Revista da CGU

ANO II - Nº 2
Outubro/2007
ISSN 1981-674X

Controladoria-Geral da União

Controladoria-Geral da União

Revista da CGU

Brasília, DF
Outubro/2007

A Revista da CGU é editada pela Controladoria-Geral da União

Tiragem: 1.500 exemplares
Periodicidade: semestral
Distribuição gratuita

Projeto gráfico, diagramação e arte: Via Brasília

Revista da CGU./ Presidência da República, Controladoria-Geral da União. - Ano II, nº 2, Outubro/2007. Brasília: CGU, 2007.

102 p. Coletânea de artigos.

1. Auditoria pública. I. Controladoria-Geral da União.

ISSN 1981- 674X
CDD 352.17

Sumário

Perspectivas para a auditoria de tecnologia da informação no âmbito da CGU

André Luiz Monteiro da Rocha, *Engenheiro de Computação, Analista de Finanças e Controle, DSSAU/DS/SFC/CGU-PR*
Eliane Barcaro, *Bacharel em Ciências de Computação, Analista de Finanças e Controle , DSEDU/DS/SFC/CGU-PR*
Maíra Hanashiro, *Engenheira De Redes de Comunicação, Analista de Finanças e Controle, SDES/DS/SFC/CGU-PR*
Rogério Vieira dos Reis*, Engenheiro de Controle e Automação, Assessor Técnico, DS/SFC/CGU-PR*
Viviane André Antunes, *Engenheira de Computação, Mestre em Engenharia Elétrica, Analista de Finanças e Controle, DSPAS/DS/SFC/CGU-PR*

1. Introdução

A Tecnologia da Informação (TI) tornou-se ferramenta imprescindível para diversas organizações. Diante desse quadro, no qual os processos passam a ficar altamente dependentes da TI, a utilização de procedimentos de Auditoria de TI mostra-se estratégica para garantir que a Gestão de TI esteja colaborando efetivamente para o atendimento dos objetivos da organização e para a mitigação das fragilidades e imperfeições que colocam em risco a confiabilidade das informações mantidas nos sistemas da organização.

No âmbito da Controladoria-Geral da União, inicia-se um processo de estruturação de procedimentos padronizados de Auditoria de TI, de forma que, em um futuro próximo, possa-se auditar a TI usada no Governo Federal utilizando-se modelos internacionalmente aceitos, detectar as fragilidades em TI dos órgãos da Administração Pública de forma subsidiada e fazer recomendações padronizadas, evitando-se, assim, que a CGU formule recomendações e advertências controversas.

O termo Auditoria de TI é muito amplo e freqüentemente objeto de confusões conceituais. Neste artigo sugerimos a seguinte taxonomia da Auditoria de TI:

- Auditoria de Dados – Ações de controle cujo objeto é uma base de dados a ser analisada com o auxílio de um software de análise de dados (ex. ACL) utilizando-se critérios estabelecidos em função da informação presente na base de dados.

- **Auditoria de Tecnologia** – Ações de controle cujo objeto é a infra-estrutura tecnológica (ex. sistema operacional, rede, etc.), exigindo conhecimento técnico aprofundado da área.

- **Auditoria de Gestão de TI** – Ações de controle cujo objeto é a própria Gestão da TI, envolvendo análise das atividades de planejamento, execução e controle dos processos de TI da Unidade examinada.

- **Auditoria de Segurança** – Ações de controle cujo objeto é o aspecto de segurança dos processos e sistemas da Unidade examinada.

- **Auditoria de Licitações e Contratos** – Ações de controle envolvendo análise de licitações ou contratos cujos objetos são bens ou serviços de TI.

- **Auditoria de Aplicativos** – Ações de controle envolvendo a análise de software tanto do ponto de vista operacional quanto do ponto de vista legal.

Com relação especificamente às áreas de Auditoria de Gestão de TI e de Auditoria de Segurança (podendo esta ser vista como inserida naquela) pode-se utilizar como referência modelos de Governança de TI (como CobiT(1) e ITIL(2)) e normas técnicas brasileiras (como a NBR 17799(3)).

As empresas brasileiras já perceberam a necessidade de se utilizar modelos e padrões de Governança de TI e Segurança da Informação para proteger seus ativos e alinhar a Tecnologia da Informação às necessidades do negócio.

