UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

METODOLOGIA PARA DESENVOLVIMENTO DE PROCEDIMENTOS E PLANEJAMENTO DE AUDITORIAS DE TI APLICADA À ADMINISTRAÇÃO PÚBLICA FEDERAL

MAÍRA HANASHIRO

ORIENTADOR: RICARDO STACIARINI PUTTINI

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: 315/2007

BRASÍLIA / DF: 09/2007

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

METODOLOGIA PARA DESENVOLVIMENTO DE PROCEDIMENTOS E PLANEJAMENTO DE AUDITORIAS DE TI APLICADA À ADMINISTRAÇÃO PÚBLICA FEDERAL

MAÍRA HANASHIRO

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

RICARDO STACIARINI PUTTINI, Doutor, UnB/ENE
(ORIENTADOR)

ANDERSON CLEYTON ALVES NASCIMENTO, Doutor, UnB/ENE
(EXAMINADOR INTERNO)

JACYR LUIZ BORDIM, Doutor, UnB/CIC
(EXAMINADOR EXTERNO)

DATA: BRASÍLIA/DF, 14 DE SETEMBRO DE 2007.

FICHA CATALOGRÁFICA

HANASHIRO, MAÍRA
Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI aplicada à Administração Pública Federal [Distrito Federal] 2007, (xxii), (166)p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2007).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Auditoria de Tecnologia da Informação 2. Controle de Acesso
3. COBIT 4. Administração Pública Federal

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

Hanashiro, Maíra (2007). Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI aplicada à Administração Pública Federal. Dissertação de Mestrado, Publicação 315/2007, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília , DF, (166)p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Maíra Hanashiro
TÍTULO DA DISSERTAÇÃO: Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI aplicada à Administração Pública Federal.
GRAU/ANO: Mestre/2007.

Maíra Hanashiro
maira@redes.unb.br
Brasília – DF - Brasil

A Deus e à minha mãe.

AGRADECIMENTOS

A Deus por tudo.
A Nossa Senhora pela proteção e inspiração.
Ao meu orientador Ricardo Staciarini Puttini por todo suporte, amizade, paciência e confiança. Por todos os ensinamentos e oportunidades.
Ao Professor Adson Ferreira Rocha pela ajuda em momentos importantes.
Aos meus pais pelo dom da vida.
À minha mãe, Vera Viana, pela dedicação, incentivo, amor e apoio incondicionais.
Ao meu pai, Walter Hanashiro, por todos os ensinamentos transformadores.
A toda minha família por sempre acreditar em mim.
A todos que contribuíram diretamente neste trabalho com idéias, materiais e fontes.
Aos amigos e colegas de trabalho pela motivação, incentivo e interesse.
Aos amigos e companheiros de vida pelos exemplos de superação, pela paciência nos momentos de minha ausência e pelo incentivo em todos os meus desafios.
A todas as pessoas que passaram pela minha vida deixando seus ensinamentos e exemplos.

RESUMO

Este trabalho objetiva propor uma metodologia, baseada nas diretrizes do COBIT e demais modelos de melhores práticas de TI, aplicável à Administração Pública Federal, que possibilite planejar uma Auditoria de TI e desenvolver procedimentos a serem aplicados durante sua execução, de forma que se possibilite padronizar os processos de auditoria dentro do órgão auditor e criar uma linguagem comum entre auditor e auditado. Para isso, foi realizado um estudo dos modelos, padrões e normas de TI mais conhecidos nacional e internacionalmente. Em seguida é apresentado o modelo de fases para realização de auditorias de TI e, por fim, uma metodologia para desenvolvimento de procedimentos para estas auditorias.

ABSTRACT

The objective of this work is to propose a new methodology, based on COBIT Guidelines and other IT best practices model, that could be applied to Federal Public Administration. This new methodology would help planning IT Audit and developing procedures in order to standardize Audit processes and to create a common language between the auditor and the auditee. To accomplish that, a study of nationally and internationally known models, standards and norms was carried through. Finally, a phase model to perform IT audit and a methodology to develop audit procedures are presented.

