, uma vez que a TI é necessária em todos os Órgãos da APF, seja como base operacional para as demais demandas da unidade, seja como fator provedor de informação essencial à sua função precípua.

Assim, a área de Tecnologia da Informação tem se tornado estratégica para toda Administração Pública. Entretanto, por ser uma área relativamente nova, possui ainda, na maioria dos Órgãos, controles internos deficientes. Diante disso, é essencial que esses controles sejam fortalecidos.

Como a Controladoria-Geral da União (CGU) é o Órgão Central do Sistema de Controle Interno do Poder Executivo da Administração Federal, torna-se importante que o Órgão dê maturidade às ações de controle de Auditoria de TI.

Portanto, o desafio deste trabalho é apresentar uma proposta para a implantação formal de um modelo de Auditoria de TI no âmbito da Controladoria, especificamente, dentro da Secretaria Federal de Controle (SFC).

Como justificativas para a proposta apresentada destacam-se a atual situação da TI no contexto da Administração Pública, a importância da Auditoria de TI para a utilização eficiente e eficaz da Tecnologia da Informação e a real situação desse tipo de auditoria dentro da Administração Pública.

A fim de se fazer um diagnóstico da situação da Auditoria de TI no âmbito da SFC, identificando-se as fragilidades e a necessidade da Auditoria de TI, foi realizada uma pesquisa de opinião, com aplicação de questionários, junto a 20 Coordenadores-Gerais das áreas finalísticas da SFC e junto a 44 servidores com conhecimento em TI que atuam nessas Coordenações. Os resultados dessa pesquisa serão apresentados nesse trabalho, servindo de motivação para a proposta do modelo apresentado.

O ponto principal desse modelo é a criação de um escritório de projetos de Auditoria de TI, que terá como objetivo ser um núcleo de realização de ações de controle[1], decisões estratégicas, capacitação e apoio técnico acerca desse tipo de auditoria.

Esta proposta de trabalho de conclusão de curso tem como objetivos específicos:

1) Fazer um diagnóstico da Auditoria de TI dentro da Secretaria Federal de Controle Interno.
2) Apresentar proposta de modelo para implementação de Auditoria de TI no âmbito da CGU.

Complementarmente, podem ser citados os seguintes objetivos secundários:

1) Levantar a discussão dentro da SFC sobre a criação de Coordenações voltadas a temas específicos, como TI, obras e convênios, a fim de complementar os trabalhos realizados pelas Coordenações voltadas a Ministérios, aumentando a qualidade das ações de controle de assuntos específicos.
2) Contribuir para a conscientização dos Gestores Públicos na melhoria da Governança de TI e da Segurança da Informação em todos os Órgãos Públicos.
3) Contribuir para a demonstração da necessidade de legislação específica que regule a TI dentro da APF, a fim de exigir que critérios de Segurança da Informação e Governança de TI sejam aplicados em todos os Órgãos.

Esse trabalho está organizado da seguinte forma:

O Capítulo 2 aborda a importância da Tecnologia da Informação no atual contexto da Administração Pública, a importância da realização de ações de controle sobre a utilização da TI e a situação da Auditoria de TI dentro da Administração Pública, com ênfase no Tribunal de Contas da União (TCU).

O Capítulo 3 trata da apresentação do resultado da pesquisa que buscou diagnosticar a situação da Auditoria de TI no contexto da SFC do ponto de vista dos Coordenadores-Gerais das áreas finalísticas e dos servidores com conhecimento em Tecnologia da Informação.

O Capítulo 4 apresenta quatro Unidades da CGU voltadas para o tratamento de temas específicos.

---

[1] As ações de controle executadas pelo Sistema de Controle Interno do Poder Executivo Federal podem ser classificadas em dois grupos de técnicas de trabalho:

a) auditoria: da avaliação técnica, operacional e/ou legal da gestão pública e da aplicação dos recursos públicos por entidades de direito público ou privado.

b) fiscalização: trata-se da verificação da existência e adequação dos produtos das ações de governo.

O Capítulo 5 apresenta, como forma de buscar a solução dos problemas apresentados no Capítulo 3, a proposta de um escritório de projetos de Auditoria de TI na estrutura organizacional da SFC.

Por fim, o Capítulo 6 apresenta as conclusões desse trabalho, as dificuldade e limitações enfrentadas para sua elaboração e as sugestões de trabalhos futuros.

2 TECNOLOGIA DA INFORMAÇÃO E SEUS CONTROLES NO CONTEXTO DA APF

Neste capítulo, far-se-á uma abordagem sobre a Tecnologia da Informação dentro da Administração Pública. Em seguida, tratar-se-á da importância da Auditoria de TI e, por fim, apresentar-se-á brevemente a situação da Auditoria de TI nesse contexto.

2.1 A Tecnologia da Informação no contexto da Administração Pública

Em 2008, o Tribunal de Contas da União realizou um trabalho de levantamento de gastos em TI na APF (TCU, 2008a). Esse levantamento verificou que os gastos identificáveis em TI dentro da APF cresceram de 4,2 a 6,5 bilhões de reais, de 2002 a 2006, como pode ser observado na Tabela 2.1 e na Figura 2.1, ambas retiradas do Relatório do TCU (2008a):

Descrição	2002	2003	2004	2005	2006
Subelementos de TI (OFSS)	2.036.284.489,57	1.870.242.033,40	2.322.875.424,48	2.572.695.553,92	2.657.370.973,08
Subfunção Tecnologia da Informação excluídos os subelementos de TI	1.024.551.927,07	971.216.010,01	621.302.338,78	912.656.959,51	1.060.686.897,57
Empresas Estatais	1.090.337.577,00	1.468.532.159,00	1.781.696.550,00	1.686.118.044,00	1.515.333.994,00
SERPRO (subfunção 126)	(no OFSS)	(no OFSS)	843.174.107,53	1.043.704.402,63	1.292.195.461,67
Total	**4.151.175.995,64**	**4.309.992.205,41**	**5.569.050.424,79**	**6.215.176.965,06**	**6.525.589.332,32**
Crescimento anual	-	4%	29%	12%	5%
Crescimento em relação a 2002	-	4%	34%	50%	57%

Fonte: SIAFI Gerencial, Dest (Anexo II, fls. 164/167) e BGU

Tabela 2.1 – Gasto Total em TI na APF.

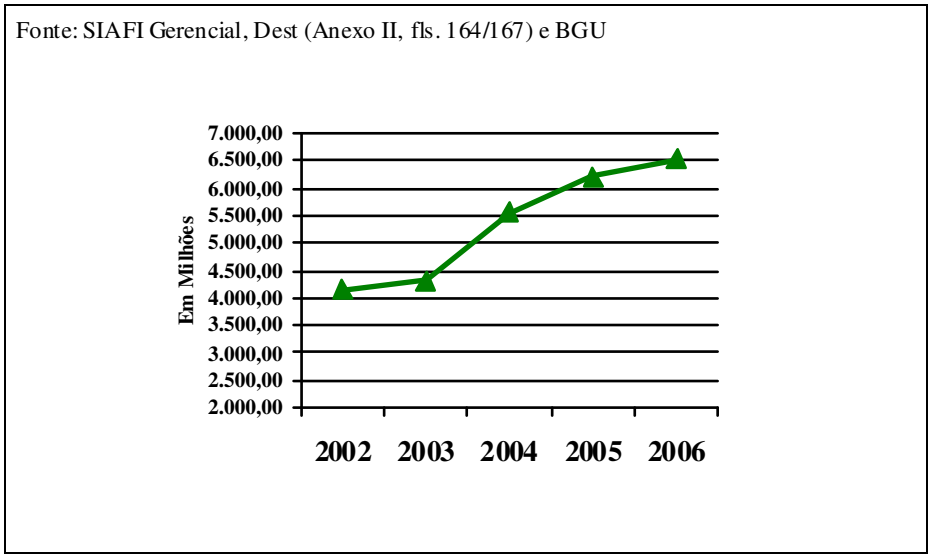


Figura 2.1 – Gasto Total em TI - Evolução

Para estimar os gastos de TI do Orçamento Geral da União (OGU), realizou-se a soma das despesas realizadas na subfunção Tecnologia da Informação (126), dos gastos efetuados em subelementos específicos de TI e dos gastos das Estatais, esses últimos contidos no Orçamento de Investimento por meio da mesma função (126) e no Programa de Dispêndios Globais (PDG) por meio de rubricas próprias de TI. A distribuição desses gastos pode ser observada na Figura 2.2:

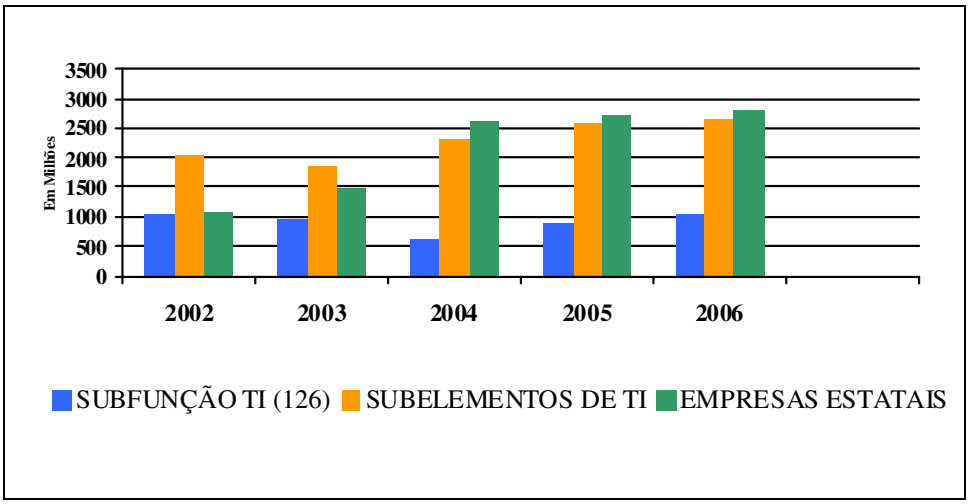


Figura 2.2 - Gasto Total em TI - Distribuição

Entretanto, apesar da realização dessa estimativa, verificou-se que a estrutura do OGU não permite a identificação precisa dos gastos em TI por não conter classificações orçamentárias específicas para todos os tipos de bens e serviços relacionados ao domínio de Tecnologia da Informação, assim como pela dispersão desses dispêndios nas ações finalísticas e de apoio de cada Órgão ou Entidade, restando sem identificação parcela significativa dos gastos em TI.

Como resultado desse trabalho, em atendimento à determinação do TCU (Acórdão nº 371/2008 – Plenário), a Secretaria de Orçamento Federal (SOF/MP) incluiu na Lei de Diretrizes Orçamentárias (LDO) 2009 dispositivo próprio à categorização de despesas com TI. Já o Departamento de Coordenação e Governança das Empresas Estatais (DEST/MP) promoveu a inclusão de rubricas específicas para a área de TI nos Programas de Dispêndios Globais das Instituições Financeiras e do Setor Produtivo Estatal.

Todavia, apesar de as estimativas de gastos já serem elevadas, a importância da Tecnologia da Informação para a Administração Pública não está apenas nos recursos utilizados diretamente na sua aquisição e manutenção. Muitas vezes, mais valiosa do que a própria TI é a informação gerida por ela. Por exemplo, o valor do Sistema Integrado de Administração Financeira do Governo Federal (SIAFI) (STN, 2009b), instrumento para controle e acompanhamento dos gastos públicos,

cresce vertiginosamente se forem considerados todos os recursos por ele geridos e os riscos envolvidos caso o Sistema apresente problemas operacionais e de segurança da informação. Nesse caso, qual seria o prejuízo se o banco de dados do SIAFI e seu *backup* fossem destruídos? Esse prejuízo seria muito maior do que valor dos recursos aplicados em seu desenvolvimento e manutenção, pois significaria a perda de todas as informações referentes às movimentações financeiras do Governo Federal.

Entretanto, não bastam o reconhecimento da necessidade da TI e o aumento dos investimentos se não houver uma aplicação correta e gerenciada destes recursos, de forma que a TI atenda às necessidades de negócio de cada Entidade, ou seja, agregue valor às suas funções finalísticas.

Assim, à medida que a tecnologia exerce influência direta sobre os produtos da Organização, a TI e as informações geradas por meio dela deixam de ser uma questão meramente operacional e administrativa para se tornar uma questão estratégica. Um dos grandes problemas observado nas organizações públicas é a falta de soluções para selecionar, processar e organizar a grande quantidade de informação disponível a um administrador (gestor), de modo a torná-las úteis no controle da gestão pública.

Além da necessidade do gestor, há também aquela do cliente que, para a organização pública, é o cidadão, que vem, cada vez mais, exigindo eficiência e transparência na gestão dos recursos públicos.

Com isso, surge, dentro da Administração Pública, a necessidade de implementação da Governança de TI[2] (IT GOVERNANCE INSTITUTE, 2007), de forma a alinhar o uso da TI aos objetivos de negócio de cada Órgão e da Administração como um todo, possibilitando que se garanta:

i. a continuidade dos serviços;
ii. o atendimento a marcos regulatórios;
iii. a definição clara do papel da TI dentro dos Órgãos;
iv. o alinhamento dos processos operacionais e de gestão a padrões que atendam a necessidade do negócio; e
v. a definição de regras claras acerca de responsabilidades sobre decisões e ações dentro da Entidade.

[2] Governança de TI é um conjunto de estruturas e processos que visa garantir que a TI suporte e maximize adequadamente os objetivos e estratégias de negócio da organização, adicionando valores aos serviços entregues, balanceando os riscos e obtendo o retorno sobre os investimentos em TI.

Essas garantias tornam-se essenciais e obrigatórias em um contexto em que a Informação torna-se muito mais acessível e, portanto, menos protegida. A disponibilidade das informações possibilita o aumento da eficácia e da eficiência de todos os processos que as utiliza. Por outro lado, se não houver garantia de que a manipulação de tais informações é monitorada e realizada de forma responsável, esta disponibilidade torna-se uma ameaça para a segurança da informação.

Importante salientar ainda que a Governança de TI não é uma disciplina isolada, ela é parte integral da Governança Corporativa[3]. O aumento da demanda por transparência e conformidade faz com que a Direção da Organização estenda a governança para a TI e forneça liderança, estruturas organizacionais e processos que assegurem que as estratégias de TI sustem e cubram as estratégias e objetivos do Órgão.

Em 2008, o TCU publicou um sumário executivo (TCU, 2008b) com os resultados sobre o levantamento da Governança de TI na APF realizado pela Secretaria de Fiscalização em TI (Sefti), com o objetivo de coletar informações acerca dos processos de aquisição de bens e serviços de TI, de segurança da informação, de gestão de recursos humanos de TI, e das principais bases de dados e sistemas da Administração Pública Federal.

Participaram dessa pesquisa 255 Órgãos/Entidades da APF, sendo que os principais achados são apresentados na Figura 2.3:

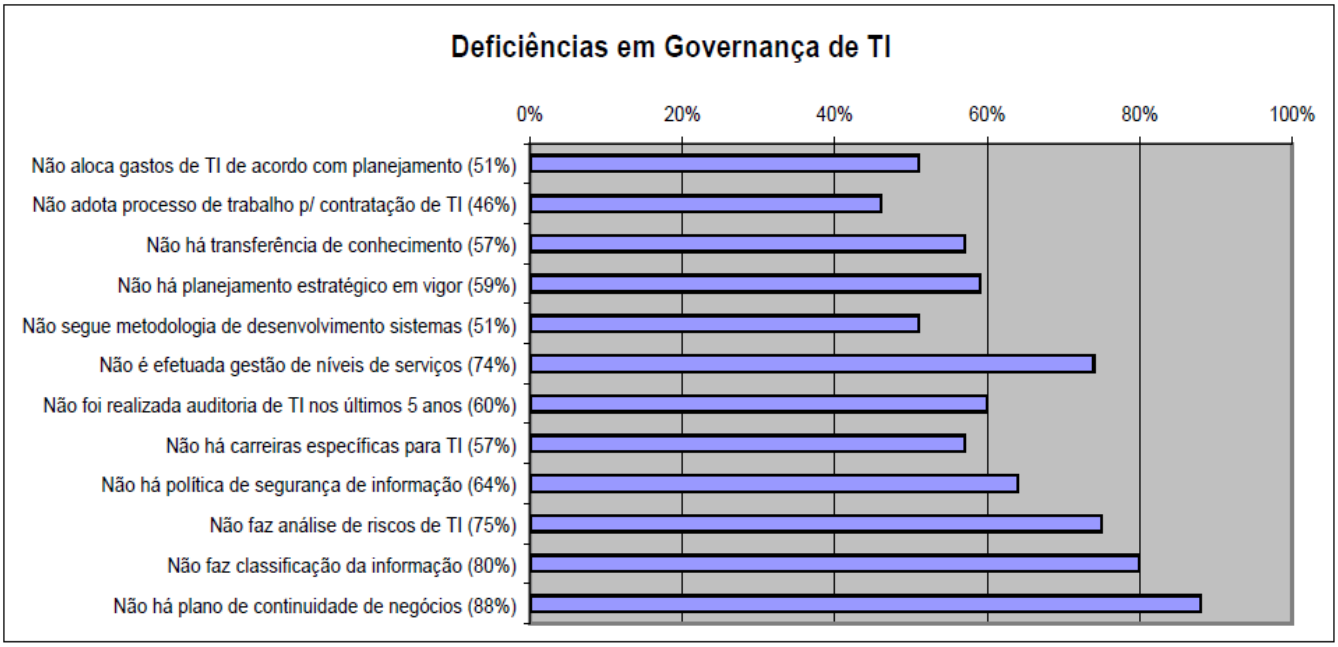


Figura 2.3 – Deficiências em Governança de TI (TCU, 2008d).

[3] De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC), Governança Corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas/cotistas, conselho e administração, diretoria, auditoria independente e conselho fiscal. As boas práticas de Governança Corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade.

Assim, em um contexto em que toda tecnologia aparenta ser atraente e milagrosa, mas são recorrentes as deficiências em Governança de TI, os processos de aquisição e desenvolvimento de tecnologia devem ser bem planejados e alinhados aos objetivos institucionais do Órgão, de modo a impedir desperdícios de recursos públicos e agregar valor à Organização.

2.2 Importância da Auditoria de TI

Diante deste novo contexto, a TI também precisa ser objeto de ações de controle do Sistema de Controle Interno da Administração Pública Federal, de forma a garantir que os critérios da informação - efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade – (IT GOVERNANCE INSTITUTE, 2007) sejam atendidos, contribuindo para a eficácia, a eficiência e a economicidade dos serviços públicos e para a prevenção de irregularidades, de desvios e de perdas de recursos públicos, auxiliando, inclusive, no combate à corrupção.

Pode-se distinguir basicamente dois tipos de auditoria que envolvem a Tecnologia da Informação:

i. Auditoria com TI: nesse tipo de auditoria, a tecnologia funciona como ferramenta de auxílio à realização dos trabalhos. As técnicas de auditoria que empregam ferramentas informatizadas para analisar bases de dados ou agregar eficiência aos trabalhos do auditor são conhecidas como Técnicas de Auditoria Assistidas por Computador (TAAC) ou, em inglês, Computer Assisted Audit Techniques (CAAT).

ii. Auditoria de TI: nesse tipo de auditoria, a tecnologia é objeto dos trabalhos, ou seja, verifica-se a conformidade e a operacionalidade dos controles dos processos baseados em Tecnologia da Informação.

O foco desse trabalho é a Auditoria de TI, que é uma área abrangente e que envolve diversos objetos da área da Tecnologia da Informação, tais como:

a) Gestão de TI – O objeto da ação de controle não é a tecnologia em si, mas a própria Gestão dessa tecnologia, envolvendo análise das atividades de planejamento, execução e controle dos processos de TI da Unidade examinada.
b) Dados – O objeto das ações de controle são bases de dados a serem analisadas, com o auxílio de *softwares* (exemplos: ACL, Excel ou Access), utilizando-se critérios estabelecidos em função dos dados analisados. A partir desse processo, são obtidas

informações sobre integridade e duplicidades dos dados, evidenciando-se fragilidades de controles das bases.[4]

c) *Softwares* – O objeto das ações de controle são *softwares* desenvolvidos ou adquiridos pelas Unidades.

d) Infra-Estrutura – O objeto das ações de controle é a infra-estrutura tecnológica, que envolve redes de computadores, servidores e demais *hardwares*.

e) Segurança da Informação – O objeto das ações de controle é a de segurança dos processos, redes, sistemas e informações da Unidade examinada, envolvendo os aspectos lógicos e físicos de segurança da informação.

f) Processos Licitatórios e Contratos de TI – O objeto das ações de controle são os processos licitatórios, dispensas e/ou inexigibilidades realizados pelas Unidades examinadas para aquisição de bens ou serviços de TI e os contratos deles resultantes.

Apesar de haver diversas classificações para as Auditorias de TI (tais como Auditoria de Dados, Auditoria de Sistemas, entre outras), elas não serão apresentadas nesse trabalho, pois, variam de autor para autor e, na realidade, são auditorias que se misturam e se sobrepõem. Por exemplo, a Auditoria de Sistemas visa analisar *softwares*. Todavia, além da avaliação de suas funcionalidades, também se costuma verificar as questões legais de seu processo de aquisição e seus requisitos de segurança. Com isso, em uma única ação de controle, há procedimentos de Auditoria de Sistemas, de Segurança e de Aquisição.

Por toda essa abrangência de objetos, a Auditoria de TI é ferramenta fundamental para que a Administração Pública controle seus atos relacionados à TI, nos mesmo moldes que fiscaliza suas outras atividades, resultado do seu poder-dever de controlar suas próprias ações do ponto de vista legal e de mérito.

Com isso, a Tecnologia da Informação pode deixar de gerar prejuízos comuns pela ineficiência de sua aquisição e gestão. Além disso, podem ser evitados muitos desvios e fraudes decorrentes de controles ainda incipientes nessa área de conhecimento.

[4] Todavia, podem ser extraídas informações para a realização de auditorias em diversas áreas, como por exemplo, bases de dados com informações de diárias e passagens concedidas a servidores. Nesse último caso, não se falaria em Auditoria de TI, mas de Auditoria com TI.

2.3 Situação atual da Auditoria de TI dentro da Administração Pública

A Auditoria de TI já está presente no controle interno de diversas instituições públicas, sendo mais atuante, estruturada e madura nas instituições públicas financeiras, como o Banco Central e o Banco do Brasil.

Entretanto, na maioria dos Órgãos de execução de programas e políticas públicas e, até mesmo, nos Órgãos de Controle, como a Controladoria-Geral da União, esse tipo de auditoria apresenta-se em um nível de maturidade iniciante e, em muitos casos, são realizadas – quando realizadas – de maneira *ad hoc*, ou seja, não há padrões, metodologias ou normas gerais a serem seguidas para planejamento e execução das ações de controle.

A ausência de uma metodologia de Auditoria de TI padronizada acarreta ações de controle desordenadas realizadas por diferentes departamentos de um mesmo Órgão, com critérios de avaliação diferentes e, muitas vezes, para um mesmo tipo de constatação, recomendações incoerentes e conflitantes.

Outra deficiência da ausência de padronização é a dificuldade de comunicação e entendimento entre auditor e auditado. O uso de uma linguagem comum facilita a compreensão do auditado sobre os parâmetros utilizados nas ações de controle e constatações e recomendações geradas. Assim, torna-se mais fácil a realização de ações corretivas por parte do gestor de forma preventiva às ações de controle ou em resposta a recomendações geradas.

A abrangência desse tipo de auditoria (vide Seção 2.2) é outro fator que dificulta os trabalhos de ações de controle em TI. A diversidade de áreas de abordagem exige que as equipes de auditoria possuam membros com amplos conhecimentos nas áreas que integram o escopo da auditoria a ser realizada, sendo essencial que haja constante treinamento dos auditores que atuem nessa área.

De acordo com o TCU (TCU, 2008b), no sumário executivo sobre o levantamento da Governança de TI na APF, as Auditorias de TI ainda são pouco freqüentes entre os pesquisados, sendo que apenas 40% dos 255 Órgãos/Entidades participantes da pesquisa declararam ter realizado alguma Auditoria de TI nos últimos cinco anos. Mesmo entre os 101 Órgãos/Entidades que a realizaram, 68% executaram, no máximo, uma Auditoria de TI por ano. Além disso, apenas 19% dos pesquisados declararam possuir equipe interna de Auditoria de TI.

Conforme conclusão desse sumário, tal resultado indica que a realização de Auditorias de TI em bases periódicas não é uma realidade entre os pesquisados. Com isso, esses Órgãos/Entidades estão perdendo a oportunidade de usar essas auditorias para aperfeiçoar os seus controles internos

de TI e, conseqüentemente, promover a melhoria da sua Governança de TI. Inclusive, no Acórdão 1.603/2008 – Plenário (ANEXO A), o TCU recomenda à Controladoria-Geral da União que realize regularmente auditorias de TI e/ou promova ações para estimular a realização dessas auditorias nos Órgãos/Entidades da APF.

Outra questão importante a ser levantada em relação à Auditoria de TI dentro da APF é o atual contexto legal e infra-legal em relação à Tecnologia da Informação. Por melhores que sejam as referências e metodologias implementadas, as Entidades que realizam ações de controle de TI sobre outros Órgãos enfrentam um problema que vai além de suas próprias infra-estruturas e capacidades fiscalizatórias. Uma das grandes dificuldades é a sustentação nas recomendações das auditorias de que as melhores práticas da Governança de TI devem ser seguidas, já que não existem instruções normativas ou legislação dentro da APF que obrigue a utilização dessas práticas, apesar de elas influenciarem diretamente na eficiência, na eficácia e economicidade da Tecnologia da Informação. Dentre as lacunas da legislação brasileira, de acordo com aula apresentada na disciplina de Auditoria de Tecnologia da Informação do curso de Auditoria Interna e Controle Governamental, podem ser citadas as seguintes omissões em relação aos seguintes eventos:

a) Acesso não autorizado aos sistemas.
b) Interceptação não autorizada de informações.
c) Uso não autorizado de sistemas de informática.
d) Alteração de dado ou programa de computador.
e) Difusão de vírus eletrônico.
f) Quebra de privacidade de banco de dados.