> *O Tribunal de Contas da União – TCU e o Banco Central são exemplos de entidades que já iniciaram o processo de utilização de padrões e modelos internacionais de Governança e Gestão de TI*

As instituições financeiras, devido à necessidade de alinhamento internacional, são aquelas que estão mais à frente tanto na implementação da Governança de TI como na utilização de suas diretrizes para realização de auditoria.

Já a Administração Pública Federal tem despertado aos poucos para os benefícios e necessidades de alinhamento da TI ao negócio e de implantação de controles. O Tribunal de Contas da União –TCU e o Banco Central são exemplos de entidades que já iniciaram o processo de utilização de padrões e modelos internacionais de Governança e Gestão de TI. Inclusive, recentemente, foi criada no TCU a Secretaria de Fiscalização de Tecnologia

da Informação que, entre outras atribuições, cuidará da fiscalização da gestão e do uso dos recursos de tecnologia da informação pela Administração Pública Federal.

2. Histórico das Ações de Controle em TI na CGU

Sistemas de Informação têm sido objeto das ações de controle da Secretaria Federal de Controle Interno da Controladoria-Geral da União ao longo dos últimos anos. Dentre as áreas de auditoria da CGU que desenvolveram atividades nessa área, a Diretoria de Auditoria da Área Social executou diversos trabalhos no âmbito do Ministério da Previdência Social, do Ministério da Saúde e do Ministério do Desenvolvimento Social e Combate à Fome.

Com relação às ações governamentais da Previdência Social, podemos destacar como resultados principais:

- Detecção de pagamento indevido de aposentadorias, pensões, auxílios doença e invalidez na área de benefícios, através do cruzamento entre bases de dados de sistemas, tais como SISBEN (Sistema de Benefícios), SISOBI (Sistema de Óbitos), SIM (Sistema de Informações de Mortos – Ministério da Saúde) e CNIS (Cadastro Nacional de Informações Sociais). O cancelamento desses pagamentos levará a uma economia anual de cerca de R$1.042.125.973,33, sendo que R$212.082.290,00 já foram efetivamente cessados.
- Na área de arrecadação, a análise de dados auxilia na avaliação dos processos de regularização da cobrança dos créditos/débitos das áreas administrativa e judicial da Previdência Social, em relação a pagamento, parcelamento, baixas e entradas de crédito/débito, perfil e classificação dos 1.000 maiores devedores, por trimestre.

> *A análise de dados também tornou-se uma importante ferramenta para as auditorias na área da saúde*

A análise de dados também tornou-se uma importante ferramenta para as auditorias na área da saúde, podendo-se destacar os seguintes resultados:

- Constatação de irregularidades no cadastramento de profissionais no Programa Saúde da Família, ao detectarem-se centenas de médicos cadastrados (e sendo pagos) em mais de um município.
- Identificação de pagamento irregular de R$512 mil detectado em função de análise da base de dados de passagens e diárias do Ministério da Saúde.
- Transferência irregular aos Estados de R$232 milhões na ação governamental de financiamento de medicamentos excepcionais.

- Durante a Operação Sanguessuga, que desvendou um gigantesco esquema de fraude em licitações, a análise de dados auxiliou na descoberta de padrões de comportamento de diversas empresas nessas licitações, o que possibilitou a identificação de vários segmentos criminosos, bem como suas áreas de atuação no País.

> *O objetivo da Governança de TI é despertar a alta administração da importância de compartilhar decisões e responsabilidades*

Em relação ao Ministério do Desenvolvimento Social e Combate à Fome, destaca-se:

- Identificação de pessoas que acumulam indevidamente o recebimento dos benefícios dos programas Bolsa Família e Bolsa Escola, por meio de cruzamento das folhas de pagamento.

- Identificação de inconsistências e multiplicidades do Cadastro Único dos Programas Sociais do Governo Federal – CadÚnico.

- Auditoria dos sorteios de seleção e classificação dos candidatos a participar do Programa multiministerial ProJovem por meio da análise prévia do *software* e do banco de dados de inscritos usados no sorteio, visando conferir maior grau de confiabilidade ao processo e eliminação de registros duplicados antes da realização do sorteio a fim de garantir o equilíbrio de chances entre os candidatos.

3. Melhores Práticas de Governança de TI

3.1 Conceito

O objetivo da Governança de TI é despertar a alta administração da importância de compartilhar decisões e responsabilidades de TI com os demais dirigentes da organização no momento do estabelecimento das regras e processos que nortearão o uso de TI.