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DE ABREVIAÇÕES

ABNT – Associação Brasileira de Normas Técnicas
AI – *Acquire and Implement*
APF – Administração Pública Federal
BID – Banco Interamericano de Desenvolvimento
BS – *British Standard*
BSC – *Balanced Scorecard*
CAAT – *Computer Assisted Audit Technique*
CGU – Controladoria Geral da União
CICA – *Canadian Institute of Chargered Accountants*
CMMI – *Capability Maturity Model Integration*
COBIT – Control Objectives for Information and Related Technology
CoCo – *Criteria of Control Board*
COSO – *Committee of Sponsoring Organizations of the Treadway Commission*
DS – *Deliver and Support*
eSCM – *eSourcing Capability Model*
FINEP – Financiadora de Estudos e Projetos
GAGAS – *Generally Accepted Government Auditing Standards*
IEC – *International Eletrotechnical Comission*
INTOSAI – *International Organization of Supreme Audit Institutions*
ISACA – *Information Systems Audit and Control Association*
ISACF – *The Information Systems Audit and Control Foundation*
ISMS – *Information Security Management System*
ISO – *International Organization for Standardization*
ISPPIA – *International Standards for the Professional Practice of Internal Auditing*
ITGI – *IT Governance Institute*
ITIL – *Information Technology Infrastructure Library*
ITSM – *Information Technology Service Management*
MCT – Ministério da Ciência e Tecnologia
ME – *Acquire and Implement*
MPS.BR – Melhoria de Processo do Software Brasileiro
NBR – Norma Brasileira

NIST – *National Institute of Standards and Technology*

OGC – *Office of Government Commerce*

PDCA – *Plan/Do/Check/Act*

PMBOK – *Project Management Body Of Knowledge*

PMI – *Project Management Institute*

PMO – *Project Management Office*

PO – *Plan and Organise*

PRINCE2 – *Projects in Controlled Environments 2*

RACI – *Responsible/Accountable/Consulted/Informed*

RBIA – *Risk Based Internal Auditing*

Sarbox – Lei Sarbanes-Oxley

SFC – Secretaria Federal de Controle

SGSI – Sistema de Gestão da Segurança da Informação

SI – Sistemas de Informação

SLTI/MP – Secretaria de Logística de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão

SOX – Lei Sarbanes-Oxley

TAAC – Técnicas de Auditoria Assistida por Computador

TCU – Tribunal de Contas da União

TI – Tecnologia da Informação

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.

De acordo com o sistema SIGA Brasil [100], dentro da Administração Pública Federal (APF) brasileira, há investimentos na ordem de bilhões de reais para capacitação e modernização tecnológica. 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.

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.

Com isso, surge dentro da Administração Pública a necessidade de implementação da Governança de TI, 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.

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.

Além disso, em um contexto em que toda tecnologia aparenta ser atraente e milagrosa, os processos de aquisição e desenvolvimento de tecnologia devem ser bem planejados e alinhados aos objetivos de negócio do órgão, de modo a impedir desperdícios de recursos públicos.

Diante do exposto, e como forma de evitar outros problemas como desvios, falhas e erros, 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.

A Auditoria de TI possibilita a avaliação dos controles implementados de forma a detectar fragilidades e incentivar a correção de problemas ou desconformidades.

Neste trabalho, propomos uma metodologia de planejamento de Auditoria de TI e desenvolvimento de procedimentos para serem utilizados em sua execução. Tal metodologia é resultado da adaptação do *framework* do COBIT [45] e de seu guia de atividades de auditoria, o *IT Assurance Guide* [62]. Complementarmente, adotamos normas e padrões de Auditoria nacionais e internacionais e, integrado aos objetivos de controle do COBIT, utilizamos normas e boas práticas de TI, como ITIL[74], CMMI[16], NBR ISO/IEC 17799 [9], PMBOK[95], entre outros.

A proposta é a simplificação e adequação destas publicações de forma a serem aplicáveis à APF e ao modelo de controle adotado pelo Estado Brasileiro.

Como forma de demonstração da metodologia apresentada para desenvolvimento de procedimentos, são desenvolvidos exemplos de procedimentos de auditoria de TI voltados para o Controle de Acesso, questão relacionada à Auditoria de Segurança da Informação.

Os objetivos almejados a partir dos resultados deste trabalho são:

- Contribuir com uma metodologia que permita a padronização das atividades dos processos de Auditoria de TI dentro dos órgãos de controle, a fim de que os resultados da análise de um mesmo objeto por áreas diferentes de um órgão auditor não sejam divergentes.

- Contribuir para o desenvolvimento de uma linguagem comum entre auditor e auditado.

- Contribuir para o alinhamento do uso da TI aos objetivos fins da Administração Pública;

- Incentivar a adequação dos órgãos às leis e melhores práticas relacionadas a TI;

- Fortalecer da Segurança da Informação dentro da APF; e

- Facilitar a detecção de problemas relacionados à TI juntamente com a responsabilização de seus agentes.