Dessa forma, por mais bem estruturado que seja o processo de auditoria, ele ainda fica amarrada à falta de instruções legais ou normativas que possam dar suporte às suas recomendações, prevalecendo, muitas vezes, apenas o bom senso de ambas as partes: auditor e auditado.

Tal lacuna legislativa também é motivação para esse trabalho, pois quanto mais se trabalhar nessa área e mostrar suas fragilidades, maiores serão os estímulos para que se legisle e regule a área de Tecnologia da Informação dentro do Governo Federal.

Todavia, apesar de todos os problemas apresentados, a Auditoria de TI na APF também apresenta evoluções. A fim de solucionar algumas das lacunas legislativas, encontra-se em tramitação no Congresso Nacional o Projeto de Lei PL-84/1999 (incorporou os projetos de lei PLC-89/2003, PLS-76/2000, PLS-137/2000 e outros) que dispõe sobre crimes cometidos na área de

informática e tipifica condutas realizadas mediante uso de rede de computadores ou *Internet*, ou que sejam praticadas contra sistemas informatizados e similares.

Em tramitação desde 2009, o Projeto foi aprovado na Câmara dos Deputados em 2005 e teve substitutivo aprovado no Senado Federal em 2009. Atualmente, encontra-se na Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados.

A transformação desse Projeto em Lei possibilitará que se responsabilizem agentes públicos que cometerem crimes na área de informática que, hoje em dia, ainda não são tipificados. Assim, será possível que haja punições, na esfera judicial, de agentes públicos responsáveis por crimes na área de tecnologia da informação, eventualmente verificados a partir de Auditorias de TI.

A publicação da Instrução Normativa nº 04/2008 (BRASIL, 2008a), que dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional, também é um grande avanço no processo de aquisição e prestação de serviços de Tecnologia da Informação.

Além da constante evolução das auditorias bancárias na área de TI, o Tribunal de Contas da União também apresenta grandes avanços, como pode ser visto na seção 2.3.1.

2.3.1 Auditoria de TI no TCU

Com o reconhecimento da importância estratégica da área de Tecnologia da Informação, da expressiva materialidade tanto das aquisições relacionadas à Tecnologia da Informação quanto dos recursos geridos por meio de sistemas informatizados no Governo Federal, e do uso cada vez mais crescente da TI para manipulação e armazenamento de dados da Administração Pública Federal, introduzindo novos riscos e aumentando a fragilidade de algumas atividades, o Tribunal de Contas da União criou, em agosto de 2006, a Secretaria de Fiscalização de Tecnologia da Informação – Sefti (TCU, 2009).

Por meio da Resolução-TCU nº 199, de 28 de dezembro de 2006 (BRASIL, 2006b) - que define a estrutura, as competências e a distribuição das funções de confiança das unidades da Secretaria do Tribunal de Contas da União, e da Portaria-SEFTI nº 001, de 02 de abril de 2007 (BRASIL, 2007b) - que dispõe sobre a organização interna e estabelece as competências das subunidades da Secretaria de Fiscalização de Tecnologia da Informação, a Sefti foi formalmente constituída e teve suas atribuições gerais definidas.

A Sefti possui a função de fiscalizar a gestão e o uso de recursos de TI na Administração Pública Federal, conduzindo trabalhos específicos em Fiscalização de Tecnologia da Informação e

servindo de suporte às demais Secretarias do Tribunal. Além disso, elabora e dissemina metodologias, manuais e procedimentos para planejamento e execução de fiscalizações de Tecnologia da Informação, visando maior qualidade dos trabalhos de fiscalização nessa área (TCU, 2009).

Inicialmente, a Sefti era dividida em duas Diretorias: a Diretoria de Fiscalização de Aquisições de Tecnologia da Informação (Difati), à qual cabia a apreciação das questões relacionadas às contratações de TI que enfatizam a conformidade legal com os preceitos da Legislação de Licitações; e a Diretoria de Auditoria de Tecnologia da Informação (Dati), à qual cabiam as questões relacionadas às auditorias de natureza operacional, como auditoria de dados e de sistemas ou mesmo de programas de governo nos quais a Tecnologia da Informação era fator predominante (ex.: e-GOV) (BORBA, 2008).

Em 25 de novembro de 2008, a Portaria-SEFTI Nº 3 (BRASIL, 2008c) revogou a Portaria-SEFTI nº 1, de 2 abril de 2007 e definiu nova organização interna e estabeleceu as competências das subunidades da Secretaria de Fiscalização de Tecnologia da Informação. Com a nova organização a Secretaria passou a ter três Diretorias (Figura 2.4), a saber:

a) Diretoria de Fiscalização de Governança de Tecnologia da Informação 1 – DIGOV1.
b) Diretoria de Fiscalização de Governança de Tecnologia da Informação 2 – DIGOV2.
c) Diretoria de Fiscalização de Governança de Tecnologia da Informação 3 – DIGOV3.

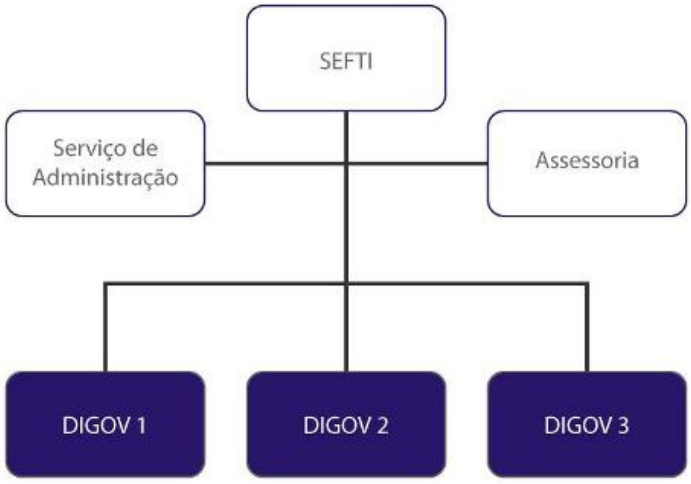


Figura 2.4 – Estrutura organizacional da Sefti (Fonte: Sítio eletrônico do TCU).

Diferentemente da organização anterior, as novas Diretorias atuam em todas as áreas de Auditoria de TI, não havendo mais divisão por assunto tratado.

Em 2008, o TCU produziu um Sumário executivo sobre um levantamento de auditoria realizada com o objetivo de coletar informações para criação de referencial estratégico para a Secretaria de Fiscalização de Tecnologia da Informação (Sefti), e identificar formas de atuação de Entidades fiscalizadoras de TI (TCU, 2008c).

Durante esse levantamento, foram realizados contatos formais mediante questionários e entrevistas em Unidades do TCU e 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. Além da consulta aos pares nacionais e estrangeiros, o mesmo levantamento permitiu que se interagisse com Entidades de auditoria de outros segmentos públicos de privados para a sondagem de boas práticas e do perfil que uma unidade de auditoria especializada em TI poderia assumir em termos de atuação e recursos humanos adequados a sua composição (BORBA, 2008).

Tal coleta de informação gerou 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; e 11. Proposta de conteúdo e de estrutura da página da Sefti no portal do TCU.

Os resultados das ações de controle de TI realizadas pela Sefti são registradas em relatórios que, após julgados, são transformados em Acórdãos do TCU, onde são emitidas várias recomendações e determinações baseadas nos padrões e modelos de Governança de TI e Segurança da Informação. Os principais Acórdãos relacionados à Auditoria de TI estão listados no ANEXO A.

Em 2009, foi realizada pela Sefti, dentro do TCU, uma pesquisa de satisfação dos consultantes sobre as consultas técnicas internas produzidas pela Secretaria. Dos 44 questionários enviados, 21 foram respondidos. A pesquisa teve como principais resultados:

a) 76% dos consultantes se declararam Muito Satisfeitos com a facilidade de acesso à consulta técnica da Sefti e 24% se declaram Satisfeitos.
b) 67% dos consultantes consideraram o tempo de resposta à informação solicitada Muito Satisfatório e 33% consideraram satisfatório.

c) 67% dos consultantes afirmaram que o grau de conhecimento demonstrado pelos consultores é Muito Satisfatório e 33% afirmaram ser satisfatório.

d) 95% dos consultantes declaram terem adotado a posição opinada pelos consultores e 5% não se lembravam.

e) 95% dos consultantes declaram que a consulta técnica correspondeu às suas expectativas e 5% não responderam.

f) 100% dos consultantes responderam que voltariam a procurar os mesmos consultores para uma nova consulta técnica.

Assim, foi verificada alta satisfação do público interno que participou da pesquisa com os trabalhos de consultoria da Secretaria.

3 SITUAÇÃO DA AUDITORIA DE TI NA CGU

Inicialmente, serão abordados o histórico da Auditoria de TI no âmbito da SFC e a estrutura organizacional da Secretaria dentro da CGU. Em seguida, serão apresentados a metodologia e os resultados do Diagnóstico de Auditoria de TI.

3.1 Histórico da Auditoria de TI na SFC

Em 2004 e 2006, foram realizados concursos para a seleção de novos servidores para a CGU, que previram vagas específicas para candidatos com conhecimento em TI para serem lotados na SFC. Além desses, há servidores e técnicos que entraram em vagas de conhecimento geral, mas com conhecimentos específicos de TI.

Com a entrada desses servidores, foram iniciadas algumas tentativas por parte das Diretorias de aumentar e aperfeiçoar as ações de controle nessa área de conhecimento.

No segundo semestre de 2006, a Diretoria de Auditoria da Área Social (DS) começou a incentivar os servidores com conhecimentos em Tecnologia da Informação a participarem de Congressos e cursos de Auditoria de TI. Além de possibilitar que servidores recém nomeados tivessem uma noção inicial acerca do assunto, esse incentivo teve como resultados os seguintes produtos:

- um minicurso de multiplicação dos conhecimentos adquiridos nos Congressos, que teve como público alvo outros colegas interessados no assunto; e
- um artigo (ANTUNES et al., 2007) sobre os critérios de Auditoria de TI mais utilizados e apresentação de trabalhos *ad-hoc* de ações de controle de TI realizados dentro da Diretoria. Ressalta-se que esse artigo foi publicado apenas um ano depois de sua elaboração, na 2ª edição da Revista da CGU.

No início de 2007, foi criado o Grupo de Soluções em TI da DR (GSTI-DR), constituído pela Ordem de Serviço nº 73/DR/SFC/CGU-PR, de 09/04/2007, com a finalidade de estudar, elaborar, propor e implementar soluções na área de Tecnologia da Informação, de forma a agregar facilidades às práticas e procedimentos gerais vinculados às ações de controle executadas e demandadas pelas Coordenações-Gerais da DR. Os detalhes dos trabalhos realizados constam dos autos do Processo n° 00190.008093/2007-13 da CGU.

O GSTI-DR submeteu 4 projetos ao Colegiado de Coordenadores desta Diretoria, dos quais dois foram aprovados, conforme disposto no item 3 da Ordem de Serviço nº 73/2007:

1) Projeto de Desenvolvimento de Procedimentos de Auditoria em TI.
2) Projeto de Padronização de Banco de Dados.

O primeiro projeto teve como resultado a criação de procedimentos de Auditoria de TI, inseridos no Sistema ATIVA[5], conforme Tabela 3.1:

ÁREA DE EXAME	CÓDIGO DO PROCEDIMENTO	TÍTULO DO PROCEDIMENTO
018000	0001	Planos de Auditoria de Tecnologia da Informação
060209	0001	Aquisições de bens e serviços de TI - Parte Geral
060209	0002	Pagamentos contratuais relacionados à TI
060209	0003	Aquisições de bens e serviços de TI - parte específica
070307	0025	Planejamento Estratégico de TI
070307	0026	Política de Segurança da Informação
070307	0027	Posição da área de Informática no organograma do Órgão/Entidade
070307	0028	Terceirização em Tecnologia da Informação
070307	0029	Gerenciamento de Projetos de TI
070307	0030	Relacionamento do Setor de Informática com os demais Setores
070307	0031	Definição de arquitetura da informação
070307	0032	Processo de desenvolvimento de sistemas
070307	0033	Capacitação dos recursos humanos de TI

Tabela 3.1 – Procedimentos de Auditoria de TI no Sistema ATIVA.

Desde a inserção dos procedimentos no Sistema, já foram geradas 179 Ordens de Serviço[6] (OS) utilizando-se desses procedimentos, conforme Tabela 3.2:

PROCEDIMENTO		
ÁREA DE EXAME	CÓDIGO DO PROCEDIMENTO	QTD. DE OS
018000	0001	112
060209	0001	16
060209	0002	16
060209	0003	10
070307	0025	3
070307	0026	3
070307	0027	2
070307	0028	3
070307	0029	4
070307	0030	3
070307	0031	2
070307	0032	3
070307	0033	2
TOTAL		**179**

Tabela 3.2 – Quantidade de Ordens de Serviço que utilizam procedimentos de TI.

[5] Sistema de informação das ações de controle da SFC.
[6] Ordem de serviço é o instrumento formal pelo qual são demandadas tarefas no âmbito da CGU.

O segundo projeto teve início com as discussões do GSTI-DR, mas seu produto final só foi gerado no segundo semestre de 2009, a partir de uma parceria entre a Diretoria de Sistemas e Informação (DSI) e a Diretoria de Planejamento e Coordenação das Ações de Controle (DC). Como desdobramento dessa parceria houve a criação da solução Banco de Dados Interativo (BDI/CGU) cujo objetivo é disponibilizar um ambiente de Sistema Gerenciador de Banco de Dados (SGBD) para manipulação e tratamento de dados às diversas Unidades da Controladoria-Geral da União. Assim, essas Unidades, com o auxílio de ferramentas de auditoria, ganharam a possibilidade de realizar o cruzamento de dados entre sistemas governamentais auditados pela CGU. Com isso, espera-se o aumento da abrangência, tempestividade e qualidade dos trabalhos de auditoria realizados. A Ordem de Serviço DSI nº 98, de 09/11/2009, institui a Política de uso da Solução BDI-CGU.

De acordo com informações de servidores, após trocas sucessivas do Diretor da área, de mudanças de lotação de servidores de TI e de priorização de outras atividades dentro das Coordenações, os trabalhos do GSTI-DR foram paralisados.

Ainda em 2007, a servidora Maíra Hanashiro elaborou uma dissertação de mestrado voltada para a Auditoria de TI, cujo título é Metodologia para Desenvolvimento de Procedimentos para Auditoria de TI Aplicada à Administração Pública (HANASHIRO, 2007), que também deu origem a um artigo (HANASHIRO; PUTTINI, 2007). Este trabalho objetivava propor uma metodologia, baseada nas diretrizes do COBIT (IT GOVERNANCE INSTITUTE, 2007) e demais modelos de melhores práticas de TI, aplicável à Administração Pública Federal, que possibilitasse planejar uma Auditoria de TI e desenvolver procedimentos a serem aplicados durante sua execução, de forma a padronizar os processos de auditoria dentro do Órgão auditor e criar uma linguagem comum entre auditor e auditado. Como resultados, foram apresentados um estudo dos modelos, padrões e normas de TI mais conhecidos nacional e internacionalmente; um modelo de fases para realização de auditorias de TI; e, por fim, uma metodologia para desenvolvimento de procedimentos para estas auditorias.

Em 2008, o servidor Rogério Xavier Rocha elaborou monografia intitulada Proposta de Procedimento Simplificado de Auditoria de Gestão em Segurança da Informação em Órgão do Poder Executivo Federal (ROCHA, 2008). Esta pesquisa teve por objetivo principal propor um Procedimento de Auditoria de Gestão em Segurança da Informação em Órgãos da Administração Pública Federal, baseado em controles de normas consagradas em Segurança da Informação, tais como a NBR ISO/IEC 17799:2005, atual NBR ISO/IEC 27002 (ABNT, 2005). A partir de

levantamentos sobre os principais riscos e vulnerabilidades encontradas que impactam uma gestão efetiva da Segurança da Informação em Órgãos da Administração Pública Federal, buscava, por meio do procedimento proposto, incentivar uma implementação gradativa e sedimentada de diversos controles por meio das ações de controle do Sistema de Controle Interno do Poder Executivo Federal, que tem por missão constitucional auxiliar a gestão pública na consecução de seus objetivos.

No mesmo ano, o servidor Carlos Alberto dos Santos Silva elaborou dissertação de mestrado intitulada Diretrizes para Auditoria do Processo de Contratação de Tecnologia da Informação na Administração Pública Federal (SILVA, 2008). Em seu trabalho, verificou que os Órgãos de controle interno do setor público, no que se refere à TI e em especial à contratação de serviços de TI¸ não vinham atuando de maneira sistemática.

Segundo o autor, um dos fatores que contribui para esta situação é a ausência de um modelo de auditoria que contemple a verificação tanto das questões relacionadas à eficiência dos processos gerenciais da contratação de serviços de TI quanto às questões relacionadas aos aspectos legais desses processos. Diante disso, sua pesquisa objetivava construir um conjunto de diretrizes para a auditoria no processo de contratação de serviços de TI, aplicável ao setor público. Para o alcance do objetivo proposto na pesquisa, inicialmente foi identificada, com base nos relatórios de auditoria da Controladoria-Geral da União, a abrangência das auditorias na contratação de serviços de TI.

Após a identificação dos processos gerenciais relacionados à contratação de serviços de TI, foram elaboradas as diretrizes de auditoria. A base técnica para a construção das diretrizes foram as orientações contidas em um Quadro Referencial Normativo (QRN), no COBIT 4.1 (IT GOVERNANCE INSTITUTE, 2007) e nas normas gerais e normas de auditoria aplicáveis ao poder Executivo Federal. A versão preliminar das diretrizes foi submetida a um grupo de auditores que apresentaram suas percepções sobre as citadas diretrizes. Essas percepções foram analisadas e culminaram na versão final das diretrizes que descrevem os pontos de controle sobre os quais se devem atuar, resultando no rol de verificações necessárias à formulação e fundamentação da opinião por parte dos auditores sobre o processo de contratação de serviços de TI no âmbito da Administração Pública.

Como produtos desse processo de pesquisa, foram identificados 101 diretrizes com seus respectivos referenciais técnicos, operacionais e legais que amparam as verificações de conformidade estabelecidas nas diretrizes.

Apesar de não tratar diretamente de Auditoria de TI, outro projeto de pesquisa importante, em curso, é a do servidor José Geraldo Loureiro Rodrigues, Diretor da Diretoria de Sistemas e Informação (DSI) da CGU. Aluno do Mestrado em Gestão do Conhecimento e Tecnologia da Informação da Universidade Católica de Brasília, o servidor criou o Wiki-GOV (RODRIGUES, 2009a) com a finalidade de compartilhar conhecimentos resultantes de suas pesquisas sobre Governança de TI no Setor Público.

3.2 Estrutura da SFC

De acordo com as informações sobre a história de criação do Órgão, contidas no sítio da CGU (CGU, 2009), a Controladoria-Geral da União (CGU) foi criada no dia 2 de abril de 2001, pela Medida Provisória n° 2.143-31, sendo inicialmente denominada Corregedoria-Geral da União (CGU/PR).

Quase um ano depois, o Decreto n° 4.177, de 28 de março de 2002 (BRASIL, 2002a), integrou a Secretaria Federal de Controle Interno (SFC) e a Comissão de Coordenação de Controle Interno (CCCI) à estrutura da então Corregedoria-Geral da União. O mesmo Decreto transferiu para a Corregedoria-Geral da União as competências de Ouvidoria-geral, até então vinculadas ao Ministério da Justiça.

A Medida Provisória n° 103, de 1° de janeiro de 2003, convertida na Lei n° 10.683, de 28 de maio de 2003, alterou a denominação do Órgão para Controladoria-Geral da União, assim como atribuiu ao seu titular a denominação de Ministro de Estado do Controle e da Transparência.

As competências da CGU foram definidas pela Lei n° 10.683, de 28 de maio de 2003 e pela Portaria n° 570, de 11 de maio de 2007, que aprova o Regimento Interno da Controladoria-Geral da União (BRASIL, 2007a).

O Decreto n° 5.683, de 24 de janeiro de 2006 (BRASIL, 2006a), alterou a estrutura da CGU, criando a Secretaria de Prevenção da Corrupção e Informações Estratégicas (SPCI), responsável por desenvolver mecanismos de prevenção à corrupção. Assim, a CGU passou a ter a competência não só de detectar casos de corrupção, mas de antecipar-se a eles, desenvolvendo meios para prevenir a sua ocorrência.

O Decreto n° 6.656, de 20 de novembro de 2008, dá nova redação a alguns artigos do Decreto n° 5.683, de 24 de janeiro de 2006, alterando Diretorias e criando a Assessoria Especial de Gestão de Projetos. Por fim, a Portaria n° 1.215, de 25 de junho de 2009, institui o Observatório da Despesa Pública – ODP da Controladoria-Geral da União.

Com a criação da SPCI, as principais funções exercidas pela CGU – controle, correição, prevenção da corrupção e ouvidoria – foram agrupadas, consolidando-as em uma única estrutura funcional, que pode ser observada na Figura 3.1 do organograma[7] do Órgão:

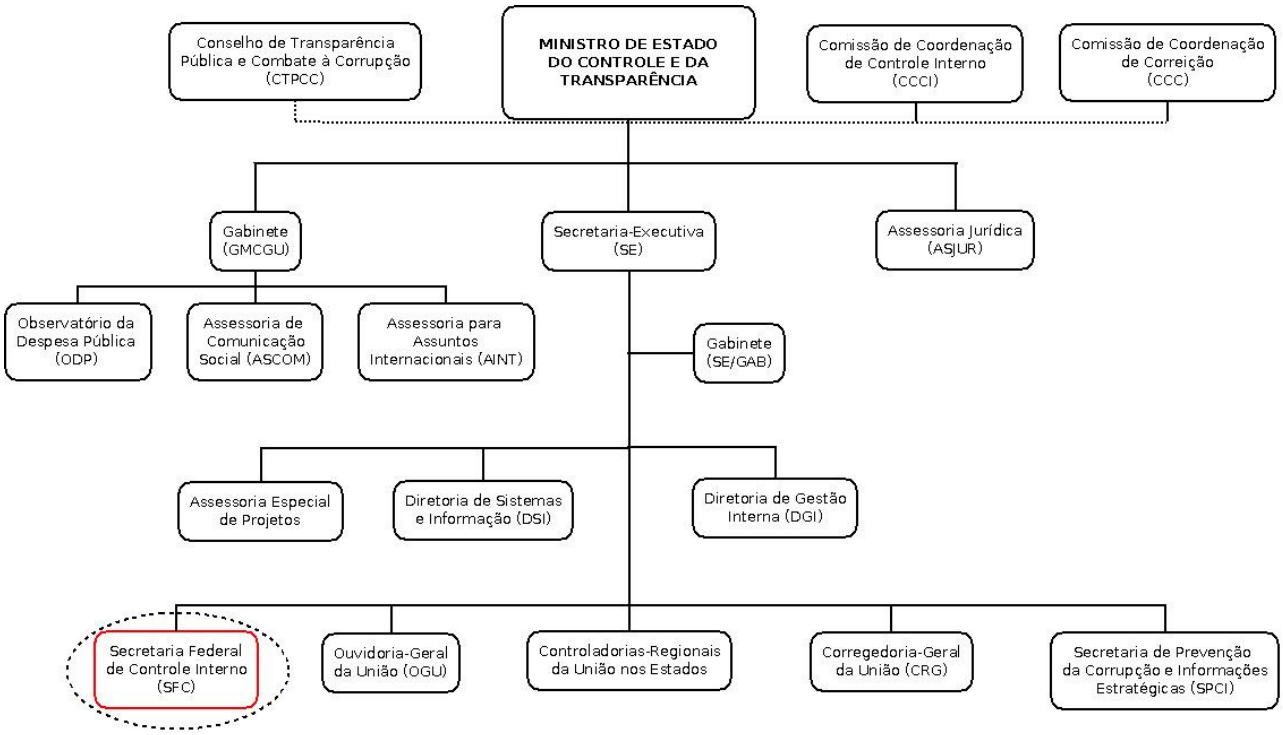


Figura 3.1 - Organograma da Controladoria-Geral da União.

A **Secretaria Federal de Controle Interno** (destacada na Figura 3.1) é responsável por avaliar a execução dos orçamentos da União, fiscalizar a implementação dos programas de governo e fazer auditorias sobre a gestão dos recursos públicos federais sob a responsabilidade de Órgãos e Entidades públicos e privados, entre outras funções. As competências da SFC podem ser observadas no Decreto n° 5.683, de 24 de janeiro de 2006. De acordo com essa Norma:

> Art. 11. Às Diretorias de Auditoria das Áreas Econômica, Social, de Infra-Estrutura, de Produção e Tecnologia e de Pessoal, Previdência e Trabalho compete realizar as atividades de auditoria e fiscalização da execução dos programas e ações governamentais dos Órgãos e Entidades da administração pública federal, nas suas respectivas áreas, à exceção dos Órgãos e unidades da Presidência da República, da Advocacia-Geral da União, do Ministério das Relações Exteriores e do Ministério da Defesa (BRASIL, 2006a).

O organograma[8] da SFC e suas Diretorias pode ser observado na Figura 3.2:

[7] Organograma adaptado do sítio eletrônico da CGU com inserção do ODP.
[8] Organograma adaptado da *intranet* da CGU.