3.2 CobiT

O CobiT é um *framework* de Governança de TI desenvolvido pela ISACA (Information Systems Audit and Control Association) e mantido pelo ITGI (IT Governance Institute) consistindo em um grande apanhado de práticas e modelos com foco sobre "O que" deve ser feito e não sobre "Como".

As principais características deste modelo são as seguintes:

- Conjunto de publicações que incluem um sumário executivo, um *framework*, objetivos de controle, guia de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento;

- Independe das plataformas de TI adotadas na organização;
- Ajuda a otimizar os investimentos de TI e fornece métricas para avaliação dos resultados;
- Orientado ao negócio;
- Voltado para gerentes, pois auxilia na avaliação de riscos e controle de investimentos em TI; para usuários, pois oferece uma forma de garantir segurança e controles dos serviços de TI e para auditores, pois permite que avaliem o nível de gestão de TI e aconselhem o controle interno.

O Modelo de Maturidade de Governança é utilizado para o controle dos processos de TI e fornece um método eficiente para classificar o estágio da organização de TI em relação à indústria

A versão 4.0 é baseada nas melhores práticas e padrões reconhecidos internacionalmente, como PMBOK(4), ITIL, CMM(5), CMMI(6), NBR 17799, entre outros.

O CobiT é dividido em quatro domínios:

1. Planejamento e organização (PO);
2. Aquisição e implementação (AI);
3. Entrega e suporte (DS);
4. Monitoração e Avaliação (ME).

Cada domínio cobre um conjunto de processos para garantir a completa gestão de TI, somando-se 34 processos (10 de PO, 7 de AI, 13 de DS e 4 de ME) e 215 objetivos de controle.

Os mapas de controle fornecidos pelo CobiT auxiliam os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas de TI e, se necessário, recomendar a implementação de novas práticas.

Esse *framework* possui algumas ferramentas de Gerenciamento de TI, como: Modelo de Maturidade, Indicadores-Chave de Metas (KGIs) e Indicadores-Chave de Desempenho (KPIs).

O Modelo de Maturidade de Governança é utilizado para o controle dos processos de TI e fornece um método eficiente para classificar o estágio da organização de TI em relação à indústria, aos padrões internacionais e ao objetivo de maturidade da organização. A governança de TI e seus processos podem ser classificados da seguinte forma:

- 0 – Inexistente
- 1 – Inicial / *Ad Hoc*

- 2 – Repetitivo mas intuitivo
- 3 – Processos definidos
- 4 – Processos gerenciáveis e medidos
- 5 – Processo otimizados

> *Os mapas de controle fornecidos pelo CobiT auxiliam os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas de TI*

Os KGIs definem como serão mensurados os progressos das ações para atingir os requisitos de negócio, traduzidos como as características de informação de eficácia, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade. Os KPIs definem medidas para determinar como os processos de TI estão sendo executados e se eles permitem atingir os objetivos planejados.

3.3 ITIL

A ITIL – IT Infrastructure Library – é uma biblioteca de melhores práticas voltada para a área de TI. Foi desenvolvida pelo atual OGC (Office of Government Commerce), órgão público que busca otimizar e melhorar os processos internos do governo britânico.

Desde o seu surgimento no início da década de 1980 as empresas privadas e outras entidades públicas perceberam que as práticas sugeridas poderiam ser aplicadas em seus processos de TI e, a partir de 1990, a ITIL tornou-se um padrão de fato em todo o mundo.

Baseada na necessidade de fornecer serviços de alta qualidade, com ênfase no serviço e no relacionamento com o cliente, parte da filosofia da ITIL tem suporte nos sistemas de qualidade, tal como a ISO-9000.

A biblioteca é composta por sete livros principais e define os objetivos, atividades, entradas e saídas de cada processo de TI, oferecendo um *framework* comum para todas as atividades da área responsável pela TI na organização:

- Perspectiva de Negócio
- Entrega de Serviço
- Suporte à Serviço
- Gerenciamento da Segurança
- Gerenciamento da Infra-estrutura
- Gerenciamento de Aplicações
- Planejamento da implementação do Gerenciamento de Serviços

3.4 NBR 17799

A necessidade de padrões e normas que refletissem as melhores práticas de mercado relacionadas à

segurança dos sistemas e informações levou o British Standards Institute (BSI) à criação de uma das primeiras normas sobre o assunto, a BS 7799, que, uma vez aceita como padrão internacional, deu origem à ISO/IEC 17799:2000. Em 2001, tendo sido traduzida pela Associação Brasileira de Normas Técnicas (ABNT), foi adotada como NBR 17799 – Código de Prática para a Gestão da Segurança da Informação, com o objetivo de padronizar melhores práticas de gestão da segurança, definindo 127 objetivos de controle relacionados à Política de Segurança, Controle de Acesso, Segurança Física, Gerenciamento de Continuidade dos Negócios, dentre outros.