1.1. ORGANIZAÇÃO DO TRABALHO

Esta dissertação está organizada da seguinte forma:

No Capítulo 2 são detalhadas as motivações que ensejaram esta pesquisa, abordando a importância da TI dentro da Administração Pública Federal, descrevendo o Sistema de Controle da APF e demonstrando a importância da auditoria de Tecnologia da Informação.

No Capítulo 3 são tratados os principais conceitos sobre Governança de TI e Controle. Além disso, há uma visão geral das melhores práticas e normas adotadas nacional e internacionalmente e uma descrição do COBIT, do PMBOK, e da norma NBR ISO/IEC 17799 que são as publicações abordadas mais detalhadamente neste trabalho.

No Capítulo 4 é apresentada uma metodologia simplificada de realização de auditorias, abrangendo todo o seu ciclo de vida e detalhando suas principais etapas e atividades.

No Capítulo 5 é apresentado um modelo de desenvolvimento de procedimentos de Auditoria de TI que é demonstrado por meio de procedimentos relacionados a controles relativos ao Controle de Acesso, segmento da Segurança da Informação.

E, finalmente, no Capítulo 6, são apresentadas as conclusões desta dissertação, suas contribuições e as sugestões de trabalhos futuros.

2. MOTIVAÇÃO

Este trabalho tem como motivação o atual contexto dos investimentos em TI e a ausência de padrões de controle padronizados nesta área dentro da Administração Pública Federal.

Neste capítulo, faremos uma breve demonstração da importância da TI dentro da APF. Em seguida, falaremos sobre o Sistema de Controle da APF e, por fim, demonstraremos a necessidade do desenvolvimento de uma metodologia padronizada para auditoria em TI dentro deste contexto.

2.1. A TECNOLOGIA DA INFORMAÇÃO DENTRO DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Nos dias de hoje, a TI tem se tornado presente e, mais ainda, essencial em todos os setores da economia. Sendo assim, a esfera governamental não fica à margem dessa evolução tecnológica.

Nos últimos cinco anos, o Governo investiu mais de R$ 13.116.133.444,00 em TI. A Tabela 2.1 e a Figura 2.1 são resultados de uma consulta ao Sistema de Informações SIGA Brasil [100] em que foi usada como parâmetro de pesquisa a subfunção 126, que é referente ao orçamento destinado ao investimento em TI. Além desses valores, há gastos em TI que são embutidos em outras subfunções e, por isso, difíceis de serem contabilizadas. Estima-se, por exemplo, que os investimentos do exercício de 2006 tenham superado o valor de R$ 5 bilhões, quando da contabilização da função 126 com outras funções que incluem gastos em TI. Este investimento tem provocado a modernização da APF, tornando-a mais dinâmica e eficiente.

Tabela 2.1 - Investimentos em TI de 2002 a 2006

Exercício	Índice	Liquidado	Correção IGP-DI	Liquidado Corrigido
2002	1,450773608	R$ 2.488.602.337	1.121.796.255	R$ 3.610.398.592
2003	1,181547283	R$ 1.934.993.089	351.292.739	R$ 2.286.285.828
2004	1,080042109	R$ 2.058.443.617	164.762.168	R$ 2.223.205.785
2005	1,019226971	R$ 2.370.010.482	45.568.123	R$ 2.415.578.605
2006	1	R$ 2.580.664.634	0	R$ 2.580.664.634