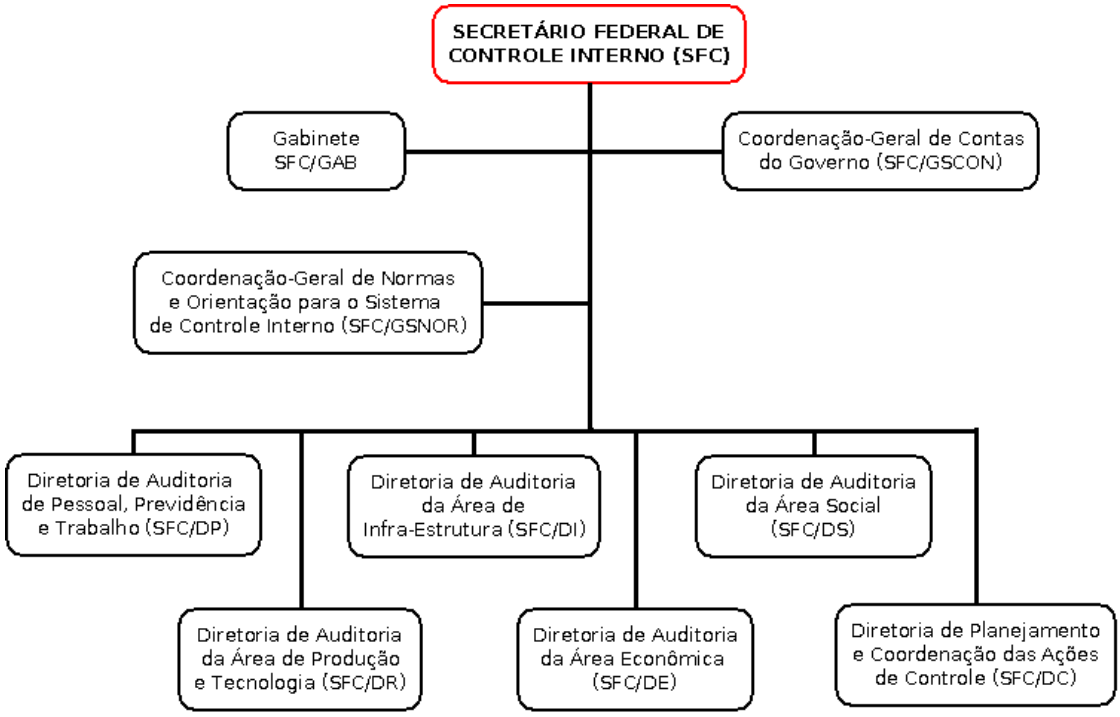


Figura 3.2 - Organograma da Secretaria Federal de Controle Interno.

A seguir são apresentados os organogramas das seis Diretorias da SFC e de suas respectivas Coordenações-Gerais[9]:

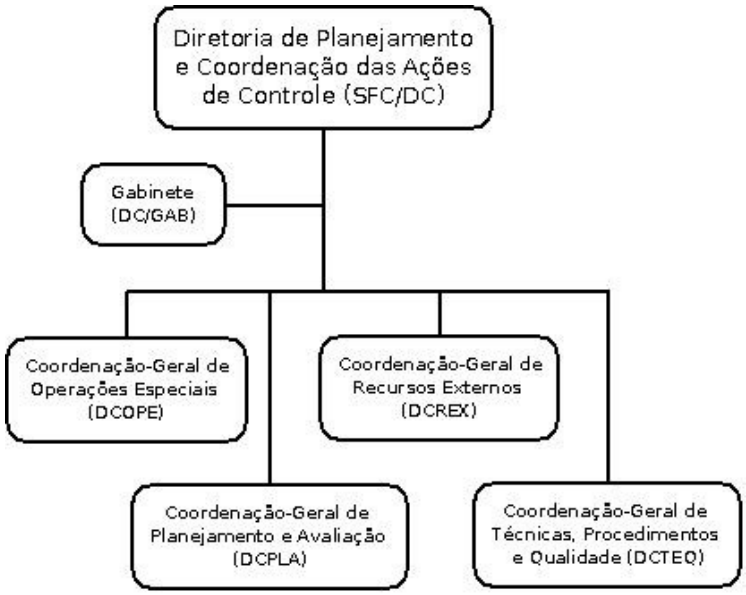


Figura 3.3 - Organograma da Diretoria de Planejamento e Coordenação das Ações de Controle (DC).

[9] Organogramas traçados a partir do estabelecido nos Decretos n° 5.683, de 24 de janeiro de 2006 e n° 6.656, de 2º de novembro de 2008.

A Diretoria de Planejamento e Coordenação das Ações de Controle (DC), apresentada na Figura 3.3, é a Diretoria que tem como funções principais orientar, aprovar, coordenar, monitorar e supervisionar a execução das atividades a cargo das Coordenações-Gerais finalísticas, realizando ações de controle apenas excepcionalmente.

As demais Diretorias são formadas por Coordenações de execução de ações de controles em suas respectivas áreas de atuação, como mostram a Figura 3.4, a Figura 3.5, a Figura 3.6, a Figura 3.7 e a Figura 3.8 a seguir apresentadas:

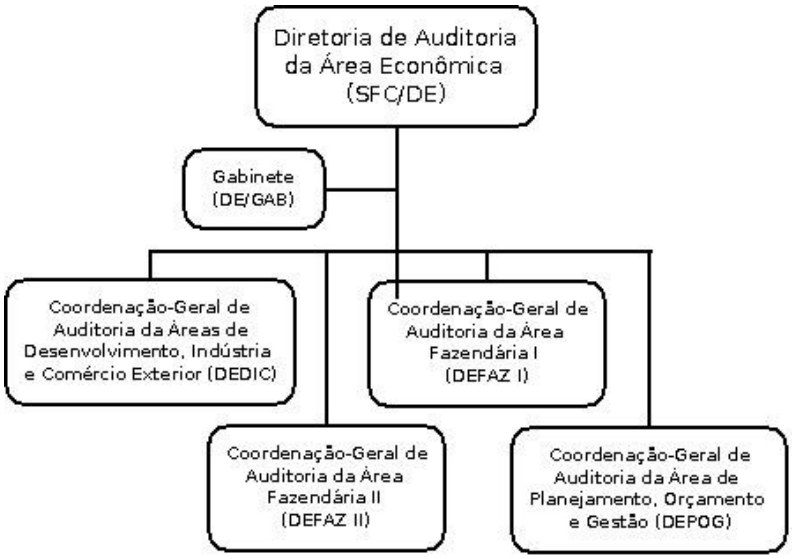


Figura 3.4 - Organograma da Diretoria da Área Econômica (DE).

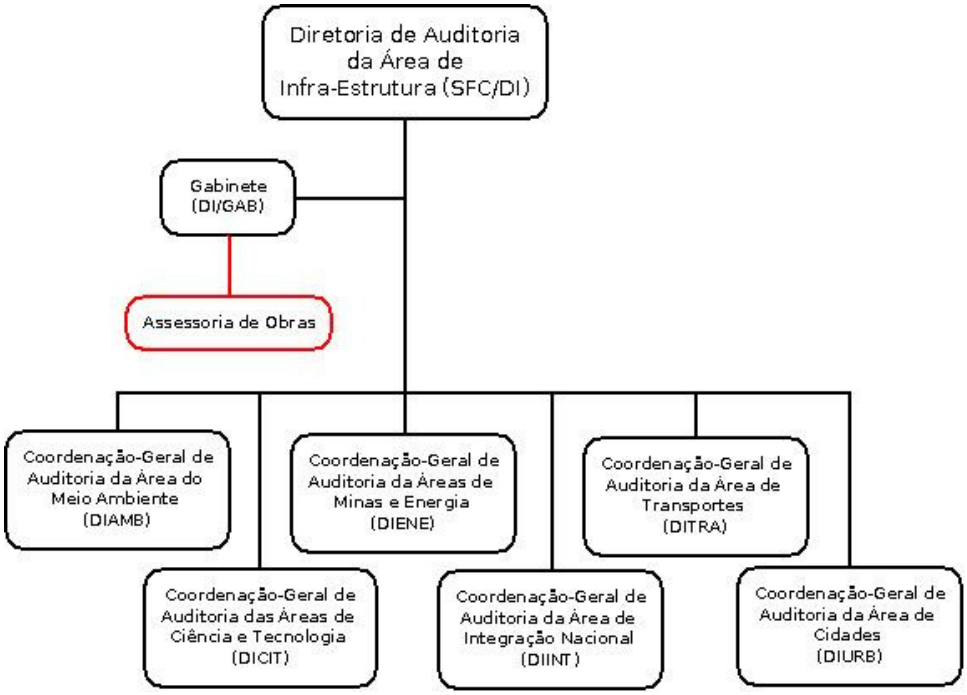


Figura 3.5 - Organograma da Diretoria da Área de Infra-Estrutura (DI).

A Assessoria de Obras da DI, apesar de constar do organograma apresentado neste trabalho, não é uma Unidade criada formalmente dentro da Diretoria e será abordada na seção 4.3.

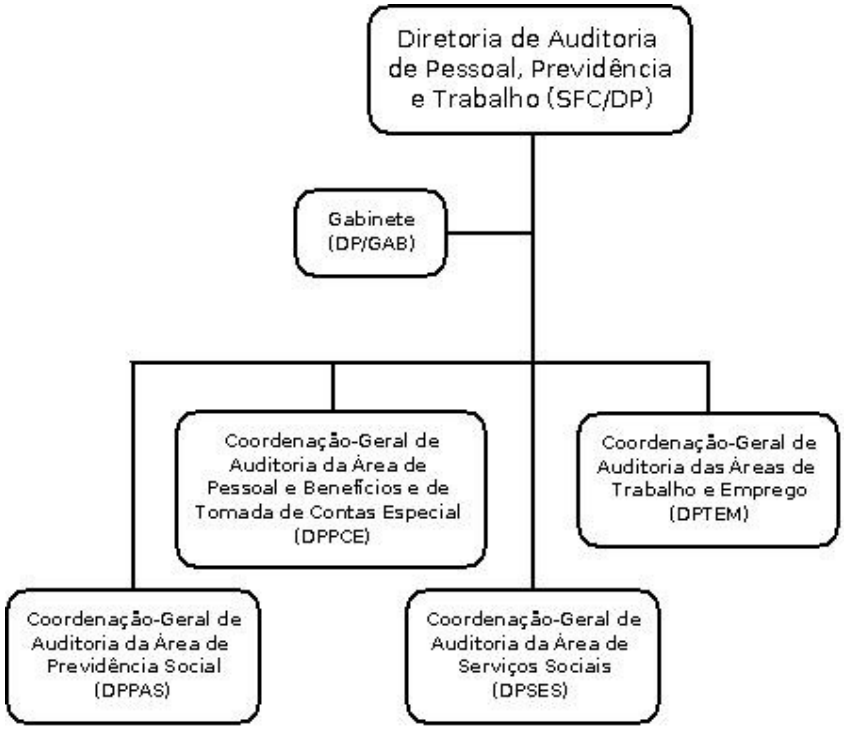


Figura 3.6 - Organograma da Diretoria de Pessoal, Previdência e Trabalho (DP).

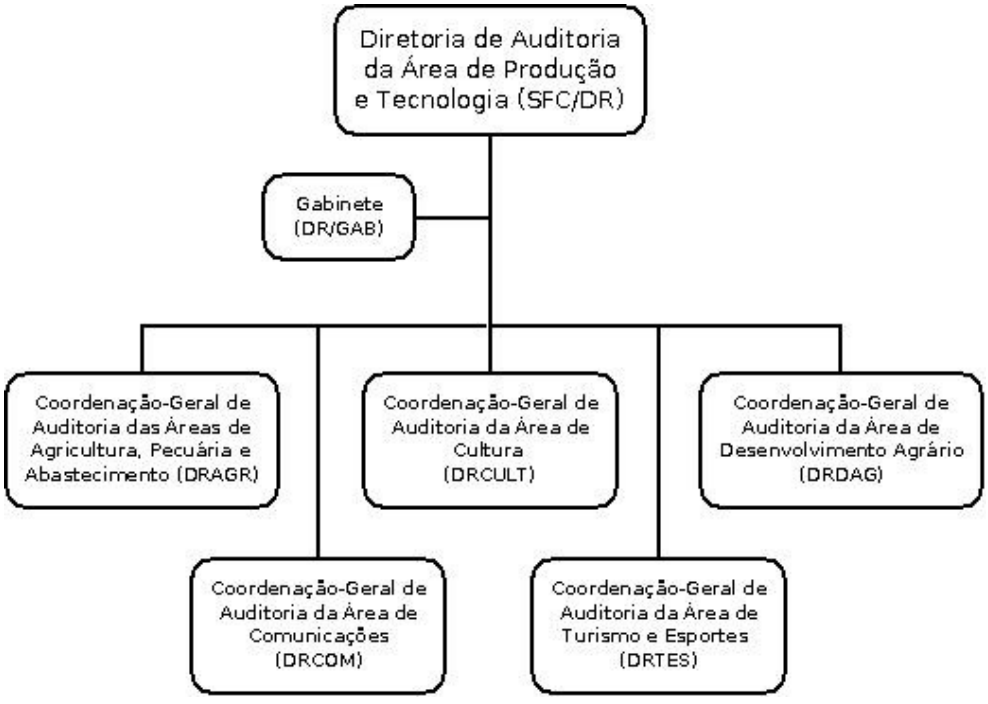


Figura 3.7 – Organograma da Diretoria de Auditoria da Área de Produção e Tecnologia (DR).

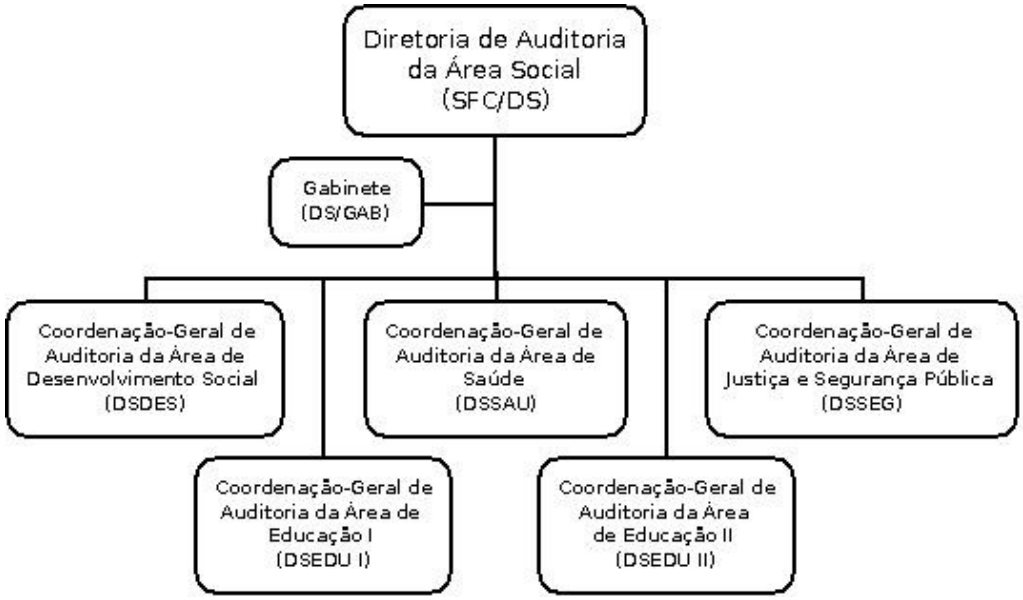


Figura 3.8 – Organograma de Auditoria da Área Social (DS).

O organograma completo da SFC, pode ser visualizado no APÊNDICE C.

3.3 Diagnóstico de Auditoria de TI

O Diagnóstico da Auditoria de TI é uma coletânea de percepções e opiniões dos Coordenadores das Unidades finalísticas da SFC e dos servidores com conhecimento em TI, doravante chamados de **servidores de TI**.

A opinião dos Coordenadores é importante porque, em geral, eles possuem a visão integral dos trabalhos de suas Unidades e possuem capacidade decisória para priorização de ações de controle. Já os servidores de TI costumam ter opiniões mais técnicas por terem conhecimento mais especializado da área.

A pesquisa demonstrará que muitas opiniões são convergentes e permitem que se trace um perfil da Auditoria de TI dentro da SFC. Algumas distorções serão observadas pela inexistência de servidores de TI em todas as Coordenações e pelas divergências de percepções inerentes aos diferentes pontos de vista dos Coordenadores e servidores no âmbito de suas atribuições.

3.3.1.1 Metodologia

Durante duas semanas, de 24/09/2009 a 09/10/2009, foram disponibilizados dois questionários para o levantamento de dados para o diagnóstico da Auditoria de TI dentro da SFC.

Os questionários foram criados com o auxílio da ferramenta *Google Docs* (Google, 2009), que permite a criação de questionários (*Forms*) para serem respondidos *online*. Os modelos dos questionários podem ser visualizados nos APÊNDICES A e B.

Para responder ao questionário, bastava-se acessar o endereço eletrônico enviado dentro da mensagem eletrônica. Ao término do preenchimento, as respostas eram automaticamente enviadas para uma planilha de consolidação de dados do *Google Docs*.

Cabe observar que o levantamento da lotação dos Coordenadores e servidores dentro da SFC tem como data de referência o dia 21/09/2009 e permaneceu inalterada durante a aplicação da pesquisa. A seguir detalha-se a estratégia adotada para aplicação dos questionários:

3.3.1.2 Coordenadores das áreas finalísticas da SFC

Para compor o universo desta pesquisa, foram selecionados todos os Coordenadores de Unidades finalísticas da SFC, resultando em 24 entrevistados, conforme lista a seguir:

COORDENAÇÃO	CARGO
DEFAZ I	Coordenador-Geral de Auditoria da Área Fazendária I
DEFAZ II	Coordenador-Geral de Auditoria da Área Fazendária II
DEPOG	Coordenador-Geral de Auditoria dos Programas das Áreas de Planejamento, Orçamento e Gestão
DEDIC	Coordenador-Geral de Auditoria das Áreas de Desenvolvimento, Indústria e Comércio Exterior
DSSEG	Coordenadora-Geral de Auditoria das Áreas de Justiça e Segurança Pública
DSDES	Coordenador-Geral de Auditoria da Área de Desenvolvimento Social
DSSAU	Coordenadora-Geral de Auditoria da Área de Saúde
DSEDU I	Coordenador-Geral de Auditoria da Área de Educação I
DSEDU II	Coordenador-Geral de Auditoria da Área de Educação II
DIAMB	Coordenadora-Geral de Auditoria da Área do Meio Ambiente
DIENE	Coordenador-Geral de Auditoria da Área de Minas e Energia
DICIT	Coordenadora-Geral de Auditoria das Áreas de Ciência e Tecnologia
DITRA	Coordenador-Geral de Auditoria da Área de Transportes
DIURB	Coordenador-Geral de Auditoria da Área de Cidades
DIINT	Coordenador-Geral de Auditoria da Área de Integração Nacional
DRAGR	Coordenador-Geral de Auditoria das Áreas de Agricultura, Pecuária e Abastecimento
DRDAG	Coordenador-Geral de Auditoria da Área de Desenvolvimento Agrário
DRTES	Coordenador-Geral de Auditoria da Área de Turismo e Esportes
DRCULT	Coordenador-Geral de Auditoria da Área de Cultura
DRCOM	Coordenador-Geral de Auditoria da Área de Comunicações
DPPCE	Coordenador-Geral de Auditoria das Áreas de Pessoal e Benefícios e de Tomada de Contas Especial
DPSES	Coordenador-Geral de Auditoria da Área de Serviços Sociais
DPTEM	Coordenador-Geral de Auditoria das Áreas de Trabalho e Emprego
DPPAS	Coordenador-Geral de Auditoria da Área de Previdência Social
Total	**24 Coordenações**

Tabela 3.3 – Lista de Coordenadores da área finalística da SFC.

No caso dos Coordenadores, foram marcadas entrevistas para auxiliá-los a preencher o questionário via *Google Docs*. Tal estratégia foi adotada para facilitar a compreensão das perguntas,

uma vez que a maioria dos Coordenadores não é da área de TI. Além disso, dessa forma, foi possível atrair a atenção integral do entrevistado e extrair informações mais detalhadas.

A solicitação de entrevista foi encaminhada via *e-mail*, com o endereço eletrônico do questionário para que o entrevistado tivesse possibilidade de ter conhecimento prévio das perguntas. Os Coordenadores que se disponibilizaram a participar responderam agendando as entrevistas.

3.3.1.3 Servidores de TI

Inicialmente, como não foi possível se obter uma lista oficial, foi realizado o levantamento informal, por meio de consulta com assessores dos gabinetes das Diretorias das SFC, da lista dos servidores da SFC com formação acadêmica em TI e/ou que atuam em Auditorias de TI.

O universo da pesquisa, que ocorreu por meio de censo, considerou apenas servidores que trabalhassem em Coordenações de atuação predominantemente finalística, não incluindo aqueles da Diretoria de Planejamento e Coordenação das Ações de Controle – DC, por se tratar de uma Diretoria que, via de regra, não realiza ações de controle regulares. Assim, a lista final possui a seguinte distribuição dentro da SFC:

DIRETORIA	COORDENAÇÃO	QTD DE SERVIDORES
DE	DEDIC	1
	DEFAZ I	4
	DEFAZ II	1
	DEPOG	3
DE Total		**9**
DI	DI/GAB	3
	DICIT	2
	DIENE	2
	DITRA	1
DI Total		**8**
DP	DP/GAB	3
	DPPAS	3
	DPPCE	1
	DPSES	1
	DPTEM	1
DP Total		**9**
DR	DR/GAB	2
	DRAGR	2
	DRCOM	3
	DRDAG	2
DR Total		**9**
DS	DS/GAB	1
	DSDES	2
	DSEDU II	5
	DSSAU	3
	DSSEG	1
DS Total		**12**
Total Geral		**47**

Tabela 3.4 – Quantidade de servidores de TI lotados nas áreas finalísticas da SFC.

Ressalta-se que, embora a autora desse trabalho também seja servidora que ingressou na CGU em vaga destinada a TI, estando lotada na DSSAU, ela não foi contabilizada no universo da pesquisa.

Os servidores foram convidados a responder ao questionário por meio de uma mensagem eletrônica enviada para seus endereços de *e-mail* funcional. Após 5 dias da primeira mensagem, foi enviado outro aviso alertando aqueles que ainda não tinham respondido sobre a proximidade do fim do prazo para resposta.

3.3.2 Resultados

Os resultados das pesquisas foram consolidados e deles foram extraídos informações e conclusões que serão aqui apresentados. Entretanto, antes da apresentação dos resultados, algumas considerações importantes devem ser feitas:

i. Os resultados demonstram percepções, ou seja, para uma mesma Coordenação há a possibilidade de existirem respostas divergentes em relação aos pontos de vista dos Coordenadores e dos servidores.
ii. O Coordenador da DRTES optou por responder o questionário duas vezes, pois sua Coordenação envolve duas realidades distintas, uma vez que é responsável por dois Ministérios: Ministério dos Esportes e Ministério do Turismo. Por isso, apenas para efeito dessa pesquisa, a DRTES será considerada como duas Coordenações separadas: DRTES-ESP e DRTES-TUR.
iii. Dos 24 Coordenadores, 20 responderam ao questionário, sendo que destes, apenas 3 preferiram responder ao questionário diretamente, sem a realização de entrevista. Entretanto, pelo motivo exposto no item anterior, serão consideradas 21 Coordenações na análise dos resultados.
iv. Dos 47 servidores do universo, 44 responderam ao questionário.
v. O Coordenador da DEFAZ I respondeu aos dois questionários, por ser Coordenador-Geral, mas ter ingressado na Carreira de Analista de Finanças e Controle nas vagas de TI.
vi. Para efeitos desse trabalho, são considerados servidores com conhecimento em TI os Analistas de Finanças e Controle (AFC) que entraram no Órgão em vagas específicas de TI; e Analistas e Técnicos de Finanças e Controle (TFC) que ingressaram em

vagas não específicas, mas são formados e/ou realizam ações de controle específicas na área de TI.

vii. Para efeito da pesquisa, foi pedido que os servidores e Coordenadores considerassem Auditoria de TI como sendo qualquer ação de controle dentro da Coordenação que envolva análise de um objeto de Tecnologia da Informação, independente de haver Ordem de Serviço formalizada.

viii. São considerados trabalhos genéricos de Auditoria de TI aqueles em que a TI não é o foco principal do trabalho, como por exemplo, a avaliação de um contrato de aquisição de *softwares* em uma Auditoria de Avaliação da Gestão.

ix. São considerados trabalhos específicos de Auditoria de TI aqueles em que a TI é o principal foco da ação de controle, como por exemplo, a análise de grandes bases de dados em busca de duplicidades e inconsistências; a avaliação de aspectos de segurança algum sistema corporativo; ou a análise da Governança de TI de alguma Unidade, entre outros.

x. Embora Auditoria de TI seja uma auditoria comum como qualquer outro tipo, para efeito desse trabalho, as demais auditorias (como de obras, de gestão, de acompanhamento, orçamentárias, entre outras) serão chamadas de Auditorias Comuns.

A seguir são apresentados os principais resultados da pesquisa:

3.3.2.1 Distribuição de Servidores de TI

A partir da lista informal de servidores de TI da SFC, de consultas a cada uma das Portarias de nomeação de servidores da CGU (de 2004 a 2008), à *intranet* da CGU e ao sistema SIAPE, foi possível fazer um levantamento da quantidade de servidores que ingressaram na CGU em vagas específicas de TI, conforme Tabela 3.5:

SERVIDORES DE TI NA CGU (PERÍODO: 2004 A 2009)			
SITUAÇÃO*	**LOTAÇÃO**		**QUANTIDADE**
TOTAL DE POSSES			**183**
TOTAL DE NOMEAÇÕES			**190**
Em exercício na CGU	SFC	Unidades finalísticas	38
		Outras Unidades	8
		TOTAL SFC	**46**
	Coordenações Regionais		13
	Outras		82
	TOTAL CGU		**141**
Exonerações e/ou vacâncias			36
Em exercício em outro Órgão			2
Aposentadoria			1
Falecimento			1

* Dados referentes à situação dos servidores de TI em 01/12/2009.