A utilização das Normas Técnicas como melhores práticas já vem sendo observada em alguns acórdãos do Tribunal de Contas da União, como no Acórdão n° 2023/05 que determina o estabelecimento institucional das atribuições relativas à segurança da informação conforme alguns itens da NBR 17799, bem como a definição de uma política de segurança nos termos de orientações da referida norma.

4. Perspectivas

Como relatado no item 2, a CGU já possui relativa experiência na área de Auditoria de Dados, cujos trabalhos têm levado a resultados interessantes. Com isso, o desafio atual é executar ações de controle nas outras áreas de Auditoria de TI, principalmente nas de Gestão de TI e de Segurança.

Em função da ausência de metodologia científica apropriada para elaboração e execução dessas ações de controle, experiências incipientes têm ocorrido no âmbito da Controladoria-Geral da União com o objetivo de adequar os procedimentos com base nas melhores práticas citadas no item 3. Com o apoio da alta administração, tem sido possível iniciar um processo de capacitação dos servidores de modo que, com o conhecimento teórico, sejam capazes de fazer a melhor adaptação dos modelos para as necessidades das demandas de trabalhos de auditoria de TI das Coordenações-Gerais.

> *Em 2001, tendo sido traduzida pela Associação Brasileira de Normas Técnicas (ABNT), foi adotada como NBR 17799 – Código de Prática para a Gestão da Segurança da Informação*

Como resultado da participação de servidores no XV Congresso Nacional de Auditoria de Sistemas, Segurança da Informação e Governança – CNASI de servidores e com a finalidade de multiplicar o conhecimento adquirido, foi realizado um ciclo de palestras com a presença de representantes de diversas áreas da CGU.

Além disso, trabalhos de auditoria têm sido realizados em Unidades nas quais processos críticos são altamente dependentes de sistemas de informação, fazendo com que o risco associado às fragilidades identificadas nos sistemas se torne muito elevado. Tanto aspectos de segurança como outros da gestão da TI são avaliados usando-se como referência as melhores práticas presentes no modelo de Governança CobiT 4 e principalmente a Norma Técnica da ABNT NBR 17799.

> *Trabalhos de auditoria têm sido realizados em Unidades nas quais processos críticos são altamente dependentes de sistemas de informação*

Para evitar que esses esforços individuais criem ilhas de excelência no âmbito das áreas de auditoria da CGU e, principalmente, para garantir que o tratamento a ser dado pelas auditorias no escopo de TI seja uniforme e institucionalmente padronizado, o cenário mais otimista consiste:

- Em um primeiro momento, na definição de uma metodologia de elaboração de procedimentos de auditoria de TI, a ser validada pela alta administração, baseada nos modelos de melhores práticas e normas citadas no item 3; e
- Em um segundo momento, por meio de um esforço coletivo, na elaboração propriamente dita de procedimentos padrões de auditoria de TI adequados às diversas realidades das áreas de auditoria da CGU.

5. Conclusão

Com procedimentos padronizados e interpretação uniforme das situações a serem detectadas nas futuras auditorias de TI, a CGU terá condições de orientar e colaborar na implantação da Governança de TI na Administração Pública Federal, baseando-se em modelos internacionalmente aceitos de melhores práticas e em normas técnicas brasileiras. Mais do que isso, terá condições de propor alterações normativas ou até mesmo na legislação, de forma a exigir o cumprimento dessas práticas e normas, a exemplo do que ocorre no setor bancário, que é obrigado a seguir normativos (*compliance*) do Banco Central que são fortemente baseados na NBR 17799 e no CobiT 4.

Referências bibliográficas

IT Governance Institute. CobiT – 4th Edition – 2005

Página oficial do ITIL no sítio da OGC – Office of Government Commerce (http://www.itil.co.uk)

ABNT. NBR ISO/IEC 17799:2005: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2005.

PMI. A guide to the Project Management Body of Knowlodge, Newton Square, Third Edition, 2004.

Página oficial do CMM no sítio da Carnagie Mellon (http://www.sei.cmu.edu/cmm/)

CMU/SEI-2002 – Capability Maturity Model Integration (CMMI), version 1.1. – Software Engineering – August/2002