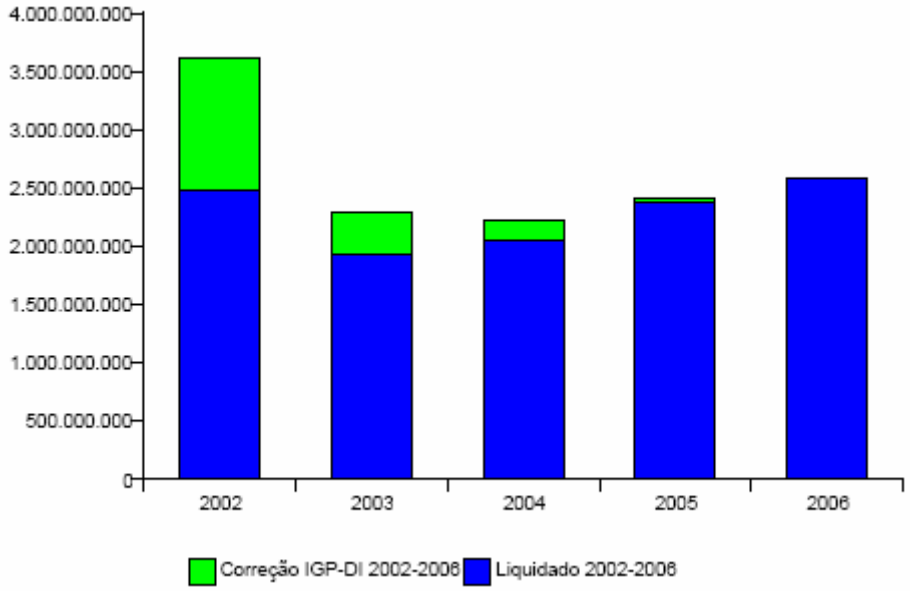

Figura 2.1 - Gráfico de Investimentos em TI de 2002 a 2006
Fonte: SIGA Brasil

Atualmente, organizações bem sucedidas, públicas ou privadas, são aquelas que sabem escolher e utilizar a tecnologia de forma apropriada para atingir seus objetivos. Isto está diretamente relacionado com a Governança de TI, que será explicada no capítulo seguinte.

Assim, à medida que a tecnologia se confunde com 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.

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.

Portanto, é fundamental que as organizações públicas se utilizem da Governança de TI satisfazer a necessidade do gestor e atender à exigência da população, garantindo eficiência, eficácia e economicidade na aplicação dos recursos.

2.2. CONTROLE NA ADMINISTRAÇÃO PÚBLICA FEDERAL

De acordo com o Decreto-Lei nº 200/1967 [ANEXO I: LEGISLAÇÃO DE CONTROLE], o Controle é um dos princípios fundamentais da Administração Pública e pode ser exercido de diversas formas e por todos os Poderes da República (Executivo, Legislativo e Judiciário).

Segundo Vicente de Paulo e Marcelo Alexandrino [14], conceitua-se Controle como o poder-dever de vigilância, orientação e correção que a própria Administração, ou outro Poder, diretamente ou por meio de órgãos especializados, exerce sobre sua atuação administrativa.

O Sistema de Controle da Administração Pública, responsável pela execução das ações de controle, é composto pela integração entre Controle Externo e Controle Interno, tendo como objetivos:

- Assegurar eficácia, eficiência e economicidade na administração e aplicação dos recursos públicos;

- Evitar desvios, perdas e desperdícios;

- Garantir o cumprimento de normas técnicas, administrativas e legais;

- Identificar erros, fraudes e respectivos agentes;

- Preservar a integridade patrimonial; e

- Propiciar informações para a tomada de decisões.

O alcance e o sentido das regras relativas à atuação da Administração Pública em geral são regidos pelos princípios fundamentais da Administração Pública que se encontram, explícita ou implicitamente, no texto da Constituição Federal Brasileira de 1988. Assim, o Sistema de Controle da Administração deve considerar tais princípios tanto na execução de seus atos como na verificação do cumprimento desses princípios dentro da administração. Os principais princípios são:

- Princípio da Legalidade: A Administração Pública, no exercício de suas funções, somente pode agir conforme o estabelecido em lei.

- Princípio da Moralidade: Além de da exigência da atuação legal, o agente público deve agir de forma ética e honesta.

- Princípio da Impessoalidade: Por este princípio, a atuação administrativa não deve visar interesse de agentes ou terceiros, mas sim o interesse da coletividade. Além disso, os atos administrativos são vinculados à Administração como um todo, não devendo ser vinculados à pessoa do administrador de forma a lhe render promoção pessoal.

- Princípio da Publicidade: Este princípio possui dupla acepção. Na primeira, um ato administrativo só possui eficácia quando de sua publicação oficial. A segunda refere-se à necessidade de transparência das atividades administrativas em geral.

- Princípio da Eficiência: Todo agente público, em suas atribuições, tem a obrigação de agir com presteza, perfeição e rendimento funcional, de forma a obter os melhores resultados.

- Princípio da Supremacia do Interesse Público: A atuação do Estado deve sempre ter por finalidade a tutela do interesse público, visando o benefício da coletividade.

- Princípio da Indisponibilidade: Os bens e interesses públicos são indisponíveis, não podendo a Administração ou seus agentes praticar atos que não sejam em prol da coletividade ou onerem a sociedade.

- Princípio da Continuidade dos Serviços Públicos: A prestação dos serviços públicos deve ser adequada e não pode sofrer interrupções, salvo em situação de emergência ou, após aviso prévio, por razões técnicas ou inadimplência do usuário.

- Princípio da Autotutela: Poder-dever de a Administração rever seus próprios atos, de acordo com mérito e legalidade.