Tabela 3.5 – Situação atual dos servidores que entraram em vagas específicas de TI.

Observa-se que a CGU registra um percentual de perda de servidores de TI, de 2004 a 2009, de 23%.

Não há dados oficiais que permitam fazer afirmações sobre a perda de servidores de TI especificamente na SFC. No entanto, com base em coleta informal, estima-se que esta perda, seja proporcional ou superior à da CGU como um todo, pois, além dos servidores que mudam de Órgão, a SFC acaba por perder servidores de TI com as remoções e permutas internas.

Cabe ressaltar que, em setembro de 2009, na ocasião de realização da pesquisa, 41 servidores que ingressaram em vagas específicas de TI estavam lotados em Unidades finalísticas da SFC. Em novembro, dois desses servidores foram removidos para Coordenações Regionais e um pediu vacância para tomar posse em outro Órgão.

No caso da lista de servidores de TI que participaram do universo da pesquisa, pelo conhecimento e percepção que possuem da área de TI, também foram considerados alguns casos excepcionais de servidores não graduados em alguma área de Tecnologia da Informação, mas que, por necessidade/interesse, atuam nessa área e de servidores formados em alguma área de conhecimento de TI, mas que ingressaram na CGU em vagas destinadas à execução de Auditoria Comum.

Portanto, para efeito dessa pesquisa, será considerado o universo dos 47 servidores apresentados na Tabela 3.4. Assim, a quantidade de servidores de TI por Coordenação de áreas finalísticas da SFC pode ser visualizado no gráfico a seguir:

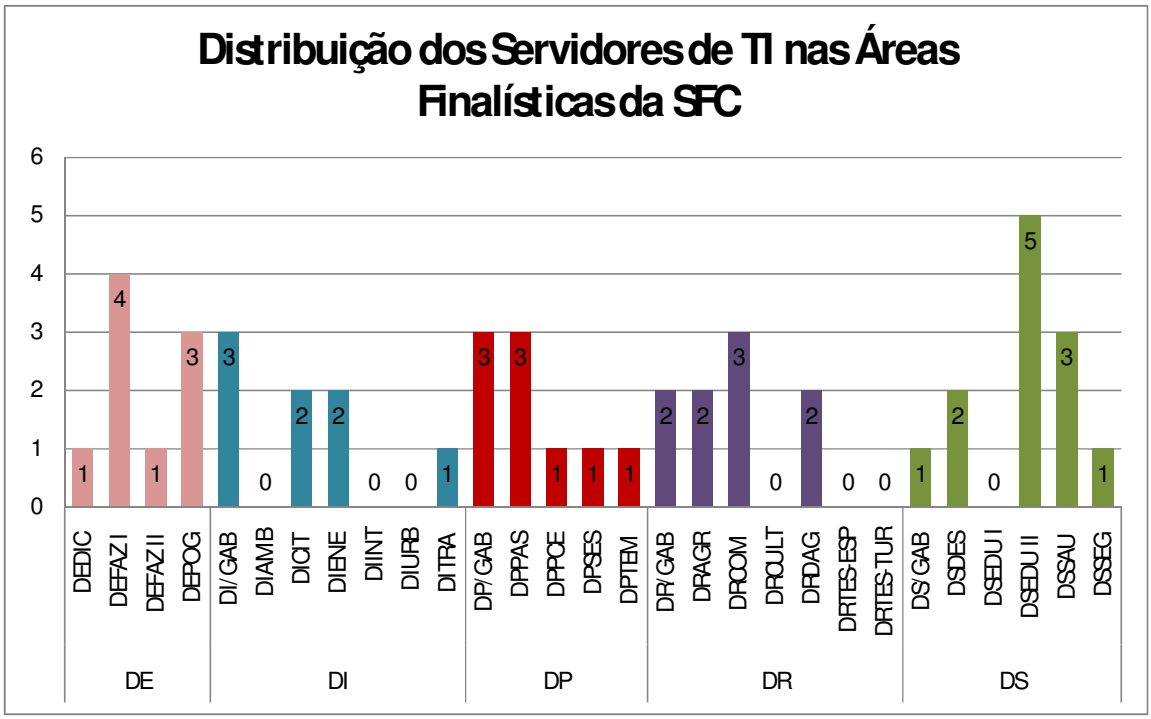


Figura 3.9 – Distribuição dos servidores de TI nas áreas finalísticas da SFC.

A distribuição dos 47 servidores de TI por Diretoria de áreas finalísticas da SFC é apresentada no gráfico a seguir:

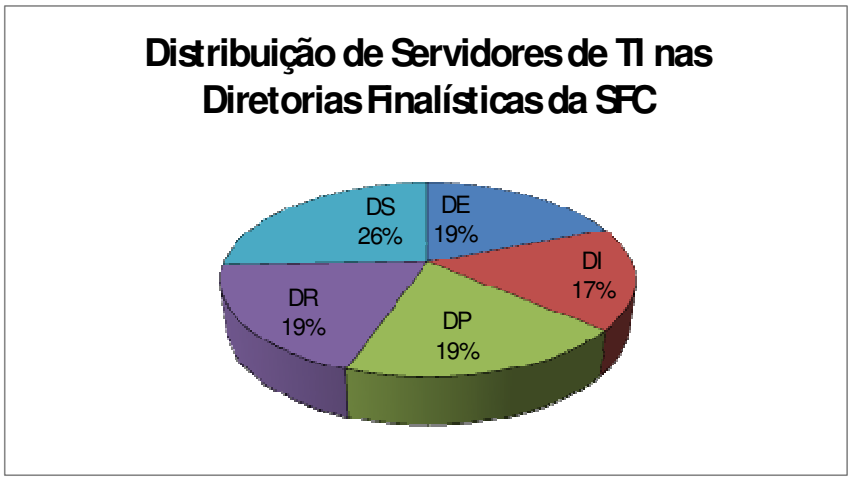


Figura 3.10 – Distribuição de servidores de TI nas Diretorias finalísticas da SFC.

Das 25 Coordenações finalísticas (considerando a DRTES como duas: DRTES-ESP e DRTES-TUR), 18 (72%) possuem servidores com conhecimento em TI em seu corpo técnico.

3.3.2.2 Grau de necessidade da Auditoria de TI dentro da SFC

Perguntados sobre como poderia ser classificada a necessidade de TI dentro do escopo da Coordenação, 24% dos Coordenadores afirmaram que a necessidade é Muito Alta, outros 52% afirmaram que a necessidade é Alta e os demais 24% afirmaram que a necessidade é Média, conforme gráfico a seguir:

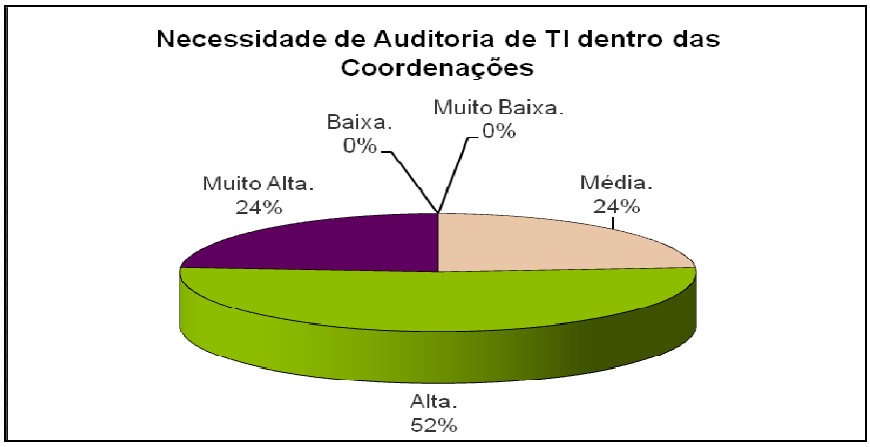


Figura 3.11 – Necessidade de Auditoria de TI (percepção dos Coordenadores).

Dos 44 servidores que participaram da pesquisa, perguntados sobre como poderia ser classificada a necessidade de TI dentro do escopo da Coordenação, 27% dos servidores afirmaram que a necessidade é Muito Alta, outros 48% afirmaram que é Alta, 11% afirmaram que é Média, 5% afirmaram que é Baixa e os demais 9% afirmaram que é Muito Baixa, conforme gráfico a seguir:

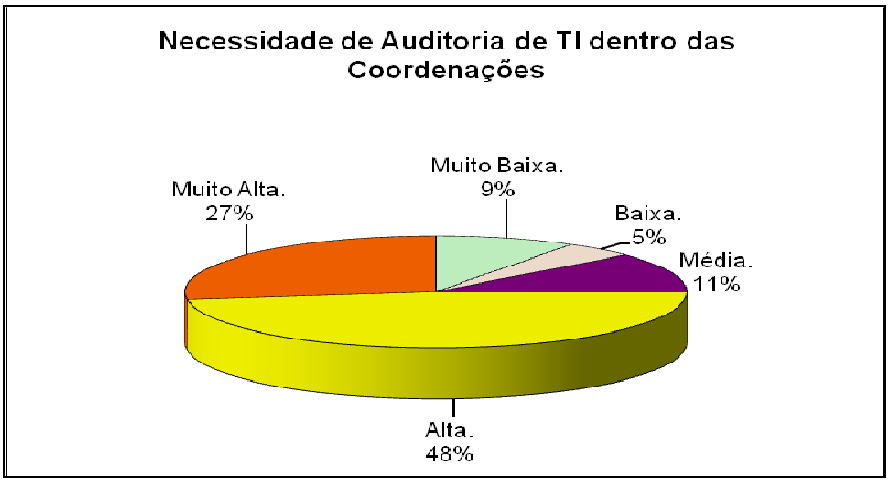


Figura 3.12 - Necessidade de Auditoria de TI (percepção dos servidores de TI).

A comparação das opiniões dos Coordenadores e dos servidores possibilita fortalecer o diagnóstico do grau de necessidade de Auditoria de TI em cada área finalística da SFC, conforme tabela a seguir:

GRAU DE NECESSIDADE DA AUDITORIA DE TI			
DIRETORIA	**COORDENAÇÃO**	**OPINIÃO DO COORDENADOR**	**DISTRIBUIÇÃO DA OPINIÃO DOS SERVIDORES**
DE	DEDIC	Alta.	Alta.
	DEFAZ I	Alta.	Média.
			Alta.
			Muito Alta.
	DEFAZ II	Alta.	Média.
			Alta.
	DEPOG	Muito Alta.	Alta.
			Alta.
			Muito Alta.
DI	GAB/DI	NA	Alta.
			Baixa.
			Muito Baixa.
	DICIT	Média.	Muito Baixa.
			Média.
	DIENE	Média.	Alta.
			Alta.
	DITRA	Alta.	QNR
DP	GAB/DP	NA	Muito Alta.
			Muito Alta.
	DPPAS	Muito Alta.	Muito Alta.
			Alta.
			Muito Alta.
	DPPCE	Muito Alta.	Alta.
	DPSES	QNR	Alta.
	DPTEM	Alta.	Muito Alta.
DR	GAB/DR	NA	Baixa.
			Muito Alta.
	DRAGR	QNR	Alta.
	DRCOM	QNR	Muito Baixa.
			Alta.
			Alta.
	DRDAG	QNR	Muito Alta.
			Muito Alta.
DS	GAB/DS	NA	Muito Baixa.
	DSDES	Muito Alta.	Muito Alta.
			Muito Alta.
	DSEDU II	Alta.	Alta.
			Alta.
			Alta.
			Alta.
			Alta.
	DSSAU	Alta.	Alta.
			Média.
			Alta.
	DSSEG	Média.	Média.

NA: Não se aplica por se tratar de Gabinete de Diretoria. QNR: Questionário não respondido.

Tabela 3.6 – Comparação das opiniões dos Coordenadores e Servidores: necessidade Auditoria de TI.

Ressalta-se que a tabela anterior apenas contemplou as respostas dos Coordenadores que possuem servidores de TI em seu corpo técnico. Observa-se que na DE, na DP e na DS, em geral, as opiniões dos servidores foram ao encontro das opiniões dos Coordenadores.

A DI foi a Coordenação que apresentou mais divergência de opiniões. Esse fato pode ser explicado pela grande importância que apresenta outro tipo de auditoria temática: a Auditoria de Obras. Como a área de atuação primária na DI é infra-estrutura, em geral, a TI acaba ficando em segundo plano, apesar de também ser necessária em algumas das Coordenações dessa Diretoria.

Em relação à DR, verifica-se que não há censo sobre a necessidade de Auditoria de TI na Diretoria, uma vez que dentro de uma mesma Unidade existem opiniões conflitantes, até mesmo pela diversidade de temas tratados pelas Coordenações que compõem a Diretoria. Além disso, devido ao fato de os Coordenadores da DR que possuem servidores de TI em seu corpo técnico não terem respondido ao questionário, não é possível fazer comparação de opiniões.

Um caso a parte são os 9 servidores que se encontram lotados nos gabinetes das Diretorias. A DP é uma Diretoria que centraliza muitos dos trabalhos de Auditoria de TI no próprio Gabinete, tendo seus servidores a percepção de que a necessidade é Muito Alta. Por outro lado, a DI tem seu Gabinete focado em Auditorias de Obras, sendo a necessidade de Auditoria de TI mínima nessa Unidade. Já o gabinete da DS não realiza trabalhos nessa área, embora a demanda seja alta nas Coordenações da Diretoria.

Já nas Coordenações que não possuem servidores de TI, o grau de necessidade de Auditoria de TI configura-se da seguinte forma:

GRAU DE NECESSIDADE DA AUDITORIA DE TI		
DIRETORIA	**COORDENAÇÃO**	**OPINIÃO DO COORDENADOR**
DI	DIAMB	Alta.
	DIINT	Alta.
	DIURB	Alta.
DR	DRCULT	Alta.
	DRTES-ESP	Média.
	DRTES-TUR	Média.
DS	DSEDUT	Muito Alta.

Tabela 3.7 – Necessidade de Auditoria de TI das Coordenações sem servidores de TI.

Observa-se que as Coordenações DIAMB, DIINT, DIURB e DRCULT, que consideram Alta a necessidade de Auditoria de TI dentro de seus trabalhos, não possuem nenhum servidor de TI em seu corpo técnico.

Cabe observar que no caso das Coordenações DSEDU I e DSEDU II, houve uma opção estratégica de se manter os 5 servidores de TI na DSEDU II como forma de se treinar os servidores e coordenar melhor os trabalhos na área de Educação. Assim, formou-se um núcleo informal de TI que atua em trabalhos de Auditoria de Tecnologia da Informação em ambas as Unidades.

Salienta-se que a pesquisa realizada apresenta as percepções dos participantes, podendo servir como base para um trabalho mais detalhado em que se realize um diagnóstico técnico para se determinar e hierarquizar as prioridades de Auditoria de TI dentro da SFC.

3.3.2.3 Trabalhos realizados

Dos 21 Coordenadores que responderam aos questionários, 14 (66,70%) possuem servidores de TI em seu corpo técnico e 7 (33,30%) não possuem.

No caso dos Coordenadores, apenas 57% afirmaram que já foram realizados trabalhos específicos de Auditoria de TI em sua Coordenação, apesar de 66,70% possuírem servidores de TI. Por outro lado, 86% afirmaram que já foram realizados trabalhos genéricos de Auditoria de TI, fato que demonstra que mesmo não possuindo servidores especializados, algumas Unidades já realizam trabalhos, mesmo que superficiais, na Área.

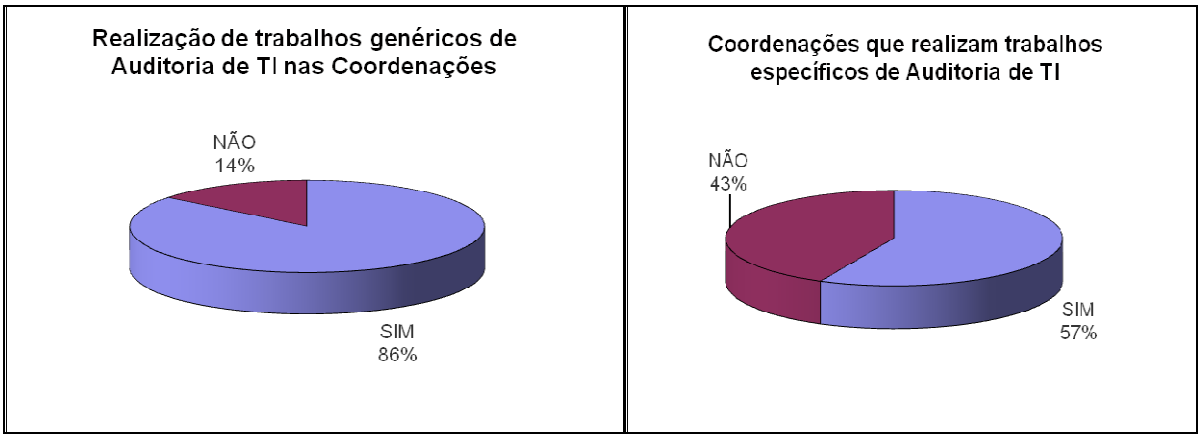


Figura 3.13 – Realização de trabalhos de Auditoria de TI (percepção dos Coordenadores).

Como exemplos de trabalhos genéricos de Auditoria de TI apresentados pelos entrevistados, podem-se citar:

- DPPAS: no âmbito do Ministério da Previdência Social - MPS, foi realizada uma verificação da contratação de empresa para a prestação de serviços de informática.
- DIINT: análise do contrato de gerenciamento de informações relativas ao projeto transposição do São Francisco.

- DSSAU: análise de contratos de aquisição de *softwares*, de terceirizados de TI, e de dispensa de licitação para desenvolvimento de sistema de gestão de despesas para uma autarquia durante Avaliação da Gestão.

Como exemplos de trabalhos específicos de Auditoria de TI citados pelos entrevistados, podem-se citar:

- DSDES: análise de duplicidades de base de dado de pagamentos do Programa Bolsa Família e cruzamento entre benefícios do PBF (Programa Bolsa Família) x Pronaf (Programa Nacional de Fortalecimento da Agricultura Familiar).
- DPPAS: batimentos das informações constantes das bases de dados dos sistemas corporativos do INSS, com vistas à verificação da regularidade dos pagamentos dos benefícios previdenciários.
- DIENE: Todos os contratos de informática, de 2003 a 2008, da SPOA do Ministério de Minas e Energia (MME).
- DSSAU: Auditoria de aspectos de segurança e integridade da informação do GESCON, sistema informatizado que gerencia convênios, no Fundo Nacional de Saúde.
- DEPOG: Auditoria de acompanhamento nos processos de pagamento do contrato celebrado entre o Ministério do Planejamento e o Serpro tendo como objeto o Sistema de Integrado de Administração de Recursos Humanos (SIAPE) e auditoria de acompanhamento na nova contratação de serviços de TI realizada pelo Ministério do Planejamento em 2009, sob a ótica da Instrução Normativa nº 04/2008.
- DSEDU II: Análise de contratos de aquisições de computadores para distribuição em escolas do Brasil e Cruzamento dos registros referentes aos 240.000 servidores ativos dos Sistemas RAIS X SIAPE x Sistema de Avaliação do INEP, a fim de diagnosticar recebimentos indevidos.

Dos Servidores que participaram da pesquisa, 66% afirmaram que já foram realizados trabalhos específicos e 77% afirmaram que já foram realizados trabalhos genéricos de Auditoria de TI em suas Unidades de lotação, desde 2004. Ressalta-se que as afirmações dos servidores não incluem os trabalhos de Auditoria de TI realizados nas Coordenações que não possuem servidores de TI.

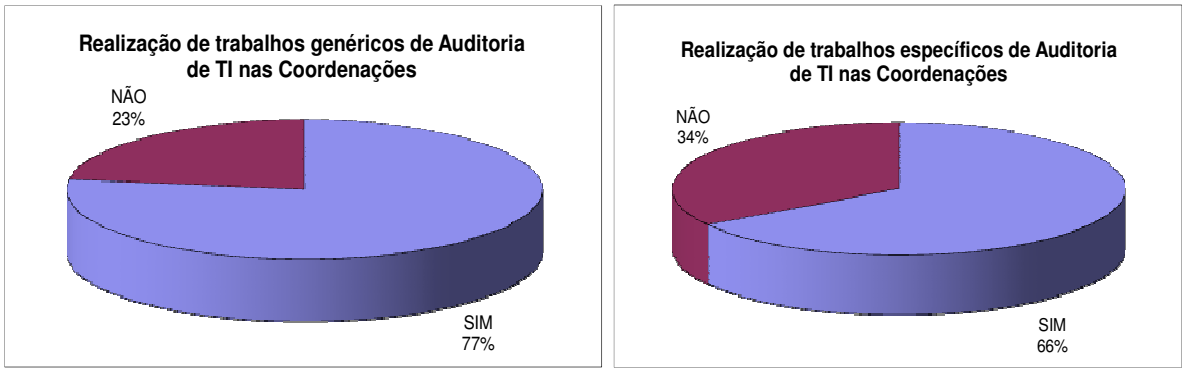
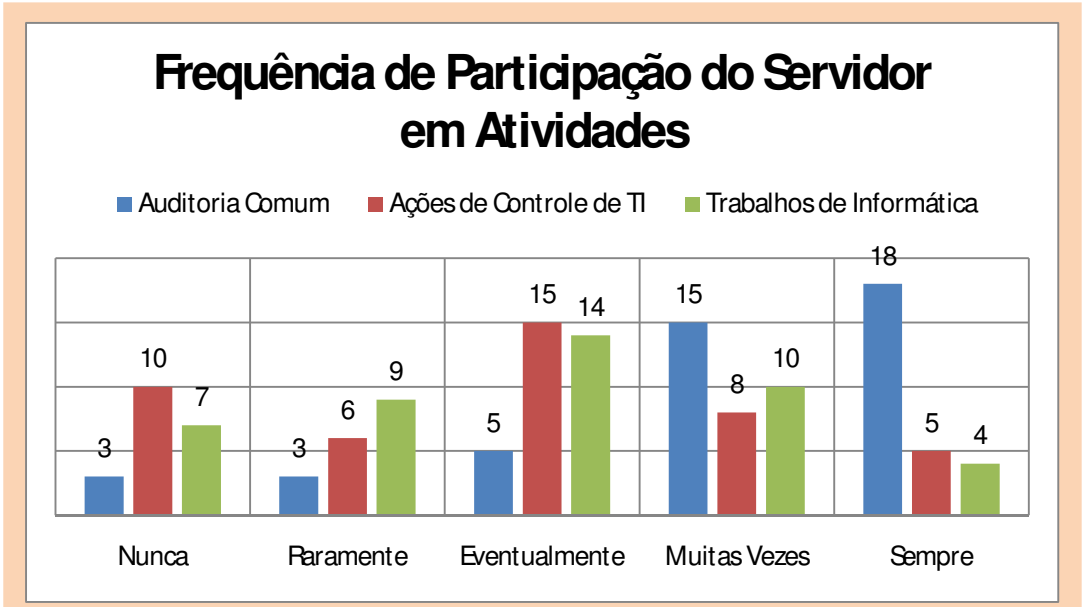


Figura 3.14 – Realização de trabalhos de Auditoria de TI (percepção dos servidores de TI).

Perguntados sobre a opção que melhor retrata a frequência com que o servidor realizou atividades de Auditoria Comum, Ações de Controle com foco em TI[10] e Trabalhos de Informática[11] no último ano, os servidores se manifestaram da forma apresentada no gráfico a seguir:



	Nunca	Raramente	Eventualmente	Muitas Vezes	Sempre
Auditoria Comum	6,82%	6,82%	11,36%	34,09%	40,91%
Ações de Controle de TI	22,73%	13,64%	34,09%	18,18%	11,36%
Trabalhos de Informática	15,91%	20,45%	31,82%	22,73%	9,09%

Figura 3.15 – Frequência de participação do servidor em atividades.

Com base nos dados apresentados, conclui-se que 75% dos servidores realizam trabalhos de Auditoria Comum Muitas Vezes ou Sempre, enquanto apenas 29,54% executam a ações de controle

[10] Auditorias e fiscalizações cujo objeto seja referente à área de Tecnologia da Informação.
[11] Trabalhos de suporte de informática, tais como configuração de impressora, formatação de documentos, entre outros.

com foco em TI Muitas Vezes ou Sempre, sendo que a maioria desses servidores (85,11% do universo) prestou concurso para vagas específicas de TI.

Outra questão que merece destaque nos resultados é que, somando-se as freqüências Eventualmente, Muitas Vezes e Sempre, observa-se que 63,64% dos colaboradores da pesquisa executam trabalhos relacionados à informática (sem foco em Auditoria), embora a CGU tenha uma área específica para esse tipo de demandas, a Diretoria de Sistemas e Informação (DSI). Inclusive, por meio do Memorando-Circular nº 0200/2004/SCGU/CGU-PR, de 22 de novembro de 2004, foi recomendado às demais áreas da CGU que não desenvolvessem soluções de informática, salvo os casos que fossem previamente justificados e acordados junto à DSI. O suporte técnico aos usuários também é realizado pela DSI, por meio de empresa terceirizada.

3.3.2.4 Níveis de Maturidade

Baseado no COBIT 4.1 (IT GOVERNANCE INSTITUTE, 2007), foram adaptados seus níveis de maturidade para o processo de Auditoria de TI, resultando nos níveis a seguir relacionados:

0 – Inexistente: A Coordenação não reconhece a existência de um processo de Auditoria de TI.

1 – Inicial /Ad-Hoc: Há evidências de que a Coordenação reconhece que o processo de Auditoria de TI existe e que as necessidades devem ser mapeadas. Entretanto, não há um processo padronizado e a execução das ações de controle de TI é feita caso a caso e baseada apenas nos processos genéricos de auditoria da Secretaria Federal de Controle.

2 – Repetível, porém intuitivo: Os processos para a realização de Auditoria de TI são estruturados e procedimentos similares são seguidos por diferentes indivíduos para a mesma tarefa dentro da Coordenação. Há forte dependência do conhecimento individual e existe alguma documentação.

3 – Definido: Os processos de Auditoria de TI são padronizados, documentados e comunicados dentro da Coordenação. Entretanto, deixa-se a cargo dos indivíduos seguirem os processos. Não há certeza de que eventuais desvios serão detectados.

4 – Gerenciado: Existe a possibilidade de monitorar e medir a conformidade dos processos de Auditoria de TI com os procedimentos definidos dentro da própria Coordenação. Há ações para melhoria.

5 – Otimizado: Os processos foram refinados até alcançarem as melhores práticas, com base no resultado de melhoria contínua e comparações com outras organizações e coordenações.

No caso dos Coordenadores, com o objetivo de não influenciar suar respostas, não lhes foi apresentado nem os números nem os nomes de cada nível, apenas as definições. Com base nessa classificação, os Coordenadores tiveram a seguinte percepção da maturidade do processo de Auditoria de TI em suas Coordenações:

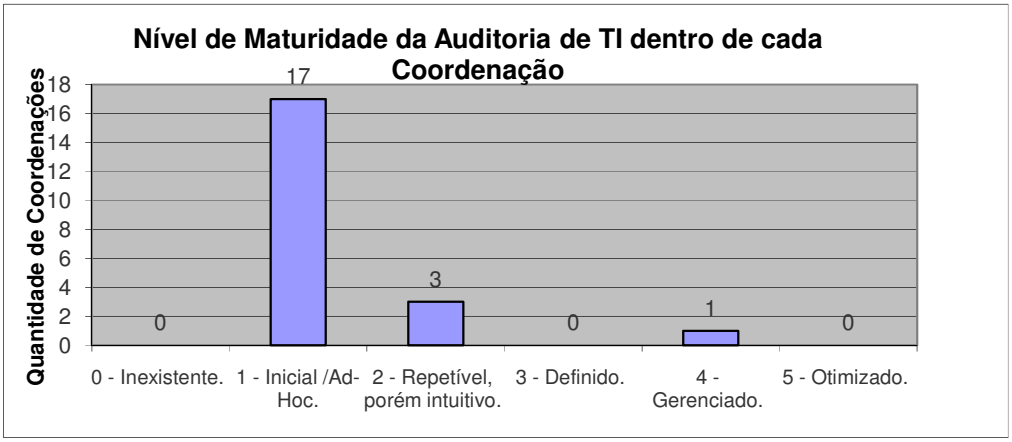


Figura 3.16 – Nível de Maturidade da Auditoria de TI (perspectiva dos Coordenadores).

Apenas um Coordenador classificou sua Unidade como estando no nível de maturidade 4 – Gerenciado, estando fora do padrão observado nas demais, onde a maioria das Unidades foi classificada no nível 1-Inicial/*Ad Hoc* e algumas no nível 2- Repetível, porém intuitivo.

A tabela a seguir apresenta as ocorrências dos Níveis de Maturidade das Coordenações sob a ótica dos servidores de TI:

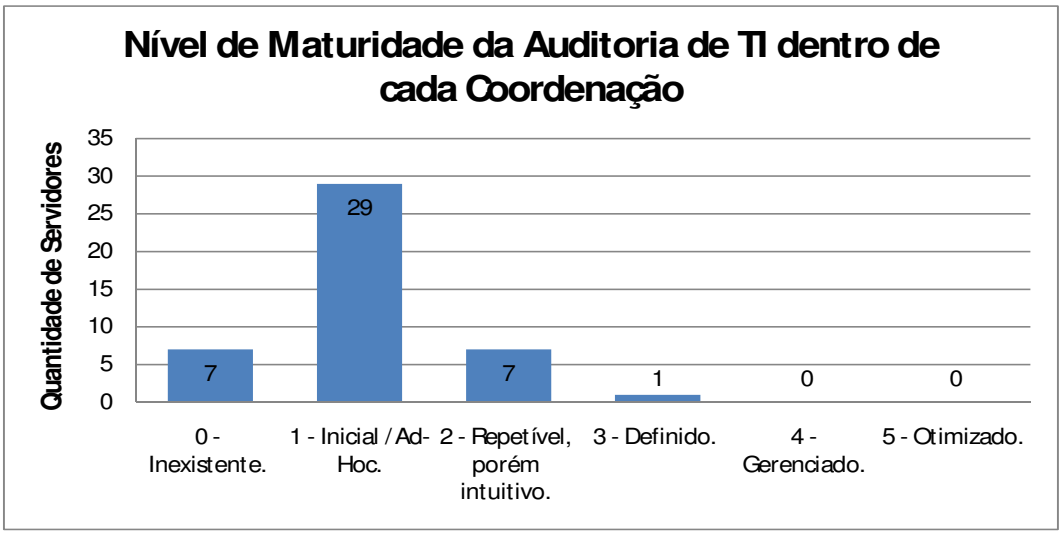


Figura 3.17 – Nível de Maturidade da Auditoria de TI (perspectiva dos servidores de TI).

Vale ressaltar que o nível de maturidade da Auditoria de TI nas Coordenações está diretamente relacionado com o nível de maturidade da Auditoria de TI na SFC. Assim, por a pesquisa ter sido censitária, pelos resultados, pode-se inferir que o nível de maturidade de Auditoria de TI predominante na SFC é o 1 - Inicial/*Ad-Hoc*. Casos em que os níveis de maturidade estão mais elevados do que a média são, provavelmente, esforços isolados da própria Coordenação.

3.3.2.5 Dificuldades

Os Coordenadores foram questionados sobre quais são as dificuldades enfrentadas para a realização de Auditorias de TI. A lista de dificuldades está a seguir apresentada:

Código	Dificuldades
A	Tempo insuficiente para a realização dos trabalhos.
B	Falta de apoio da alta administração.
C	Não é uma prioridade dentro da Coordenação.
D	Falta de servidores capacitados em Auditoria de TI.
E	Deficiência nos procedimentos de Auditoria de TI.
F	Deficiência de recursos tecnológicos.
G	Ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI.
H	Falta de apoio técnico sobre Auditoria de TI.
I	Inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC.
J	Outras.

Tabela 3.8 – Dificuldades enfrentadas para a realização de Auditoria de TI (perspectiva dos Coordenadores).

Solicitou-se aos entrevistados que selecionassem todas as alternativas aplicáveis à Coordenação, mas que somente escolhessem aquelas que representassem problemas efetivamente enfrentados durante trabalhos de Auditoria de TI. Assim, por mais que não exista apoio técnico sobre Auditoria de TI dentro da SFC, por exemplo, esse item só deveria ser escolhido se esse fato já tivesse sido um problema enfrentado pela Coordenação. Os resultados são apresentados a seguir:

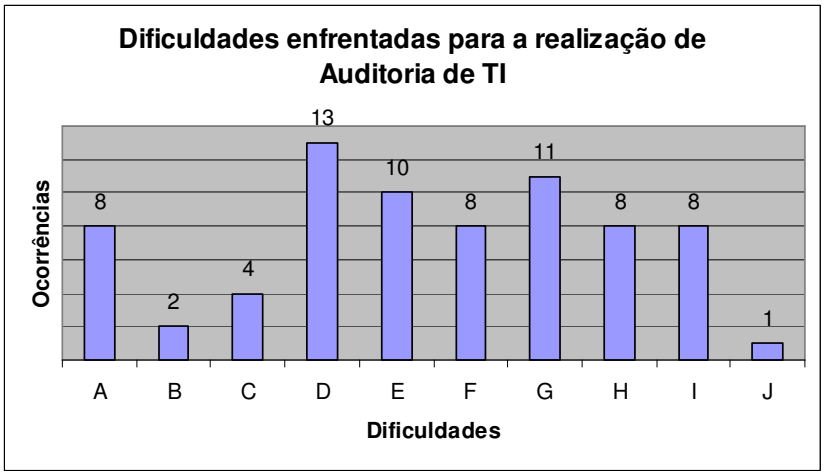


Figura 3.18 – Ocorrências das dificuldades enfrentadas para a realização de Auditoria de TI (perspectiva dos Coordenadores).

Dessa forma, a dificuldade relatada com maior freqüência foi a falta de servidores capacitados em Auditoria de TI. Esse item foi marcado todas as vezes em que a quantidade de servidores de TI fosse insuficiente dentro da Coordenação para o volume de ações de controle necessárias nessa área e/ou quando as especificidades dos trabalhos exigissem capacitações/treinamentos mais específicos.

As outras duas dificuldades de maior freqüência entre os entrevistados foram a deficiência nos procedimentos de Auditoria de TI e a ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI.

Os servidores também foram questionados sobre as dificuldades enfrentadas para a realização de Auditorias de TI. A lista de dificuldades está a seguir apresentada:

Código	Dificuldades
A	Tempo insuficiente para a realização dos trabalhos.
B	Falta de apoio da alta administração.
C	Falta de prioridade dentro da Coordenação.
D	Falta de incentivo dentro da Coordenação.
E	Deficiência na capacitação para esse tipo de auditoria.
F	Deficiência nos procedimentos de Auditoria de TI.
G	Deficiência de recursos tecnológicos.
H	Ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI.
I	Falta de apoio técnico sobre Auditoria de TI.
J	Inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC.
K	Outras.

Tabela 3.9 – Dificuldades enfrentadas para a realização de Auditoria de TI (perspectiva dos servidores de TI).

Assim como ocorreu com os Coordenadores, solicitou-se aos servidores que selecionassem as alternativas aplicáveis à Coordenação, mas que somente escolhessem aquelas que realmente tenham sido problemas enfrentados durante trabalhos de Auditoria de TI. Os resultados estão relacionados a seguir:

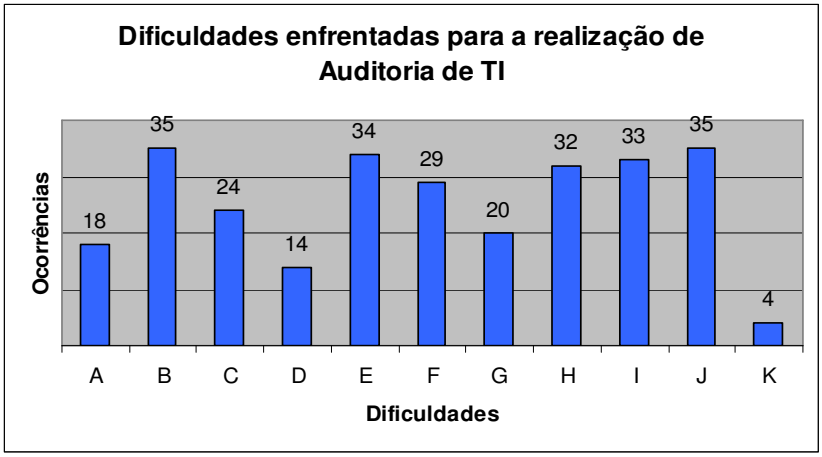


Figura 3.19 – Ocorrências das dificuldades enfrentadas para a realização de Auditoria de TI (perspectiva dos servidores de TI).

No caso dos servidores, cinco dificuldades foram apontadas por mais de 80% dos servidores: falta de apoio da alta administração, deficiência na capacitação para esse tipo de auditoria, ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI, falta de apoio técnico sobre Auditoria de TI e inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC.

3.3.2.6 Critérios de Auditoria utilizados

De acordo com o GAO (GAO, 1994), os critérios de auditoria são os "(...) padrões utilizados para determinar se uma dada condição satisfaz ou supera o esperado."

Segundo o Manual de Auditoria de Natureza Operacional do TCU (TCU, 2000), os critérios de auditoria são fixados no decorrer do levantamento, ao final do qual devem estar suficientemente precisos e detalhados, para que possam desempenhar, em relação à auditoria que será executada, os papéis descritos abaixo:

- definição de um arcabouço conceitual básico, facilitando a comunicação entre os membros da equipe, bem como entre essa e, de um lado, os demais integrantes do TCU e, de outro, os gestores do objeto da auditoria;
- delimitação do escopo da auditoria, tornando palpáveis os seus objetivos;
- orientação da coleta de dados, indicando como obter evidências significativas;
- fixação de parâmetros balizadores das conclusões e recomendações da auditoria.

Os critérios de auditoria podem ser encontrados nos relatórios de auditorias já realizadas, na legislação pertinente, nas normas internas do objeto da auditoria, nas informações prestadas pelos gestores e no desempenho observado no passado ou em situações similares.

Na pesquisa, foi solicitado aos servidores que, no caso de existirem Auditorias de TI na Coordenação, informassem quais os critérios de auditoria utilizados nessas ações de controle. O resultado é apresentado na tabela seguinte:

CRITÉRIOS DE AUDITORIA	OCORRÊNCIA
LEI nº 8.666/93. (BRASIL, 1993)	27
Acórdãos do TCU.	26
Instrução Normativa nº 04/2008. (BRASIL, 2008a)	20
LEI nº 10.520/2002. (BRASIL, 2002b)	19
COBIT 4.1. (IT GOVERNANCE INSTITUTE, 2007)	14
NBR ISO/IEC 27002:2005 (NBR ISO/IEC 17799:2005). (ABNT, 2005)	11
ITIL v.3. (OGC, 2009)	7
Outros.	2

Tabela 3.10 – Critérios de Auditoria de TI.

Importante observar que os Acórdãos do TCU só ficam abaixo da Lei nº 8.666/93 em número de ocorrências. Tal fato pode dar-se por três motivos: 1) a abrangência dos assuntos tratados pelos Acórdãos; 2) as lacunas legais existentes para vários problemas encontrados durante as ações de controle; e 3) a experiência já adquirida pelo TCU nesse tipo de auditoria. Por emanarem recomendações e determinações acerca do assunto, servem de diretrizes para os trabalhos.

Verificou-se que a base utilizada para definição dos critérios de Auditoria de TI são essencialmente a mesma utilizada por outros Órgãos de controle, como o TCU, demonstrando que a maioria dos instrumentos teóricos para a realização desse tipo de auditoria está disponível e é conhecida. Todavia, observa-se que esse simples conhecimento não é suficiente para a estruturação e aprimoramento do processo de auditoria de TI no âmbito da SFC.

Os critérios mais utilizados também são um indicativo de que o tipo de Auditoria de TI predominante nos trabalhos da SFC é a que envolve a análise de licitações e contratos de TI.

3.4 Considerações acerca do Diagnóstico

No contexto da SFC, a perda de aproximadamente 23%, de 2004 a 2009, dos servidores de TI, abordada no item 3.3.2.1, acarreta na perda de quase ¼ do conhecimento da Secretaria em Auditoria de Tecnologia da Informação, uma vez que, em geral, em decorrência do nível de maturidade predominante na SFC**,** o conhecimento nesse tipo de Auditoria é baseado no indivíduo e não nos processos organizacionais. Quando se analisa cada Coordenação isoladamente, a perda de conhecimento pode chegar a 100%, principalmente no caso daquelas que possuem apenas um servidor de TI.

Com base na seção 3.3.2.2, observou-se que, no geral, é consenso entre Coordenadores e servidores de TI a alta necessidade da Auditoria de TI no âmbito de suas Coordenações.

Além disso, verificou-se que a estratégia de distribuir os servidores de TI dentro da SFC sem que houvesse apoio institucional formalizado, apoio técnico e capacitação para a realização de Auditoria de TI teve como consequência o subaproveitamento do conhecimento específico desses servidores e o desvio de foco dos trabalhos realizados por eles.

A maioria, 70% de todos os participantes da pesquisa, considerou que suas Coordenações se enquadram no Nível de Maturidade **"1 – Inicial /Ad-Hoc"**, em que há evidências de que a Coordenação reconhece que o processo de Auditoria de TI existe e que as necessidades devem ser mapeadas. Entretanto, não há um processo padronizado e a execução das ações de controle de TI é

feita caso a caso e baseada apenas nos processos genéricos de auditoria da Secretaria Federal de Controle.

Observou-se também que as dificuldades enfrentadas para a realização de Auditoria de TI dentro da Coordenação guardam coerência entre ambos os pontos de vista:

a) Para os Coordenadores, a falta de servidores capacitados, que envolve tanto a quantidade insuficiente de servidores de TI quanto a deficiência de capacitação específica para os servidores de TI existentes nas Unidades, foi o item de maior ocorrência. Essa dificuldade é coerente com a terceira de maior ocorrência por parte dos servidores, a deficiência na capacitação para esse tipo de auditoria.
b) A ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI e a falta de apoio técnico sobre Auditoria de TI foram duas dificuldades que foram apontadas por mais de 60% do total de participantes da pesquisa. Essas duas dificuldades influenciam diretamente na qualidade dos trabalhos realizados, uma vez que a ausência de uma padronização de linguagem de Auditoria de TI contribui para a realização de ações de controle desordenadas, com critérios de avaliação diferentes e, muitas vezes, para um mesmo tipo de constatação, recomendações incoerentes e conflitantes, dificultando a comunicação entre auditor e auditado. A falta de apoio técnico impossibilita o monitoramento e uma melhoria institucional e eficaz desse tipo de auditoria.
c) As dificuldades do item b são consequência de outra dificuldade que apresentou alta ocorrência (66,15%): a inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC. Em decorrência do modelo de alocação pulverizada dos servidores de TI dentro da SFC, a inexistência desse núcleo é uma barreira à centralização de conhecimentos e informações sobre Auditoria de TI, que poderiam ser acessados e repassados a todos de maneira institucional, evitando que a única opção aos servidores que realizem esse tipo de auditoria seja a consulta a fontes alternativas e, muitas vezes, ineficazes e não seguras.

Todavia, houve a aparente discordância entre Coordenadores e servidores acerca de uma dificuldade: a falta de apoio da alta administração para a realização de Auditorias de TI. Esse tipo de questão, diferentemente das demais, está sujeita a percepções altamente influenciadas por fatores organizacionais do Órgão. Provavelmente, os Coordenadores interpretaram essa dificuldade como

uma questão impositiva, ou seja, para a maioria deles, não há da alta administração nenhum ato que impossibilite a realização de Auditorias de TI. Por outro lado, para os servidores de TI, essa dificuldade pode ter sido interpretada como uma questão omissiva, ou seja, o fato de a alta administração não emitir atos que demonstrem incentivo à Auditoria de TI demonstram sua falta de apoio.

Dessa forma, verificou-se que a Auditoria de TI ainda é um processo incipiente dentro da SFC, apesar da alta necessidade diagnosticada. Assim, o resultado do Diagnóstico vem ao encontro da proposta a ser apresentada nesse trabalho, uma vez que este visa mitigar os principais problemas enfrentados.

4 UNIDADE DE TEMAS ESPECÍFICOS

Apesar de a SFC ter como forma tradicional de atuação a divisão de Coordenações baseada na divisão ministerial do Governo Federal, existem algumas Unidades que são voltadas para atuação acerca de temas específicos.

Das Unidades voltadas a temas dentro das SFC, três são voltadas a atividades de auditorias e fiscalizações: a Coordenação-Geral de Recursos Externos (DCREX), a Coordenação-Geral de Auditoria da Área de Pessoal e Benefícios e de Tomada de Contas Especial (DPPCE) e a Assessoria de Obras da Diretoria de Auditoria da Área de Infra-Estrutura.

Por meio da aplicação de questionários procurou-se compreender as atribuições, a forma de atuação e os motivos que levaram à criação dessas Unidades que exercem ou apóiam ações de controles voltadas a temas. Os três Coordenadores das Unidades de temas específicos responderam ao questionário por meio de entrevista.

Além disso, foi realizada uma entrevista, não prevista inicialmente, com o responsável pelo Observatório de Despesas Públicas (ODP), Unidade não pertencente à SFC, devido às suas características inovadoras em relação ao contexto da CGU.

4.1 DCREX

A Coordenação-Geral de Recursos Externos (DCREX) existe desde 1992, quando fazia parte da Secretaria do Tesouro Nacional (STN), tendo recebido seu nome atual em 2006. O Decreto nº 5.683/2006 vinculou a Coordenação-Geral de Recursos Externos ao Gabinete da SFC e, posteriormente, foi alterado pelo Decreto nº 6.656/2008 que transferiu a Coordenação para o âmbito da Diretoria de Planejamento e Coordenação das Ações de Controle.

A criação da Coordenação foi motivada pelo fato de que, por exigência dos Organismos Internacionais, o Governo Federal teria que manter uma unidade de controle para atender às auditorias específicas demandadas pelos acordos internacionais.

Dentre as diversas atribuições da Unidade, para o contexto desse trabalho, destacam-se principalmente:

- Coordenar as ações de controle relativas ao acompanhamento e avaliação dos projetos de cooperação técnica internacional e projetos de financiamentos externos.
- Negociar com os Bancos internacionais e Organismos de Cooperação as carteiras de projetos auditadas ano a ano.

- Manter o controle de qualidade dos relatórios por intermédio de revisões constantes de todos os relatórios produzidos pelas Unidades da SFC.
- Elaborar material instrucional referente a normas e procedimentos internacionais aplicáveis ao tema.
- Elaborar e Ministrar cursos de atualização dos auditores sobre o tema auditoria de recursos externos.
- Elaborar e ministrar cursos de capacitação de gestores.
- Realizar auditorias em projetos de outros poderes (legislativo e judiciário), além de projetos estaduais, quando a SFC/CGU é convidada a proceder desta forma.
- Assessorar o Gabinete da SFC e da Secretaria Executiva sobre o tema.

A Coordenação funciona como apoio técnico às demais Unidades, realizando apenas ações de controle em casos excepcionais. Assim, as ações de controle que envolvem recursos externos são realizadas prioritariamente pelas Coordenações finalísticas da SFC/CGU, ficando a cargo da DCREX a realização direta apenas de auditorias específicas em projetos de outros poderes no âmbito federal (por exemplo, os projetos do TCU, do Senado e dos Tribunais Superiores), de Estados e/ou de Municípios quando solicitada pelos Organismos Internacionais ou por algum outro Órgão do governo.

De acordo com o Coordenador da Unidade, a importância da existência de unidade especializada, como é o caso da DCREX, deve-se ao fato de ser necessária a manutenção de um acervo de conhecimento vivo, além de registros documentais, sobre a experiência de auditoria junto a Organismos Internacionais. Sem esta experiência não seria possível o reconhecimento das técnicas de trabalho da CGU na esfera internacional e também seria dificultada a atualização dos procedimentos de auditoria. Ainda de acordo com o Coordenador, os especialistas são a garantia de que os generalistas não se percam em sua generalidade, tendendo à superficialidade. Com isso, as unidades especializadas complementam a visão generalista das unidades finalísticas.

4.2 DPPCE

A Coordenação-Geral de Auditoria da Área de Pessoal e Benefícios e de Tomada de Contas Especial (DPPCE) é resultante da união da Coordenação-Geral de Auditoria da Área de Pessoal (DPPES) e da Coordenação-Geral de Auditoria de Tomada de Contas Especial (DPTCE).

A criação dessas Unidades, em 2000, foi motivada pelas diversas normas do TCU que exigem o cumprimento de atribuições como: registro dos atos de aposentadorias, pensões e admissões e o envio de TCE.

Embora o Regimento Interno da Controladoria-Geral da União ainda não contemple a união das duas Unidades, as atribuições da DPPCE estão definidas em seus Artigos 37 e 38, destacando-se:

- Criar trilhas e indicadores de pessoal para subsidiar as ações de controle.
- Verificar a exatidão e suficiência dos dados relativos à admissão e desligamento de pessoal e concessão de aposentadorias e pensões na Administração direta, autárquica e fundacional, e emitir parecer sobre tais atos.
- Orientar as unidades de controle interno sobre o exame da regularidade dos dados relativos à folha de pagamento de pessoal e benefício de servidores públicos;
- Orientar as unidades de controle interno no planejamento e execução de auditorias nos programas e ações destinados a pagamento de pessoal e benefícios de servidores públicos;
- Examinar e controlar os processos de tomadas de contas especiais e emitir os respectivos relatórios e certificados de auditoria;
- Acompanhar o julgamento das tomadas de contas especiais e tornar disponíveis os registros das ações realizadas, para fins de acompanhamento de resultados da CGU;
- Propor normas técnicas e procedimentos relativos às ações de controle na área de Pessoal, benefícios e TCE para fins de implementação pela DCTEQ;
- Propor a realização de atividades de treinamento, com o respectivo conteúdo programático, relativas às ações de controle na área de pessoal, benefícios e TCE para implementação pela DCTEQ;
- Propor a edição de manuais pertinentes à área de pessoal, benefícios e TCE, e mantê-los Atualizados.

As ações de controle acerca dos temas de pessoal e TCE são executadas predominantemente pela Unidade e complementarmente por outras Coordenações e pelas Controladorias-Regionais.

De acordo com o Coordenador, a criação da Unidade voltada para as ações de controle do tema em questão proporcionou diversos benefícios, tais como: melhor orientação para as unidades, roteirização, manualização, treinamento e concentração de técnicos.

4.3 Assessoria de Obras da DI

Diferentemente das duas Unidades tratadas anteriormente, a Assessoria de Obras da Diretoria de Auditoria da Área de Infra-Estrutura (DI) não se trata de uma Coordenação, mas sim de uma Unidade de assessoramento da Diretoria. Ela foi informalmente criada em outubro de 2008, como resultado da percepção, por parte do Diretor da área, da necessidade de uma Unidade de apoio técnico para a realização de auditorias de obras.

Assim, surgiu a Assessoria com as atribuições de capacitar e orientar tecnicamente as demais Unidades da SFC e as Controladorias-Regionais da CGU na realização de auditorias de obras, além de padronizar entendimentos e procedimentos do assunto. A ideia da Assessoria é servir de apoio técnico às demais Unidades, realizando ações de controle apenas em casos excepcionais.

A despeito da sua criação recente, a Assessoria já apresenta como resultado os seguintes benefícios:

1. Diagnóstico dos diferentes entendimentos das unidades da CGU nas ações de controle de Obras.

2. Uniformização e consolidação de conceitos e opiniões sobre controle de obras, por meio da geração de Notas técnicas.

3. Preparação de material para capacitação dos analistas/técnicos da SFC e das Controladorias-Regionais em auditoria de obras.

4. Início da padronização e validação dos procedimentos e entendimentos de Auditoria de Obras.

Apesar dos benefícios já percebidos com a criação da Assessoria, a área ainda não foi formalizada pela Alta Administração do Órgão, não constando do Regimento Interno da CGU e, em decorrência disso e da baixa comunicação entre as Coordenações de Diretorias distintas, ainda não se presta formalmente a dar apoio técnico a outras Coordenações da SFC fora da DI.

4.4 ODP

Diante da percepção da importância da utilização da informação, por meio da Portaria nº 1215, de 25 de junho de 2009, foi criado o Observatório da Despesa Pública (ODP) da Controladoria-Geral da União, Unidade de operação permanente, ligada hierarquicamente ao Gabinete do Ministro e operacionalmente à Diretoria de Informações Estratégicas (SPCI/DIE), com os seguintes objetivos (Artigo 1º):

I - antecipar situações críticas para encaminhamento preventivo de soluções;

II - construir cenários que subsidiem estrategicamente as atividades cotidianas;

III - fornecer informação útil para identificação de focos pontuais para o processo de controle;

IV - possibilitar a produção imediata de conhecimentos para demandas específicas; e

V - potencializar a velocidade e a precisão nas tomadas de decisões estratégicas.

O desenvolvimento dos trabalhos técnicos ocorre por meio do levantamento de dados e geração de informação de interesse relacionada ao tema em foco por meio da utilização de soluções de tecnologia da informação. Em seguida, a informação gerada é transferida às unidades técnicas da CGU para a análise de pertinência e posterior devolução das confirmações para realimentação do ciclo de produção de informações até sua síntese final.

Dessa forma, de acordo com o Artigo 3º da Portaria supra, o ODP deverá produzir os seguintes resultados técnicos:

I - o monitoramento de temas por quadros de indicadores, como um insumo gerencial à disposição dos dirigentes da CGU;

II - a produção de material preditivo, com o uso de técnicas de mineração de textos e dados, recursos de inteligência artificial e integração de bases de dados para possibilitar a antecipação de fatos e o encaminhamento de soluções; e

III - a organização de aglomerados de informações para que os dirigentes da CGU tenham conhecimento útil e oportuno à disposição para tomada de decisão.

4.5 Considerações sobre as Unidades temáticas

As entrevistas com os Coordenadores das Unidades temáticas se mostraram de fundamental importância para que se conheça e analise as situações que levaram a essa organização funcional diferente das demais Coordenações da SFC.

Comparando-se as três Unidades temáticas da SFC, observa-se que as características da Auditoria de TI se aproximam muito mais das necessidades que motivaram a criação da Assessoria de Obras, por envolverem tipos de auditorias que, embora não demandadas por legislação, necessitam de conhecimentos mais específicos e técnicos dos temas para a realização de ações de controle.

Assim como está sendo realizado na Assessoria de Obras, é necessário que haja um núcleo técnico na SFC para centralizar o conhecimento de Auditoria de TI; capacitar servidores das Coordenações da SFC e das Controladorias-Regionais da CGU; padronizar metodologias,

entendimentos e procedimentos; servir de apoio técnico para as demais áreas; e uniformizar recomendações. Além disso, diferente de como ocorre na Assessoria de Obras, uma Unidade de Auditoria de TI também teria a necessidade de realizar ações de controle mais complexas ou que envolvam várias áreas da Administração Pública.

O ODP, apesar de ainda se encontrar em processo de estruturação, é um exemplo de Unidade uma visão mais moderna, que valoriza a informação e utiliza-se fortemente da comunicação entre as diversas áreas da CGU. O aumento da comunicação eficiente entre as áreas fortalece o funcionamento da CGU como um Órgão único, agrega qualidade às ações de controle e diminui o retrabalho. O ODP é, ainda, uma fonte de informações importante para uma Unidade de Auditoria de TI.

Todavia, nenhuma das posições organizacionais ocupadas pelas Unidades temáticas já existentes na SFC atenderia as necessidades de uma Unidade de Auditoria de TI. As três Unidades da SFC encontram-se ligadas à estrutura de alguma Diretoria já existente. Todavia, no caso da Assessoria de Obras da DI e da DPPCE, os trabalhos ficam restritos às suas Diretorias, havendo pouca ou nenhuma interação com Coordenações de outras Diretorias, diminuindo o alcance dos trabalhos de apoio técnico e capacitação. Já a DCREX, apesar de possuir alto grau de comunicação com as demais Diretorias, está ligada a uma Diretoria de atividades de planejamento e coordenação que, em regra, oferece apoio técnico, mas não executa ações de controle.

5 PROPOSTA

Para tentar minimizar as dificuldades de realização de Auditoria de TI detectadas no Capítulo 3 e com base nas forças e fraquezas detectadas nas Unidades temáticas já existentes na SFC, será proposto um modelo de Unidade de Auditoria de TI dentro da SFC, baseado no conceito de escritório de projetos.

5.1 Fundamentos do Modelo

Por meio da utilização das técnicas de Gerência de Projetos, é possível tornar ordenadas e controláveis atividades geralmente realizadas de forma desordenada e pontual (*ad hoc*). Agregando, assim, valor à organização e às atividades realizadas por ela.

O modelo apresentado é baseado nos conceitos do *Project Management Body of Knowledge* - PMBOK (2008), que é um conjunto de conhecimentos em gestão de projetos amplamente reconhecidos como boas práticas, elaborado pelo *Project Management Institute* (PMI). Não se trata de uma metodologia, mas de uma visão geral sobre a correta aplicação de habilidades, ferramentas e técnicas que pode aumentar a chance de sucesso dos projetos.

Devido à diversidade das áreas de Auditoria de TI, às peculiaridades de cada ambiente auditado, à vasta possibilidade de definição de escopos e à delimitação de tempo para realização, cada auditoria pode ser tratada como um projeto.

De acordo com a Associação Brasileira de Normas Técnicas (ABNT), na norma NBR 10006 (ABNT, 2000), Projeto é "processo único consistindo de um grupo de atividades coordenadas e controladas com datas para início e término, empreendido para alcance de um objetivo conforme requisitos específicos, incluindo limitações de tempo, custo e recursos". Na mesma linha, segundo o PMBOK (PMI, 2008), "Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo.".

Temporário significa que todos os projetos possuem um início e um final definidos. Toda auditoria é delimitada no tempo.

Um projeto cria entregas exclusivas, que são produtos, serviços ou resultados. Uma auditoria produz resultados finais em forma de documentos, como pareceres, recomendações e relatórios.

A exclusividade ou singularidade é uma característica importante das entregas do projeto. Por exemplo, muitas auditorias podem ser realizadas, mas cada uma possui um escopo específico, uma equipe diferente, procedimentos específicos voltados para o escopo, tempo de execução diferentes, entre outras particularidades. A presença de elementos repetitivos não muda a

singularidade da auditoria. Neste contexto, ao se analisar a Auditoria de TI no âmbito de um Órgão de controle governamental, devido à variedade de áreas e extensão de assuntos a serem abordados, percebe-se que cada auditoria, regra geral, será única, com seus requisitos e limitações específicos.

Diante disto, tratar a Auditoria de TI como um projeto é possibilitar que se apliquem a ela as técnicas de Gerenciamento de Projeto conhecidas e mais aceitas no mercado nacional e internacional, aumentando-se a qualidades dos produtos e diminuindo-se os riscos de fracasso das ações de controle. Nesse contexto, cada ação de controle de Auditoria de TI poderá ser considerada um projeto.

Dessa forma, este trabalho propõe a criação de um escritório de projetos de Auditoria de TI no âmbito da SFC.

De acordo com o PMBOK 2008, "um escritório de projetos (*Project Management Office* - PMO) é um corpo ou Entidade organizacional à qual são atribuídas várias responsabilidades relacionadas ao gerenciamento centralizado e coordenado dos projetos sob seu domínio." Ainda de acordo com a literatura em questão, "as responsabilidades de um PMO podem variar desde fornecer funções de suporte ao gerenciamento de projetos até ser responsável pelo gerenciamento direto de um projeto."

O PMO se concentra no planejamento, na priorização e na execução coordenados de projetos e subprojetos vinculados aos objetivos gerais de negócios. Além disso, ele pode centralizar as lições aprendidas e metodologias utilizadas nos projetos, de forma a permitir acesso a esse conhecimento a todas as equipes e projetos de auditoria; gerenciar recursos compartilhados entre todos os projetos administrados; orientar, treinar e supervisionar projetos; desenvolver e gerenciar políticas, procedimentos, formulários e outras documentações compartilhadas do projeto; e coordenar as comunicações entre projetos.

Portanto, o escritório de projetos seria uma Unidade onde os projetos de Auditoria de TI poderiam ser centralizados e coordenados de forma a melhor distribuí-los dentro da organização, possibilitando que as iniciativas de auditoria deixem de ser predominantemente *ad hoc* e possam ser padronizadas e bem gerenciadas de acordo com padrões e técnicas selecionados pelo próprio escritório, de forma a criar uma metodologia documentada e homologada dentro da organização.

Além disso, a existência dessa unidade possibilita a melhoria contínua do processo, uma vez que pode centralizar o aprendizado e os problemas resultantes de cada projeto, utilizando-os para corrigir fragilidade da metodologia e adaptá-la a mudanças que possam ocorrer em padrões e modelos a embasam.

Assim, os projetos de auditoria poderiam ser mais bem programados e coordenados, o conhecimento adquirido nas auditorias não se perderia em Coordenações isoladas e a padronização de diretrizes e linguagem dentro do Órgão de controle seria viabilizada.

Portanto, propõe-se nesse trabalho a criação de um escritório de projetos de Auditoria de TI com denominação de Coordenação-Geral de Auditoria de Tecnologia da Informação (GSTIN), seguindo o padrão de nomenclatura da Secretaria Federal de Controle.

5.2 Estrutura da GSTIN

Inicialmente, a Coordenação-Geral de Auditoria de Tecnologia da Informação (GSTIN), com o *status* de Coordenação da SFC, devido ao fato de não haver Diretoria com ações de controle voltadas a temas, estaria diretamente ligada ao Secretário Federal de Controle Interno, na forma mostrada na Figura 5.1.

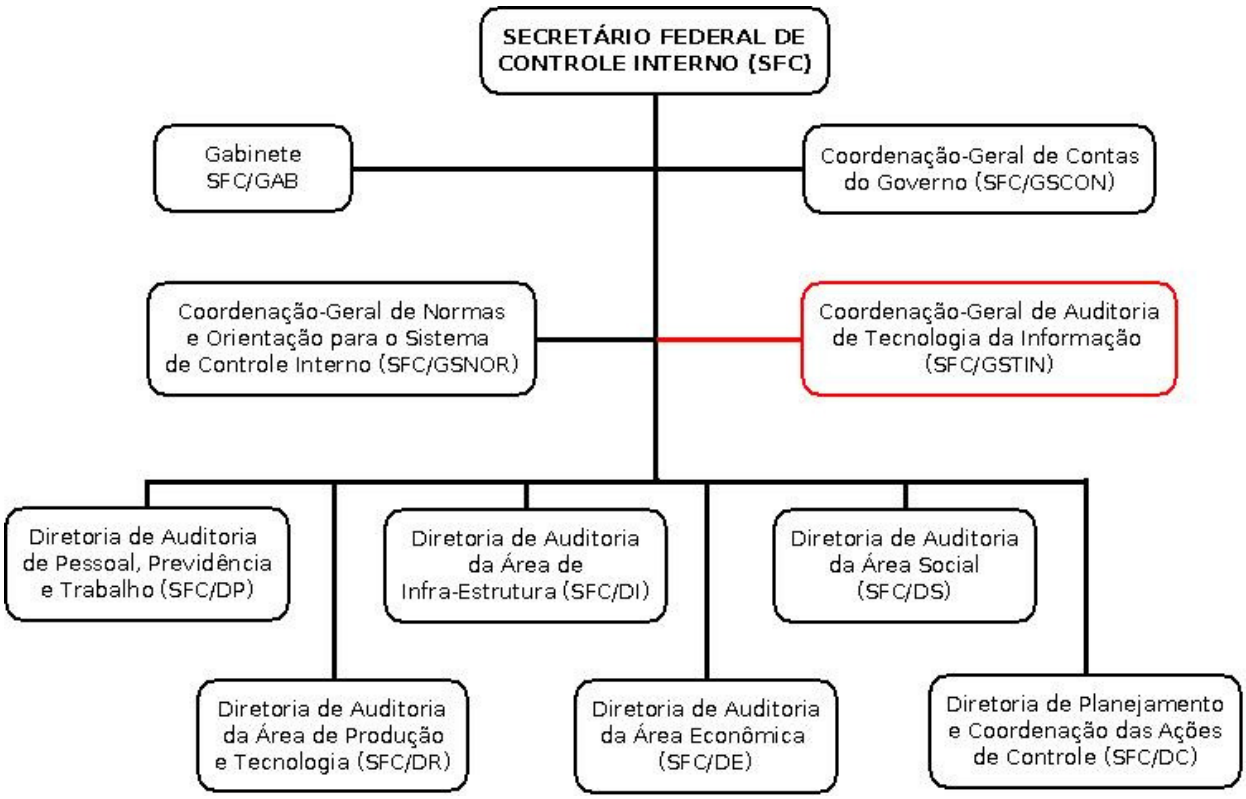


Figura 5.1 – Organograma da SFC com a inserção da GSTIN.

Futuramente, com a criação de outras coordenações baseadas em temas, tais como Obras e Convênios, poderia ser criada uma Diretoria temática, à qual a GSTIN estaria subordinada. Tal

Diretoria teria a mesma estrutura organizacional das demais da SFC, com a diferença de que suas Coordenações seriam organizadas com base nos temas que tratariam e não divididas por Ministério.

Como forma de atuação inicial, propõe-se a criação da Coordenação nos seguintes moldes:

- 1 Coordenador-Geral;
- 1 Assistente Técnico; e
- 5 Chefes de Divisão.

Cada Divisão forma uma equipe de projeto, em que o Chefe de Divisão teria o papel de Gerente de Projetos, conforme Figura 5.2 a seguir apresentada:

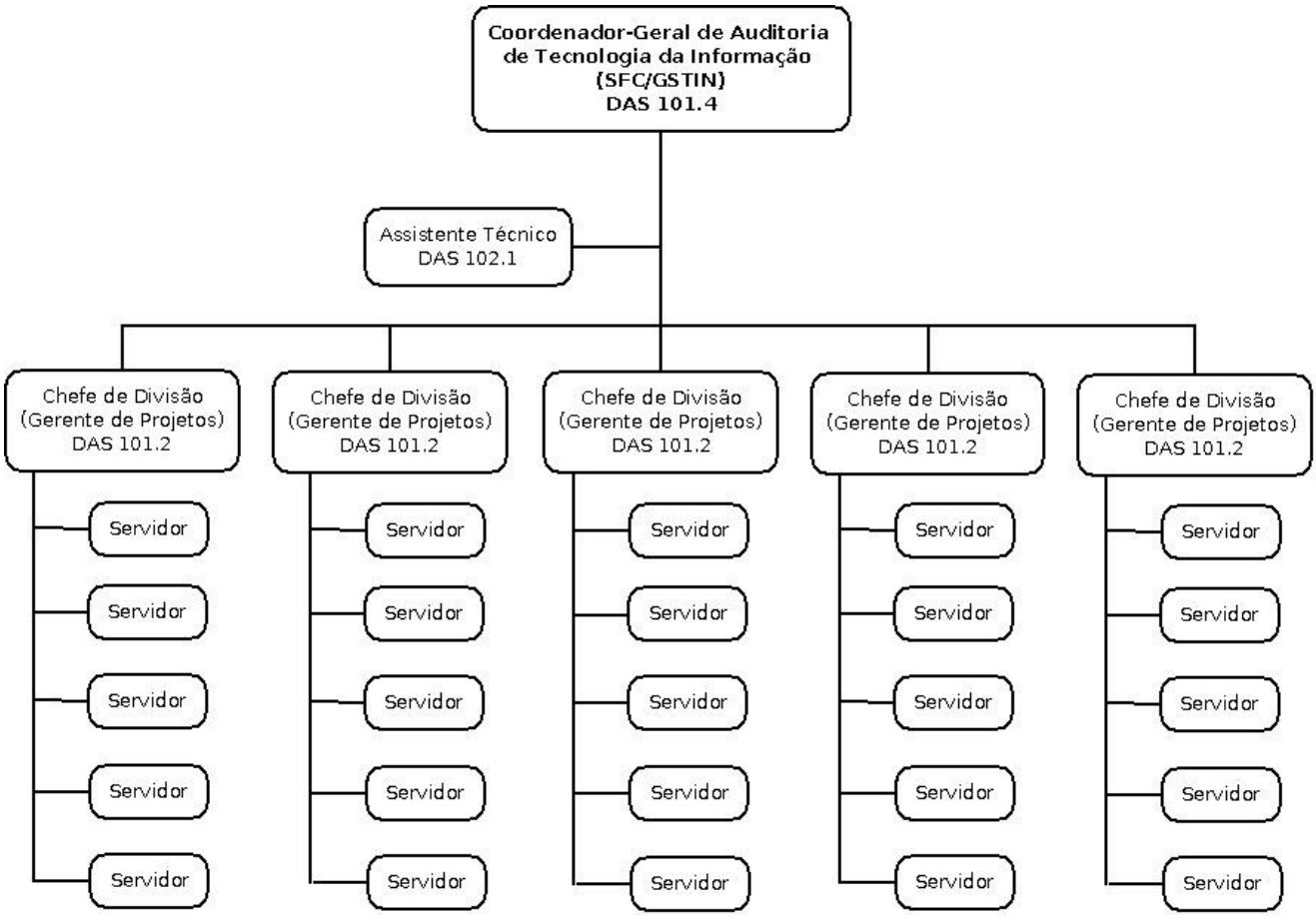


Figura 5.2 – Estrutura da GSTIN.

O modelo apresenta 5 Divisões, pois cada Equipe de Projeto atuaria com contraparte de uma Diretoria da SFC, de forma a se estabelecer 5 canais de comunicação. Cada Equipe seria responsável pelo gerenciamento, comunicação e apoio técnico das Coordenações de sua Diretoria contraparte.

Cada Divisão teria 5 servidores compondo a Equipe de Projeto. Essa configuração poderia ser remanejada caso houvesse a percepção, após estudos técnicos e realização de auditorias, de que determinada Diretoria demandasse mais força de trabalho do que as outras. O remanejamento temporário de servidores dentro da GSTIN também seria possível para composição de equipes de projetos de acordo com o mapeamento de perfis mais indicados para cada projeto.

Por fim, as Unidades finalísticas deveriam continuar dispondo de servidores de TI para a realização de trabalhos de Auditoria de TI que necessitem apenas de orientação e/ou apoio técnico da GSTIN.

5.3 Atribuições da GSTIN

O Coordenador-Geral da GSTIN, sem prejuízo das demais atribuições inerentes ao cargo, teria como funções principais: planejar e coordenar as atividades técnicas e administrativas desenvolvidas na Coordenação; aprovar os relatórios de auditoria e de fiscalização na sua área de competência; identificar as necessidades e propor treinamentos e capacitação de seus servidores; e praticar os atos de administração da Coordenação-Geral.

A Coordenação atuaria nos Ministérios e respectivas Entidades supervisionadas, exceto no Ministério das Relações Exteriores, no Ministério da Defesa, na Advocacia-Geral da União e nos Órgãos da Presidência da República, pois são escopo de suas Secretarias de Controle Interno (CISET), como consta no Decreto n.º 3.591, de 6 de dezembro de 2000, que dispõe sobre o Sistema de Controle Interno do Poder Executivo Federal. Cabe ressaltar que a Advocacia-Geral da União ainda não possui sua CISET, mas o Órgão já possui um projeto para sua criação que está em trâmite por meio do Processo n° 00400.016613/2009-01.

Para definição das atribuições da GSTIN, foi realizado um estudo do Regimento Interno da CGU (BRASIL, 2007a) e das competências da Sefti (BRASIL, 2008c), tendo como resultado as atribuições apresentadas a seguir:

a) Elaborar o planejamento das ações de controle que envolvam a área de Tecnologia da Informação a serem executadas ou coordenadas pela própria Coordenação.
b) Elaborar os pedidos de ações de controle, que posteriormente serão convertidos em ordens de serviço, contendo a definição dos trabalhos, em forma, período e escopo.
c) Coordenar, acompanhar e monitorar as ações de auditoria e fiscalização específicas da área de Tecnologia da Informação executadas por outras Coordenações-Gerais ou Controladorias-Regionais.

d) Executar ações de controle que envolvam objetos de Tecnologia da Informação selecionados por sua média/alta materialidade, criticidade e/ou relevância; por não serem alcançados pelas demais Coordenações-Gerais ou Controladorias-Regionais; ou, ainda, por exigirem auditorias operacionais com alta especificidade técnica.
e) Recomendar, quando for o caso, a instauração de tomadas de contas especiais, de sindicâncias e de processos administrativos e disciplinares.
f) Coordenar o processo de alocação da força de trabalho, quando necessário, junto às unidades de controle interno para a execução de ações de controle específicas da área de Tecnologia da Informação.
g) Acompanhar a implementação das recomendações decorrentes das ações de controle da respectiva área de atuação.
h) Apurar, em articulação com a CRG e com a SPCI, os atos ou fatos inquinados de ilegalidade ou irregularidade, praticados por agentes públicos ou privados, na utilização de recursos públicos federais nos assuntos referentes à Tecnologia da Informação.
i) Manter comunicação constante com troca de informações estratégicas com o Observatório de Despesas Públicas com o objetivo de utilizar os produtos dessa Unidade para possibilitar o adiantamento das ações de controle e, em contrapartida, mantê-la atualizada sobre informações acerca dos Sistemas de Informação da Administração Pública Federal.
j) Manter comunicação constante com a DSI com o objetivo programar cursos técnicos de capacitação e manter atualizados informações referentes à gestão de TI.
k) Propor a realização de atividades de treinamento, com o respectivo conteúdo programático, relativas às ações de controle da área de Tecnologia da Informação, para implementação em conjunto com a DCTEQ, em consonância com a política de desenvolvimento de recursos humanos da CGU.
l) Elaborar normas técnicas e procedimentos relativos às ações de controle da área de Tecnologia da Informação em conjunto com a DCTEQ.
m) Propor a edição de manuais pertinentes às ações de controle da área de Tecnologia da Informação, e mantê-los atualizados.
n) Exercer outras atividades correlatas.

5.4 Auditoria de Conformidade x Auditoria de Operacional

O termo Auditoria pode ser entendido como a aplicação de um conjunto de metodologias, procedimentos, técnicas e métodos de revisão, avaliação, aferição e análise com a finalidade de obtenção de informação ou conhecimento acerca da regularidade ou dos resultados das finanças, atividades, projetos, programas, políticas e Órgãos governamentais (TCU, 2004).

Para efeitos desse trabalho, de acordo com seu foco e escopo, uma auditoria pode ser classificada como de Conformidade ou Operacional.

A Auditoria de Conformidade consiste na verificação da obediência a normas e a regulamentos internos ou externos, além da verificação da salvaguarda de ativos a fim de impedir fraudes e desvios de recursos.

A Auditoria Operacional consiste na avaliação sistemática dos programas, projetos, atividades e sistemas governamentais, assim como dos Órgãos e Entidades da Administração Pública. Esse tipo de auditoria abrange duas modalidades: a auditoria de desempenho operacional, também conhecida como *performance audit*, e a avaliação de programa.

De acordo com TCU (2000), o objetivo da auditoria de desempenho operacional é examinar a ação governamental quanto aos aspectos da economicidade, eficiência e eficácia, enquanto a avaliação de programa busca examinar a efetividade dos programas e projetos governamentais.

Entretanto, na prática, não existem limites definidos entre os dois tipos de auditoria, uma vez que uma auditoria operacional pode apresentar verificações de conformidade e vice-versa. Assim, na realidade, existem as auditorias predominantemente de conformidade, em que o foco é a aderência à Normas, e aquelas que são predominantemente operacionais, em que o foco é a verificação dos resultados.

No caso do modelo proposto, a GSTIN seria prioritariamente responsável pela realização de Auditorias de TI predominantemente operacionais, enquanto as Coordenações finalísticas ficariam responsáveis pelas Auditorias de TI predominantemente de Conformidade. Isso porque as auditorias operacionais, em geral, necessitam de conhecimento aprofundado das questões técnicas que envolvem o escopo escolhido. Mesmo que a Coordenação finalística possua um servidor de TI em seu corpo técnico, pela abrangência de áreas de conhecimento dentro do universo da Tecnologia da Informação, muitas vezes, esse servidor se depara com dificuldades de realizar uma ação de controle de TI de forma independente, sem algum apoio técnico.

Todavia, como ocorre com as demais Coordenações finalísticas, a GSTIN deve fazer o planejamento das auditorias a serem realizadas em um determinado período. Nesse momento, deve-

se analisar caso a caso para se definir quais ações de controle serão realizadas pela própria Coordenação e quais serão realizadas pelas Unidades finalísticas.

Dessa forma, pode acontecer de uma Unidade finalística ficar responsável pela realização de uma auditoria operacional de pequeno porte ou de a GSTIN ficar responsável por uma auditoria de conformidade de grande porte e que envolva a análise de mais de uma área da Administração Pública, englobando vários Ministérios.

5.5 Funcionamento Organizacional

Com a criação da GSTIN, é importante que seja analisada a nova estrutura organizacional da SFC, uma vez que se trata de um fator ambiental que pode interferir na disponibilidade de recursos e na maneira como os projetos serão conduzidos.

De acordo com o PMBOK (PMI, 2008), as estruturas organizacionais variam de funcionais a projetizadas, com diversas estruturas matriciais entre elas, com as características genericamente apresentadas na Tabela 5.1:

	Estrutura da Organização				
		Matricial			
Características do Projeto	**Funcional**	**Fraca**	**Balanceada**	**Forte**	**Por Projeto**
Autoridade do gerente de projetos	Pouca ou nenhuma	Limitada	Baixa a moderada	Moderada a alta	Alta a quase total
Disponibilidade de recursos	Pouca ou nenhuma	Limitada	Baixa a moderada	Moderada a alta	Alta a quase total
Quem controla o orçamento do projeto	Gerente funcional	Gerente funcional	Misto	Gerente de projetos	Gerente de projetos
Função do gerente de projetos	Tempo parcial	Tempo parcial	Tempo integral	Tempo integral	Tempo integral
Equipe administrativa do gerenciamento de projetos	Tempo parcial	Tempo parcial	Tempo parcial	Tempo integral	Tempo integral

Tabela 5.1 – Influência das estruturas organizacionais nos projetos (Fonte: PMBOK).

Na CGU, atualmente, predomina a estrutura funcional clássica, salvo algumas exceções, como as operações especiais (ações de controle realizadas com coordenação da DCOPE[12], mas envolvendo servidores de diversas Coordenações-Gerais e Controladorias-Regionais).

[12] Coordenação-Geral de Operações Especiais.

Com a criação da GSTIN, a SFC seria uma organização mista, pois teria uma estrutura projetizada dentro da própria Coordenação, uma estrutura funcional clássica nas demais Unidades da Secretaria e uma estrutura Matricial Balanceada na relação da GSTIN com as demais Unidades finalísticas.

> A organização funcional clássica é uma hierarquia em que cada funcionário possui um superior bem definido. No nível superior, os funcionários são agrupados por especialidade, como produção, *marketing*, engenharia e contabilidade. As especialidades podem ser subdivididas em organizações funcionais, como engenharia mecânica e elétrica. Cada departamento em uma organização funcional fará o seu trabalho do projeto de modo independente dos outros departamentos. (PMI, 2008)

No caso da SFC, as Diretorias são divididas por temas de especialidade e os servidores são alocados em Coordenações-Gerais de acordo com os Ministérios nos quais exercerão ações de controle.

> Em uma organização projetizada, os membros da equipe são geralmente colocados juntos. A maior parte dos recursos da organização está envolvida no trabalho do projeto e os gerentes de projetos possuem grande independência e autoridade. As organizações projetizadas em geral possuem unidades organizacionais denominadas departamentos, mas esses grupos se reportam diretamente ao gerente de projetos ou oferecem serviços de suporte aos vários projetos. (PMI, 2008)

No caso da GSTIN, em relação aos trabalhos que envolvam apenas essa Coordenação, cada Chefe de Divisão será um Gerente de Projetos e cada Divisão será o equivalente a um departamento de projetos, que pode ser divido em uma ou mais equipes de auditoria, como já apresentado na Figura 5.2.

> As organizações matriciais são uma combinação de características das organizações funcionais e projetizadas. As matrizes fracas mantêm muitas das características de uma organização funcional e o papel de gerente de projetos é mais parecido com a de um coordenador ou facilitador do que com o de um gerente de projetos propriamente dito. As matrizes fortes possuem muitas das características da organização projetizada e podem ter gerentes de projetos em tempo integral com autoridade considerável e pessoal administrativo trabalhando para o projeto em tempos integral. Enquanto a organização matricial balanceada reconhece a necessidade de um gerente de projetos, ela não fornece a ele autoridade total sobre o projeto e sobre seu financiamento. (PMI, 2008)

A SFC possuirá uma estrutura matricial balanceada decorrente da atuação da GSTIN, pois ela poderá realizar auditorias apenas com os membros de seu quadro técnico ou em conjunto com servidores das Unidades finalísticas.

Quando os trabalhos forem mistos, qualquer integrante da GSTIN poderá ser gerente do projeto. Os trabalhos mistos podem envolver uma ou mais Coordenações da área fim, como mostram as situações 2 e 3 da Figura 5.3:

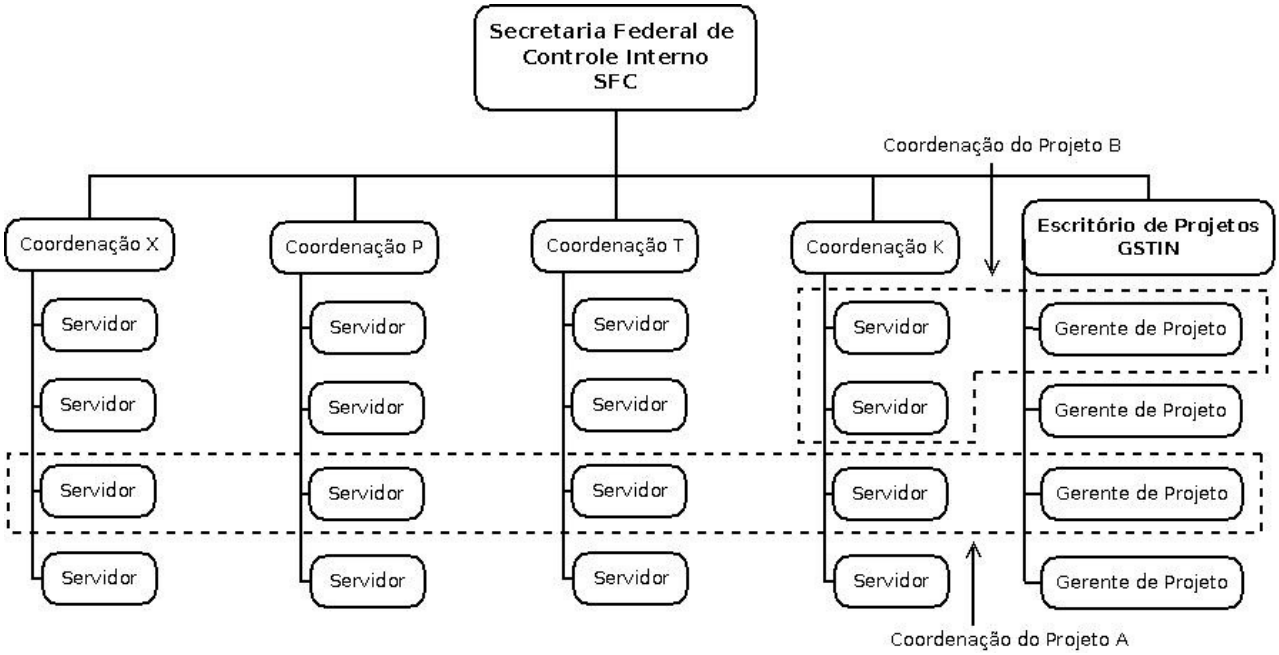


Figura 5.3 – Estrutura matricial balanceada da relação GSTIN x Unidades finalísticas.

Quando os trabalhos forem na Unidade finalística com apoio técnico da GSTIN, o gerente de projetos pertencerá à Coordenação demandante e, caso necessário, com apoio técnico de algum gerente de projeto do Escritório de Projetos de Auditoria de TI.

Cabe observar que a adoção de uma Coordenação Projetizada em uma estrutura tradicionalmente funcional, como a maioria dos órgãos públicos, é um grande desafio, que exigirá um planejamento bem elaborado e uma reeducação cultural na Instituição, a fim de que sejam evitados dificuldades de comunicação, deficiências na execução de projetos e choques de autoridade entre a hierarquia tradicional e os gerentes de projeto.

5.6 Papel do Gerente de Projetos

Na estrutura projetizada, a autoridade do gerente de projeto varia de alta a quase total, assim como sua disponibilidade de recursos. O gerente exerce seu papel e possui sua equipe disponível em tempo integral, como descrito na tabela Tabela 5.1.

Já na matriz balanceada, a autoridade do gerente de projeto varia de baixa a moderada, assim como sua disponibilidade de recursos. O gerente exerce seu papel em tempo integral, mas só possui a equipe disponível em tempo parcial, como descrito na tabela Tabela 5.1.

Dessa forma, no âmbito da GSTIN, o gerente de projetos teria um alto nível de autoridade, guardados os limites das competências da Coordenação, e equipe disponível em tempo integral do projeto. Todavia, quando gerenciasse equipes mistas, com servidores das Unidades finalísticas,

apesar de sua atuação como gerente ser de tempo integral, a abrangência de sua autoridade e a disponibilidade dos membros da equipe teriam que ser negociados juntamente com os Coordenadores das demais Unidades participantes.

De acordo com o PMBOK, o gerente de projetos é a pessoa designada pela organização executora para atingir os objetivos do projeto. Além de todas as habilidades da área específica e das proficiências ou competências de gerenciamento geral exigidas, o gerenciamento de projetos eficaz requer que o gerente tenha conhecimento sobre as técnicas de gerenciamento e tenha capacidade de aplicá-las, além de ter capacidade para liderar e orientar sua equipe, bem como atingir os objetivos do projeto e equilibrar as restrições existentes.

Dentre as competências que necessitam de grande atenção de um gerente de projeto estão a comunicação eficiente e a capacidade de lidar com os *stakeholders* ou partes interessadas.

> As partes interessadas são pessoas ou organizações (por exemplo, clientes, patrocinadores, organização executora ou o público) ativamente envolvidas no projeto ou cujos interesses podem ser **positiva ou negativamente** afetados pela execução ou término do projeto. Elas também podem exercer influência sobre o projeto, suas entregas e sobre os membros da equipe do projeto. (PMI, 2008)

No caso da GSTIN, vários atores podem ser considerados *stakeholders*, dos quais podem ser citados: os Coordenadores das Unidades finalísticas, os Órgãos e Entidades auditados, o Coordenador da GSTIN, o Secretário Federal de Controle Interno, empresas de informática, a sociedade, entre outros. Os interesses de todas essas organizações podem influenciar positiva ou negativamente os projetos de Auditoria de TI. Cabe ao gerente saber conduzir seus projetos de forma a diminuir os impactos negativos causados por essas partes interessadas e aproveitar ao máximo as influências positivas.

> A equipe de gerenciamento do projeto precisa identificar as partes interessadas, tanto internas quanto externas, a fim de determinar os requisitos e as expectativas em relação ao projeto de todas as partes envolvidas. Além disso, o gerente do projeto precisa gerenciar a influência das várias partes interessadas em relação aos requisitos do projeto para garantir um resultado bem sucedido. (PMI, 2008)

Para isso, o gerente de projetos precisa saber se comunicar, de forma a distribuir informações àqueles que tenham direito e/ou obrigação de acessá-las e de forma a agregar eficiência ao processo de gerenciamento. Uma boa comunicação junto à equipe de projeto (interna) e junto aos demais *stakeholders* (externa) são de extrema importância para o sucesso de um projeto.

5.7 Requisitos de Implantação

A implantação da GSTIN deve ser planejada e executada considerando-se também as técnicas de gerenciamento de projetos. Antes que seja criada por meio de um instrumento legal, seu processo de implantação já deve estar integralmente planejado.

Para a implantação da Coordenação, devem ser atendidos alguns requisitos:

a) **Projeto básico:** o projeto deve contemplar a estrutura organizacional da Coordenação, os recursos necessários e o planejamento contendo as etapas, as atividades e o cronograma de implantação.

b) **Concurso público:** realização de concurso para contratação de novos servidores com área de formação em Tecnologia da Informação. Tais servidores seriam alocados de forma a suprir as necessidades da DSI, atender Coordenações deficitárias em servidores de TI e compor o corpo técnico da GSTIN.

c) **Formação da equipe:** a seleção da equipe da GSTIN deve considerar as áreas de conhecimento dos servidores, a experiência em auditorias e as competências de gerenciamento de projetos. A equipe de servidores deve possuir servidores com especialidades nas mais diversas áreas da Tecnologia da Informação, mesclando novos servidores com experiência no mercado de TI da iniciativa privada e servidores da Casa com experiência em auditorias, licitações e contratos.

d) **Recursos tecnológicos:** a GSTIN deve ser provida de recursos tecnológicos suficientes para a realização de suas atividades. Por exemplo, para a realização de Auditorias de Dados, deve haver computadores com processamento adequado ao tamanho e complexidade das operações. Além disso, a Coordenação deve possuir ferramentas informatizadas de apoio às auditorias.

e) **Plano de comunicação:** deve ser elaborado um plano de comunicação entre a GSTIN e as demais Coordenações da SFC, o ODP, a CRG, SPCI e as Controladorias-Regionais, de forma a buscar uma comunicação eficiente entre as Unidades. Além disso, devem ser estabelecidas parcerias com outros Órgãos, como Banco Central, Banco do Brasil, Tribunal de Contas da União e Secretaria de Logística de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, a fim de conjuntamente melhorem as metodologias e técnicas de Auditoria de TI e fomentarem a Governança de TI, a Segurança da Informação e o fortalecimento dos controles internos de TI no âmbito da Administração Pública.

f) **Capacitação em gerenciamento de projetos:** a equipe da GSTIN deve ser treinada em boas práticas de gerenciamento de projetos, de forma a utilizarem esses conhecimentos nas auditorias e servirem de multiplicadores junto a outros servidores que terão atuação de gerentes de projetos de Auditoria de TI nas Unidades finalísticas e nas Controladorias-Regionais.

g) **Capacitação em licitações e contratos:** como praticamente toda a Tecnologia da Informação da Administração Pública envolve licitações e contratos, a equipe deve ser amplamente capacitada nessa área, com grande enfoque na Instrução Normativa nº 04/2008.

h) **Capacitação em Auditoria de TI:** a equipe deve ter um treinamento introdutório sobre os principais conceitos e técnicas de Auditoria de TI e sobre problemas reais já encontrados na Administração Pública.

i) **Capacitação técnica de TI:** a equipe deve ter treinamento de assuntos técnicos específicos da Tecnologia da Informação, de maneira a nivelar seus conhecimentos com os das Unidades Auditadas.

j) **Mapeamento técnico das necessidades de Auditoria de TI:** deve ser realizado um mapeamento técnico junto às Unidades finalísticas e os Ministérios para identificar e classificar a necessidade de Auditoria de TI de cada área e detectar os possíveis objetos de auditoria.

k) **Testes piloto de auditoria operacional:** o Coordenador-Geral da GSTIN deve escolher objetos para a realização de testes piloto de Auditoria de TI de natureza Operacional. Para a realização dos testes já devem ser utilizadas as boas práticas de gerenciamento de projetos e devem ser elaborados procedimentos específicos para os escopos das auditorias a serem realizadas.

l) **Testes piloto em conjunto com outras Coordenações:** devem ser realizados testes pilotos em conjunto com as Unidades finalísticas, de maneira a modelar a forma de comunicação e de atuação com as demais áreas envolvidas.

m) **Correções:** com os resultados do mapeamento e dos testes piloto, devem ser realizados ajustes e correções na estrutura da GSTIN e nos processos de trabalho.

n) **Planejamento dos trabalhos sistemáticos:** após a realização das correções necessárias, deve ser elaborado um planejamento dos trabalhos a serem realizados pela Coordenação. O planejamento deve estar alinhado com os objetivos estratégicos

da CGU e com o mapeamento técnico realizado das necessidades de Auditoria de TI na Administração Pública Federal, respeitados os limites de atuação da SFC.

o) **Apoio técnico:** elaboração de protocolo de fornecimento de apoio às Coordenações finalísticas e às Controladorias-Regionais. Devem ser estabelecidas as regras e as formas de realização de consultas técnicas pelas demais áreas.

p) **Fornecimento de treinamentos:** devem ser elaborados treinamentos para servidores das Unidades finalísticas e das Controladorias-Regionais para a realização de Auditorias de TI de complexidade baixa e média.

q) **Capacitação contínua:** devem ser promovidos cursos de capacitação contínua para os servidores da GSTIN de acordo com as necessidades detectadas com a realização dos trabalhos.

r) **Melhoria contínua:** a GSTIN deve possuir indicadores para medição de qualidade de suas metodologias e dos resultados de seus trabalhos com o objetivo de se detectar fragilidades e implementar soluções.

s) **Banco de práticas comuns da iniciativa privada:** deve ser criado (e atualizado constantemente) um banco de dados com informações sobre as práticas comuns da iniciativa privada na aquisição de bens e serviços de TI, tais como: formas de contratação mais usuais de determinado produtos, produtos exclusivos por sua funcionalidade ou qualidade técnica, cotação de preços de mercados dos produtos mais comercializados, empresas detentoras de produtos exclusivos que realizam vendas diretas, empresas que apenas realizam vendas por meio de parceiros, entre outras.

Além de todos os requisitos apresentados, a Auditoria de TI não deve ser implantada sem alinhamento com os objetivos de negócio da Instituição. Nesse caso, os conceitos de Governança também devem ser aplicados, de maneira que a atuação da GSTIN não seja independente da SFC como uma Coordenação isolada, mas que esteja alinhada aos objetivos estratégicos da CGU e das políticas governamentais.

6 CONCLUSÃO

A partir da verificação dos altos investimentos e da crescente dependência em Tecnologia da Informação no contexto da Administração Pública, observou-se a necessidade de fortalecimento da Auditoria de TI.

Todavia, observou-se que, na maioria dos Órgãos e Entidades da Administração Pública, as ações de controle de Tecnologia da Informação são ainda incipientes. Por isso, com o objetivo de se verificar a percepção dos servidores sobre a necessidade e a situação desse tipo de Auditoria, realizou-se um Diagnóstico de Auditoria de TI no âmbito da SFC.

A partir daí, constatou-se que a maioria dos servidores de TI e dos Coordenadores-Gerais das Unidades finalísticas da SFC consideram a necessidade de Auditoria de TI alta dentro do escopo de suas áreas de atuação, bem como declararam que o nível de maturidade dos processos de Auditoria de TI ainda é Inicial, ou seja, não há um processo padronizado e a execução das ações de controle de TI é feita caso a caso e baseada apenas nos processos genéricos de auditoria da Secretaria Federal de Controle.

Ademais, foram também detectadas, dentre outras fragilidades, o subaproveitamento dos servidores de TI nas ações de controle de TI; a falta de capacitação nessa área de atuação; a ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI; e a inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC.

A fim de buscar solucionar tais questões, foi proposta a criação de um escritório de projetos de Auditoria de TI para a SFC, a Coordenação-Geral de Auditoria de TI (GSTIN). Essa Coordenação teria como principais funções a execução de ações de controle de TI, o gerenciamento de auditorias de TI realizadas em conjunto com outras Coordenações, a centralização de conhecimento nesse tipo de ação de controle, a capacitação dos servidores de TI e o apoio técnico a outras unidades na realização de Auditorias de TI. Sua forma de atuação seria orientada pelas melhores práticas de gerenciamento de projetos, de forma a agregar eficiência e eficácia às auditorias realizadas.

Com isso, criar-se-iam condições para que se elevasse o nível de maturidade da Auditoria de TI no âmbito da SFC, aumentasse a capacidade técnica nesse tipo de ação de controle, realizasse um melhor aproveitamento do conhecimento dos servidores de TI, padronizasse uma linguagem de Auditoria de TI para a SFC, elevasse a qualidade dos trabalhos, expandisse a capacidade de atuação da SFC nesse tipo de auditoria, executassem ações de controle em áreas em que a SFC ainda não teve capacidade técnica e operacional de atuação.

Ademais, os impactos das exonerações, vacâncias, remoções e permutas poderiam ser diminuídos se houvesse a concentração formal do conhecimento em um núcleo técnico de Auditoria de TI, diminuindo o foco no indivíduo e fortalecendo a Instituição.

Além desses benefícios primários, são conseqüências secundárias da implementação do modelo proposto: a identificação de problemas crônicos de Tecnologia da Informação na Administração Pública, o fortalecimento da Governança e da Segurança de TI nas Unidades auditadas, identificação de problemas crônicos de Tecnologia da Informação na Administração Pública, o incentivo à produção de normas específicas que regulem a TI dentro da APF e, por fim, o fortalecimento da comunicação com outros órgãos de controle na área de TI.

A pesquisa também possibilitou a percepção da aprovação, por parte dos Coordenadores-Gerais e servidores de TI, de que é necessário o investimento da CGU no fortalecimento desse tipo de auditoria dentro da SFC por meio da criação de um núcleo técnico. O apoio desses agentes também é de fundamental importância para que a proposta alcance o êxito desejado. Dessa forma, a implementação do modelo não seria uma imposição da Alta Administração, mas o resultado da detecção de uma necessidade real por parte da maioria dos futuros clientes da nova Coordenação dentro da SFC.

Portanto, este trabalho alcançou seus objetivos iniciais de se fazer um diagnóstico da Auditoria de TI dentro da SFC e de se apresentar uma proposta de modelo para implementação de Auditoria de TI no âmbito da CGU.

O alcance dos objetivos secundários só poderá ser efetivamente verificado a partir dos desdobramentos futuros, pois é conseqüência do fortalecimento da discussão dos problemas apresentados e das soluções propostas sobre Auditoria de TI e de outras auditorias especializadas no âmbito da SFC.

Durante a realização dessa pesquisa, foram verificadas as seguintes **dificuldades e limitações**:

a) Ausência de previsão específica para liberação dos servidores em horário de expediente para elaboração da monografia e realização de pesquisas. Essa liberação não necessitaria ser em tempo integral, pois a liberação parcial já agregaria qualidade ao trabalho e à pesquisa.
b) Inexistência de lista oficial dos servidores que atuam na SFC e que entraram na carreira de Analista de Finanças e Controle em vagas específicas de TI ou que

tenham conhecimento técnico sobre o assunto. Tal fato ensejou o levantamento de uma lista não oficial que, além do gasto de tempo para sua realização, está sujeita ao risco de estar incompleta, mesmo com a realização de circularização.

c) Dificuldade de agendamento de entrevistas com os Coordenadores-Gerais devido à quantidade de compromissos inerentes aos seus cargos, fato que ocasionou a prorrogação de prazo inicialmente previsto para a realização da pesquisa.
d) Dificuldade de levantamento das informações sobre o histórico da Auditoria de TI dentro da CGU. Os dados levantados referem-se ao período de 2004 a novembro de 2009, uma vez que não foram encontradas informações sobre anos anteriores. Além disso, as informações disponíveis estão pulverizadas e altamente vinculadas ao conhecimento individual de alguns servidores.

Por fim, com objetivo de dar continuidade a essa pesquisa, como **trabalhos futuros**, sugerem-se:

a) A realização de um mapeamento técnico, junto aos Órgãos e Entidades da Administração Pública dos possíveis objetos de Auditoria de TI, com a finalidade de se identificarem os trabalhos que possam ser escopo das ações de controle.
b) A elaboração de metodologia de Auditoria de TI baseada nas melhores práticas de Gerenciamento de Projetos.
c) A elaboração de novos procedimentos de Auditoria de TI e a atualização daqueles já existentes com base nos critérios mais aceitos e na legislação brasileira. Tal processo é iterativo e deve sofrer melhoria contínua.

7 REFERÊNCIAS

ANTUNES, V.A.; BARCARO, E.; HANASHIRO, M.; REIS, R.V. dos; ROCHA, A. L. M da. Perspectivas para a auditoria de tecnologia da informação no âmbito da CGU. *Revista da CGU*, Brasília, Ano II, n° 2, p. 62-69, out. 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ABNT. *NBR 10006: Gestão da qualidade – diretrizes para a qualidade no gerenciamento de projetos.* Rio de Janeiro, dez. 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ABNT. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de Prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ABNT. *NBR ISO/IEC 27001:2006*: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006.

BORBA, Edward Lúcio Vieira. *A Estratégia de Implantação de uma Unidade Especializa em Auditoria de TI (Estudo de caso da SEFTI/TCU).* Monografia de Pós-Graduação, Faculdade Omini, Brasília, 2008.

BRASIL. Lei nº 8.666, de 21 de junho de 1993. *Sítio oficial da Presidência da República.* Disponível em <http://www.planalto.gov.br/legislacao>. Acesso em 24 nov. 2009.

BRASIL. Decreto n.º 3.591, de 6 de dezembro de 2000. *Sítio oficial da Presidência da República.* Disponível em <http://www.planalto.gov.br/legislacao>. Acesso em: 06 ago. 2009.

BRASIL. Decreto n° 4.177, de 28 de março de 2002. *Sítio oficial da Presidência da República.* Disponível em <http://www.planalto.gov.br/legislacao>. Acesso em: 06 ago. 2009.

BRASIL. Decreto n° 10.520, de 17 de julho de 2002. *Sítio oficial da Presidência da República.* Disponível em <http://www.planalto.gov.br/legislacao>. Acesso em: 22 ago. 2000.

BRASIL. Decreto n° 5.683, de 24 de janeiro de 2006. *Sítio oficial da Presidência da República.* Disponível em <http://www.planalto.gov.br/legislacao>. Acesso em: 06 ago. 2009.

BRASIL. Tribunal de Contas da União. Resolução nº 199, de 28 de dezembro de 2006. Disponível em <http://portal2.tcu.gov.br/portal/page/portal/TCU/isc/legislacao_isc/RES2006_199.pdf>. Acesso em: 29 nov. 2009

BRASIL. Portaria n.º 570, de 11 de maio de 2007, aprova o Regimento Interno da Controladoria-Geral da União. *Controladoria-Geral da União*. Brasília, DF, 11 maio 2007.

BRASIL. Tribunal de Contas da União. Portaria nº 001, de 02 de abril de 2007. *Secretaria de Fiscalização de Tecnologia da Informação.* Brasília, 2007.

BRASIL. Instrução Normativa nº 04, de 19 de maio de 2008. *Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão*. Brasília, DF, 04 maio 2008.

BRASIL. Tribunal de Contas da União. Acórdão nº 1.603 - Plenário. 2008. *Levantamento do referencial estratégico da Secretaria de Fiscalização de Tecnologia da Informação (Sefti)*. Brasília, 2008.

BRASIL. Tribunal de Contas da União. Portaria Nº 003, de 25 de novembro de 2008. *Secretaria de Fiscalização de Tecnologia da Informação.* Brasília, 2008.

CONTROLADORIA-GERAL DA UNIÃO. *Histórico da CGU*. Disponível em <http://www.cgu.gov.br/CGU/Historico/index.asp>. Acesso em: 30 set. 2009.

GAO (1994). *Government auditing standards: 1994 revision*. Washington, 1994.

GOOGLE. *Google Docs*. Disponível em <http://www.docs.google.com>. Acesso em: 5 ago. 2009.

HANASHIRO, Maíra. 2007. *Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI aplicadas à Administração Pública Federal.* Dissertação de Mestrado - Universidade de Brasília, Brasília, 2007.

HANASHIRO, M. ; PUTTINI, R. S. Metodologia para Desenvolvimento de Procedimentos de Auditoria de Tecnologia da Informação Aplicada à Administração Pública Federal Brasileira. *Proceedings of 6th International Information and Telecommunication Technologies Symposium,* Brasília, 2007.

IT GOVERNANCE INSTITUTE. *COBIT 4.1*, Rolling Meadows, 2007.

OFFICE OF GOVERNMENT COMMERCE. *Informações Oficiais sobre o ITIL***.** Disponível em <http://www.itil-officialsite.com/home/home.asp>. Acesso em: 20 out. 2009.

PROJECT MANAGEMENT INSTITUTE. *A guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Quarta Edição, 2008.

ROCHA, Rogério Xavier. *Proposta de Procedimento Simplificado de Auditoria de Gestão em Segurança da Informação em Órgão do Poder Executivo Federal*. Monografia (Aperfeiçoamento/Especialização em Gestão da Segurança da Informação e Comunicações) – Universidade de Brasília. Brasília, 2008.

RODRIGUES, José Geraldo Loureiro. *Wiki-GOV: Governança de TI para o Setor Público*. <http://www.governanca.net> Acesso em: 23 nov. 2009.

SECRETARIA DO TESOURO NACIONAL. *Informações sobre o SIAFI.* Disponível em <http://www.tesouro.fazenda.gov.br/SIAFI>. Acesso em: 25 out. 2009.

SILVA, Carlos Alberto dos Santos. *Diretrizes para Auditoria do Processo de Contratação de Tecnologia da Informação na Administração Pública*. Dissertação de mestrado - Universidade Católica de Brasília, Brasília, 2008.

TRIBUNAL DE CONTAS DA UNIÃO. *Manual de Auditoria de Natureza Operacional* - TCU, Coordenadoria de Fiscalização e Controle. Brasília, 2000.

TRIBUNAL DE CONTAS DA UNIÃO. *Apostila do curso de TEORIA DA AUDITORIA*. Brasília, fev. de 2004.

TRIBUNAL DE CONTAS DA UNIÃO. *Relatório de Levantamento de Auditoria elaborado no âmbito da Secretaria de Auditoria de Tecnologia da Informação – SEFTI (Gastos em Tecnologia da Informação na Administração Pública Federal)*, TC nº 007.972/2007-8. Brasília, 2008.

TRIBUNAL DE CONTAS DA UNIÃO. Sumário Executivo: *Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal*, 2008. Disponível em <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/sumarios>. Acesso em: 17 out. 2009.

TRIBUNAL DE CONTAS DA UNIÃO. Sumário Executivo: *Levantamento do Referencial Estratégico da Secretaria de Fiscalização de Tecnologia da Informação*, 2008. Disponível em <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/sumarios>. Acesso em: 10 out. 2009.

TRIBUNAL DE CONTAS DA UNIÃO. Auditoria da Sefti alerta para situação preocupante da governança de TI. *Informativo do Tribunal de Contas da União*, ano XXIII, nº 152, 27 nov. 2008.

TRIBUNAL DE CONTAS DA UNIÃO. *Fiscalização de Tecnologia da Informação.* Disponível em <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao>. Acesso em: 13 ago. 2009.

APÊNDICE A – QUESTIONÁRIO PARA SERVIDORES DA SFC COM CONHECIMENTOS NA ÁREA DE TI

Prezados Colegas,

Esse questionário é parte da etapa de elaboração do meu Trabalho de Conclusão de Curso - TCC do curso de Especialização em Auditoria Interna e Controle Governamental, promovido conjuntamente pela Câmara dos Deputados, Advocacia-Geral da União, Controladoria-Geral da União e Tribunal de Contas da União. O tema desse TCC é "Proposta de Modelo de Implementação de Auditoria de Tecnologia da Informação - TI no âmbito da Controladoria-Geral da União". Os resultados advindos da aplicação desse questionário subsidiarão a motivação para a proposta a ser apresentada.

Para efeitos desse questionário, considerar Auditoria de TI como sendo toda ação de controle realizada pela Coordenação que tenha como objetivo avaliar os processos de compra e de fornecimento para infra-estrutura de TI, a integridade dos registros (dados), a segurança da informação, a prestação de serviços de informática, a aquisição de softwares, entre outros. Ressalta-se que a ação de controle não precisa ter uma Ordem de Serviço formal para ser considerada Auditoria de TI.

Os nomes dos colaboradores não serão divulgados.

Caso não visualize o questionário no corpo do e-mail, clique no *link* https://spreadsheets.google.com/viewform?formkey=dHJLdzZSZEZRMUJCelExR2ZvRXNmZnc6MA para responder ao questionário.

Solicito que respondam às questões aqui apresentadas até o dia 02/10/2009.

Desde já, agradeço pela colaboração e coloco-me à disposição para fornecer qualquer informação adicional.

Maíra Hanashiro
Analista de Finanças e Controle
CGU/SFC/DS/DSSAU
Ramal: 7307

Questionário

1 – Como pode ser classificada a necessidade de Auditoria de TI dentro do escopo da Coordenação?
* Para efeito de avaliação, considerar Auditoria de TI como sendo qualquer ação de controle dentro da Coordenação que envolva análise de um objeto de Tecnologia da Informação, independente de haver Ordem de Serviço formalizada.

( ) Muito Baixa
( ) Baixa.
( ) Média.
( ) Alta.
( ) Muito Alta.

2 - Selecione as opções que melhor retratam a frequência com que você realizou as atividades a seguir no último ano: *

	Nunca	Raramente	Eventualmente	Muitas vezes	Sempre
Auditoria Comum.	( )	( )	( )	( )	( )
Ações de controle com foco em TI.	( )	( )	( )	( )	( )
Trabalhos relacionados à informática, mas não à Auditoria.	( )	( )	( )	( )	( )

3 - Na sua Coordenação, existem trabalhos genéricos de Auditoria de TI? Exemplo: avaliação de um contrato de aquisição de softwares em uma Auditoria de Avaliação da Gestão.

( ) SIM
( ) NÃO

Caso a resposta seja SIM, citar o(s) exemplo(s) mais relevante(s):
_____
_____
_____

4 - Na sua Coordenação, já foram realizados trabalhos específicos de Auditoria de TI, em que o objeto de TI é o foco principal? Exemplo: análise de grandes bases de dados em busca de duplicidades, avaliação de algum sistema corporativo, entre outros.

( ) SIM
( ) NÃO

Caso a resposta seja SIM, citar o(s) exemplo(s) mais relevante(s), informando se houve ou não a emissão de Ordem de Serviço para as ações citadas. Caso a resposta seja NÃO, apresentar sua opinião sobre as razões pelas quais tais trabalhos não sejam realizados.
_____
_____
_____

5 - Classificar o nível de maturidade da Auditoria de TI dentro da Coordenação: Classificação adaptada com base nos níveis de maturidade do COBIT (Control Objectives for Information and related Technology).

( ) 0 – Inexistente. A Coordenação não reconhece a existência de um processo de Auditoria de TI.

( ) 1 – Inicial /*Ad-Hoc*. Há evidências de que a Coordenação reconhece que o processo de Auditoria de TI existe e que as necessidades devem ser mapeadas. Entretanto, não há um processo padronizado e a execução das ações de controle de TI é feita caso a caso e baseada apenas nos processos genéricos de auditoria da Secretaria Federal de Controle - SFC.

( ) 2 – Repetível, porém intuitivo. Os processos para a realização de Auditoria de TI são estruturados e procedimentos similares são seguidos por diferentes indivíduos para a mesma tarefa dentro da Coordenação. Há forte dependência do conhecimento individual e existe alguma documentação.

( ) 3 – Definido. Os processos de Auditoria de TI são padronizados, documentados e comunicados dentro da Coordenação. Entretanto, deixa-se a cargo dos indivíduos seguirem os processos. Não há certeza de que eventuais desvios serão detectados.

( ) 4 – Gerenciado. Existe a possibilidade de monitorar e medir a conformidade dos processos de Auditoria de TI com os procedimentos definidos dentro da própria Coordenação. Há ações para melhoria.

( ) 5 – Otimizado. Os processos foram refinados até alcançarem as melhores práticas, com base no resultado de melhoria contínua e comparações com outras organizações e coordenações.

6 - Quais as dificuldades enfrentadas para a realização de Auditorias de TI? Marcar todas as que se aplicarem ao caso da Coordenação, mas apenas quando a opção realmente consistir em um fator dificultador para a realização de ações de controle de TI.

( ) Tempo insuficiente para a realização dos trabalhos.
( ) Falta de apoio da alta administração.
( ) Falta de prioridade dentro da Coordenação.
( ) Falta de incentivo dentro da Coordenação.
( ) Deficiência na capacitação para esse tipo de auditoria.
( ) Deficiência nos procedimentos de Auditoria de TI.
( ) Deficiência de recursos tecnológicos.
( ) Ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI.
( ) Falta de apoio técnico sobre Auditoria de TI.
( ) Inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC.
( ) Outros: _____

7 - Citar potenciais objetos de Auditoria de TI que ainda não sofrem ação de controle ou sofrem ações incipientes e as razões pelas quais deveriam ser escopo de auditorias: Exemplos de razões: grande materialidade, criticidade e/ou relevância, entre outras. Se possível, dar detalhes sobre o contexto do objeto e sobre os recursos financeiros envolvidos.

_____
_____
_____

8 - No caso de existirem auditorias de TI na Coordenação, informar quais as referências bibliográficas, normas e bases legais utilizadas:

( ) COBIT.
( ) ITIL.
( ) LEI nº 8.666/93.
( ) NBR ISO/IEC 27002:2005 (NBR ISO/IEC 17799:2005).
( ) LEI nº 10.520/2002.
( ) Instrução Normativa nº 04/2008.
( ) Acórdãos do TCU.
( ) Outros: _____

9 - Citar ferramentas de auxílio na Auditoria de TI, caso sejam utilizadas.

_____
_____
_____

Observações Gerais

Se necessário, acrescentar informações adicionais acerca do assunto, de acordo com a realidade de sua Coordenação.

_____
_____
_____

Informações Básicas do Entrevistado

Nome Completo: _____

* Ressalta-se que os nomes dos colaboradores não serão divulgados em nenhum momento desse trabalho.

E-mail: _____

_
Cargo: _____

Ano de ingresso na carreira: _____

Coordenação: _____
* Usar a sigla. Por exemplo: DSSAU.

Formação Acadêmica: _____

APÊNDICE B – QUESTIONÁRIO PARA COORDENADORES-GERAIS DA SFC

Prezados Coordenadores,

Esse questionário é parte da etapa de elaboração do meu Trabalho de Conclusão de Curso - TCC do curso de Especialização em Auditoria Interna e Controle Governamental, promovido conjuntamente pela Câmara dos Deputados, Advocacia-Geral da União, Controladoria-Geral da União e Tribunal de Contas da União. O tema desse TCC é "Proposta de Modelo de Implementação de Auditoria de Tecnologia da Informação - TI no âmbito da Controladoria-Geral da União". Os resultados advindos da aplicação desse questionário subsidiarão a motivação para a proposta a ser apresentada. O questionário deve respondido, preferencialmente, por meio de entrevista a ser agendada de acordo com a disponibilidade de cada Coordenador. Caso não seja viável, solicito a gentileza de respondê-lo eletronicamente até o dia 02/10/2009.

Para efeitos desse questionário, considerar Auditoria de TI como sendo toda ação de controle realizada pela Coordenação que tenha como objetivo avaliar os processos de compra e de fornecimento para infra-estrutura de TI, a integridade dos registros (dados), a segurança da informação, a prestação de serviços de informática, a aquisição de softwares, entre outros. Ressalta-se que a ação de controle não precisa ter uma Ordem de Serviço formal para ser considerada Auditoria de TI.

Os nomes dos colaboradores não serão divulgados.

Caso não visualize o questionário no corpo do e-mail, clique no *link* https://spreadsheets.google.com/viewform?formkey=dFhOc3hXQ1M1OEozcERHdDJLQ3lKS2c6MA para responder ao questionário.

Solicito que respondam às questões aqui apresentadas até o dia 02/10/2009.

Desde já, agradeço pela colaboração e coloco-me à disposição para fornecer qualquer informação adicional.

Maíra Hanashiro
Analista de Finanças e Controle
CGU/SFC/DS/DSSAU
Ramal: 7307

Questionário

1 – Como pode ser classificada a necessidade de Auditoria de TI dentro do escopo da Coordenação?
* Para efeito de avaliação, considerar Auditoria de TI como sendo qualquer ação de controle dentro da Coordenação que envolva análise de um objeto de Tecnologia da Informação, independente de haver Ordem de Serviço formalizada.

( ) Muito Baixa
( ) Baixa.

( ) Média.
( ) Alta.
( ) Muito Alta.

2 – Existem servidores com conhecimentos em Tecnologia da Informação dentro da Coordenação?

( ) SIM
( ) NÃO

Caso a resposta seja SIM, informar a quantidade desses servidores: _____

Caso a resposta seja SIM, informar o(s) nome(s) desse(s) servidore(s):
_____
_____
_____

3 - Na sua Coordenação, existem trabalhos genéricos de Auditoria de TI? Exemplo: avaliação de um contrato de aquisição de softwares em uma Auditoria de Avaliação da Gestão.

( ) SIM
( ) NÃO

Caso a resposta seja SIM, citar o(s) exemplo(s) mais relevante(s):
_____
_____
_____

4 - Na sua Coordenação, já foram realizados trabalhos específicos de Auditoria de TI, em que o objeto de TI é o foco principal? Exemplo: análise de grandes bases de dados em busca de duplicidades, avaliação de algum sistema corporativo, entre outros.

( ) SIM
( ) NÃO

Caso a resposta seja SIM, citar o(s) exemplo(s) mais relevante(s), informando se houve ou não a emissão de Ordem de Serviço para as ações citadas. Caso a resposta seja NÃO, apresentar sua opinião sobre as razões pelas quais tais trabalhos não sejam realizados.
_____
_____
_____
_____

Caso a resposta seja SIM, se possível, informar a quantidade de auditorias de TI realizadas no ano de 2008. _____

5 - Escolher a opção que melhor represente o nível de maturidade da Auditoria de TI dentro da Coordenação: Classificação adaptada com base nos níveis de maturidade do COBIT (*Control Objectives for Information and related Technology*).

( ) A Coordenação não reconhece a existência de um processo de Auditoria de TI.

( ) Há evidências de que a Coordenação reconhece que o processo de Auditoria de TI existe e que as necessidades devem ser mapeadas. Entretanto, não há um processo padronizado e a execução das ações de controle de TI é feita caso a caso e baseada apenas nos processos genéricos de auditoria da Secretaria Federal de Controle – SFC.

( ) Os processos para a realização de Auditoria de TI são estruturados e procedimentos similares são seguidos por diferentes indivíduos para a mesma tarefa dentro da Coordenação. Há forte dependência do conhecimento individual e existe alguma documentação.

( ) Os processos de Auditoria de TI são padronizados, documentados e comunicados dentro da Coordenação. Entretanto, deixa-se a cargo dos indivíduos seguirem os processos. Não há certeza de que eventuais desvios serão detectados.

( ) Existe a possibilidade de monitorar e medir a conformidade dos processos de Auditoria de TI com os procedimentos definidos dentro da própria Coordenação. Há ações para melhoria.

( ) Os processos foram refinados até alcançarem as melhores práticas, com base no resultado de melhoria contínua e comparações com outras organizações e coordenações.

6 - Quais as dificuldades enfrentadas para a realização de Auditorias de TI? Marcar todas as que se aplicarem ao caso da Coordenação, mas apenas quando a opção realmente consistir em um fator dificultador para a realização de ações de controle de TI.

( ) Tempo insuficiente para a realização dos trabalhos.
( ) Falta de apoio da alta administração.
( ) Não é uma prioridade dentro da Coordenação.
( ) Falta de servidores capacitados em Auditoria de TI.
( ) Deficiência nos procedimentos de Auditoria de TI.
( ) Deficiência de recursos tecnológicos.
( ) Ausência de uma linguagem comum ou padrão dentro da SFC sobre Auditoria de TI.
( ) Falta de apoio técnico sobre Auditoria de TI.
( ) Inexistência de um núcleo consultivo de Auditoria de TI dentro da SFC.
( ) Outros: _____

7 - Citar potenciais objetos de Auditoria de TI que ainda não sofrem ação de controle ou sofrem ações incipientes e as razões pelas quais deveriam ser escopo de auditorias: Exemplos de razões: grande materialidade, criticidade e/ou relevância, entre outras. Se possível, dar detalhes sobre o contexto do objeto e sobre os recursos financeiros envolvidos.

_____
_____
_____

Observações Gerais

Se necessário, acrescentar informações adicionais acerca do assunto, de acordo com a realidade de sua Coordenação.

_____
_____
_____

Informações Básicas do Entrevistado

Nome Completo: _____

* Ressalta-se que os nomes dos colaboradores não serão divulgados em nenhum momento desse trabalho.

E-mail: _____

Cargo: _____

Ano de ingresso na carreira: _____

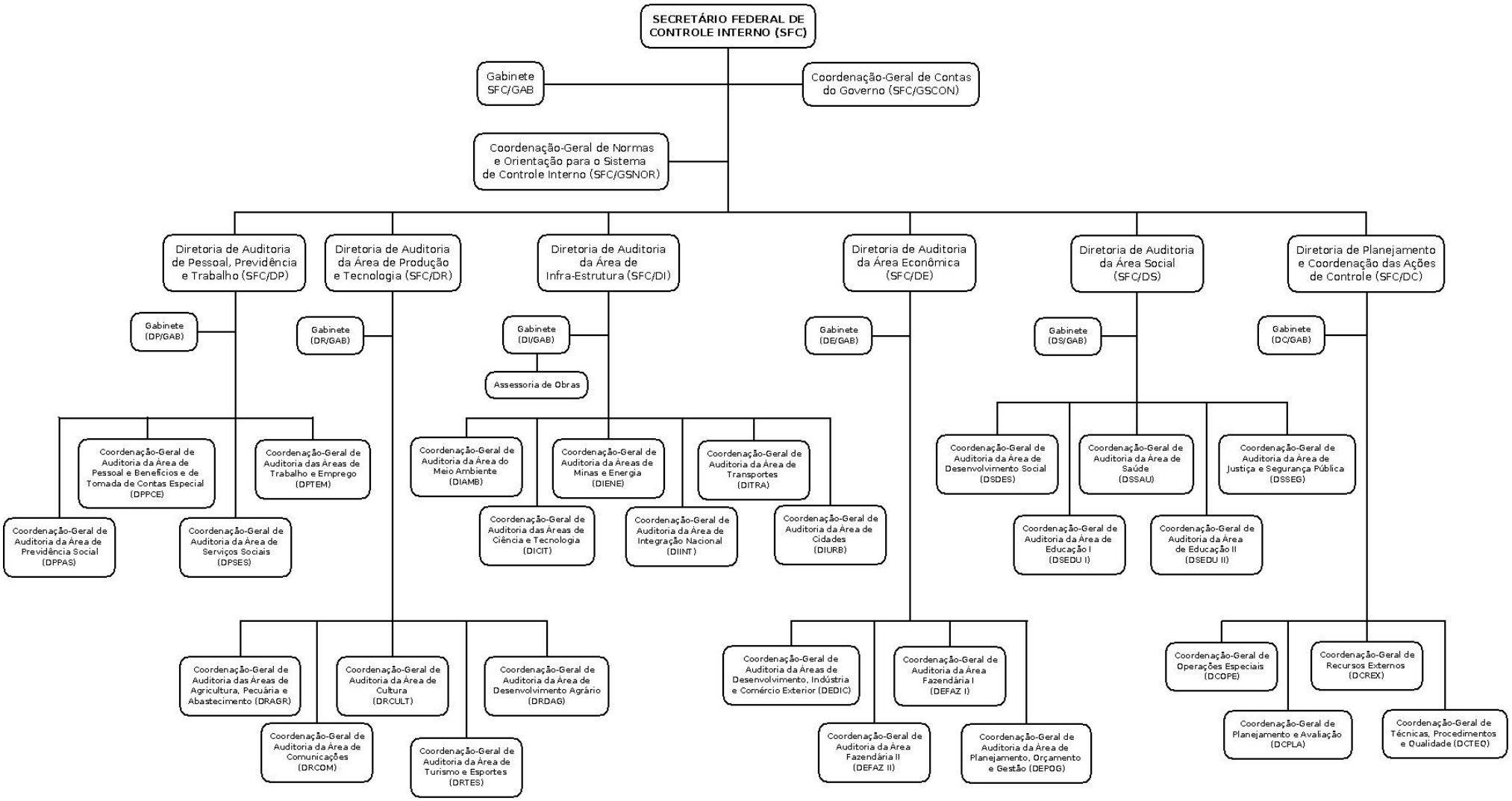
Coordenação: _____
* Usar a sigla. Por exemplo: DSSAU.

Formação Acadêmica: _____

Orçamento total previsto para 2009: _____

Orçamento de TI previsto para 2009: _____
* Deixar em branco caso não seja possível essa identificação.

APÊNDICE C – ORGANOGRAMA COMPLETO DA SFC



ANEXO A – ACÓRDÃOS DO TCU

A tabela abaixo apresenta os principais Acórdãos do TCU envolvendo Tecnologia da Informação:

Decisão / Acórdão	Assunto
Decisão 669/1995 – Plenário	Auditoria nos sistemas de arrecadação da SRF
Decisão 445/1998 – Plenário	Auditoria nos sistemas do FGTS
Decisão 957/1999 – Plenário	Auditoria para verificação dos procedimentos preparatórios para se evitar problemas com o *Bug* do ano 2000
Decisão 1049/2000 – Plenário	Auditoria de Segurança da Informação na Previdência Social
Decisão 295/2002 – Plenário	Auditoria no Sistema de Patrimônio da União
Decisão 1098/2002 – Plenário	Auditoria nos sistemas INSS e Dataprev
Decisão 1380/2002 – Plenário	Auditoria no Siafi
Acórdão 38/2003 – Plenário	Auditoria nos sistemas de loterias da Caixa
Acórdão 94/2003 – Plenário	Auditoria no Siape
Acórdão 1921/2003 – Plenário	Auditoria na base de benefícios da Previdência Social
Acórdão 1558/2003 – Plenário	Problemas na Contratação de Serviços de TI no MDIC
Acórdão 1521/2003 – Plenário	Inadequação de compra de *softwares* por meio do Contrato Select da Microsoft
Acórdão 461/2004 – Plenário	Auditoria no Datasus
Acórdão 782/2004 – 1ª Câmara	Auditoria no Sistema de Pagamentos do Exército
Acórdão 2094/2004 – Plenário	Entendimentos acerca da Contratação de Bens e Serviços de TI
Acórdão 140/2005 – Plenário	Auditoria no Ministério da Agricultura (insuficiência de RH de TI)
Acórdão 441/2005 – 1ª Câmara	Auditoria no Sistema Financeiro da Caixa
Acórdão 2023/2005 – Plenário	Auditoria na Gestão de TI do MTE
Acórdão 2138/2005 – Plenário	Uso do pregão nas licitações de TI
Acórdão 562/2006 – Plenário	Auditoria no Sistema de Doação de Órgãos
Acórdão 786/2006 – Plenário	Auditoria no MDIC (padrões do novo modelo para contratação de TI)
Acórdão 914/2006 – Plenário	Auditoria no Sistema Fies (Educação)
Acórdão 1386/2006 – Plenário	Auditoria no Governo Eletrônico Federal
Acórdão 1663/2006 – Plenário	Auditoria no Sistema de Informações Para Infância e Adolescência
Acórdão 71/2007 – Plenário	Auditoria na base Infoseg (Segurança Pública)
Acórdão 1092/2007 – Plenário	Auditoria nos sistemas de arrecadação da Infraero
Acórdão 1480/2007 – Plenário	Recomendações para o novo modelo para contratação de TI
Acórdão 1505/2007 – Plenário	Auditoria no Módulo de Consignações do Siape
Acórdão 1999/2007 – Plenário	Recomendações para o novo modelo para contratação de TI
Acórdão 1934/2007 – Plenário	Levantamento da legislação e jurisprudência aplicáveis às contratações de serviços de TI
Acórdão 1603/2008 – Plenário	Levantamento acerca da Governança de TI na Administração Pública Federal
Acórdão 2471/2008 – Plenário	Auditoria na Terceirização de TI na Administração Pública Federal
Acórdão 906/2009 – Plenário	Auditoria no Cadastro Único do Programa Bolsa Família
Acórdão 2812/2009 – Plenário	Auditoria no Sistema Informatizado de Controle de Óbitos da Previdência Social