A Constituição Federal de 1988 estabelece, em seus artigos 70, 71 e 74, as finalidades dos Controles Externo e Interno:

> *"**Art. 70**. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder.*
>
> ***Parágrafo único**. Prestará contas qualquer pessoa física ou jurídica, pública ou privada, que utilize, arrecade, guarde, gerencie ou administre dinheiros, bens e valores públicos ou pelos quais a União responda, ou que, em nome desta, assuma obrigações de natureza pecuniária.*
>
> ***Art. 71**. O controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União, ao qual compete:*
> *I - apreciar as contas prestadas anualmente pelo Presidente da República, mediante parecer prévio que deverá ser elaborado em sessenta dias a contar de seu recebimento;*
> *II - julgar as contas dos administradores e demais responsáveis por dinheiros, bens e valores públicos da administração direta e indireta, incluídas as fundações e sociedades instituídas e mantidas pelo Poder Público federal, e as contas daqueles que derem causa a perda, extravio ou outra irregularidade de que resulte prejuízo ao erário público;*
> *III - apreciar, para fins de registro, a legalidade dos atos de admissão de pessoal, a qualquer título, na administração direta e indireta, incluídas as fundações instituídas e mantidas pelo Poder Público, excetuadas as nomeações para cargo de provimento em comissão, bem como a das concessões de aposentadorias, reformas e pensões, ressalvadas as melhorias posteriores que não alterem o fundamento legal do ato concessório;*

IV - realizar, por iniciativa própria, da Câmara dos Deputados, do Senado Federal, de Comissão técnica ou de inquérito, inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial, nas unidades administrativas dos Poderes Legislativo, Executivo e Judiciário, e demais entidades referidas no inciso II;
V - fiscalizar as contas nacionais das empresas supranacionais de cujo capital social a União participe, de forma direta ou indireta, nos termos do tratado constitutivo;
VI - fiscalizar a aplicação de quaisquer recursos repassados pela União mediante convênio, acordo, ajuste ou outros instrumentos congêneres, a Estado, ao Distrito Federal ou a Município;
VII - prestar as informações solicitadas pelo Congresso Nacional, por qualquer de suas Casas, ou por qualquer das respectivas Comissões, sobre a fiscalização contábil, financeira, orçamentária, operacional e patrimonial e sobre resultados de auditorias e inspeções realizadas;
VIII - aplicar aos responsáveis, em caso de ilegalidade de despesa ou irregularidade de contas, as sanções previstas em lei, que estabelecerá, entre outras cominações, multa proporcional ao dano causado ao erário;
IX - assinar prazo para que o órgão ou entidade adote as providências necessárias ao exato cumprimento da lei, se verificada ilegalidade;
X - sustar, se não atendido, a execução do ato impugnado, comunicando a decisão à Câmara dos Deputados e ao Senado Federal;
XI - representar ao Poder competente sobre irregularidades ou abusos apurados.
§ 1º - No caso de contrato, o ato de sustação será adotado diretamente pelo Congresso Nacional, que solicitará, de imediato, ao Poder Executivo as medidas cabíveis.
§ 2º - Se o Congresso Nacional ou o Poder Executivo, no prazo de noventa dias, não efetivar as medidas previstas no parágrafo anterior, o Tribunal decidirá a respeito.
§ 3º - As decisões do Tribunal de que resulte imputação de débito ou multa terão eficácia de título executivo.
§ 4º - O Tribunal encaminhará ao Congresso Nacional, trimestral e anualmente, relatório de suas atividades.

***Art. 74**. Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, sistema de controle interno com a finalidade de:*
I - avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União;
II - comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado;
III - exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;
IV - apoiar o controle externo no exercício de sua missão institucional."

Portanto, o Controle Externo é o controle exercido pelo Congresso Nacional, dentro dos limites estabelecidos pela legislação, com auxílio do Tribunal de Contas da União - TCU, sobre os demais Poderes.

Segundo a Lei nº 10.180 [ANEXO I: LEGISLAÇÃO DE CONTROLE], o Sistema de Controle Interno do Poder Executivo Federal é integrado pela Secretaria Federal de Controle Interno (SFC), como órgão central, e pelos órgãos setoriais. A SFC faz parte da

Controladoria Geral da União (CGU) e os órgãos setoriais são aqueles de controle interno que integram a estrutura do Ministério das Relações Exteriores, do Ministério da Defesa, da Advocacia-Geral da União e da Casa Civil.

Dentre outras, são competências dos órgãos e unidades do Sistema de Controle Interno do Poder Executivo Federal:

- Fiscalizar e avaliar a execução dos programas de governo, inclusive ações descentralizadas realizadas à conta de recursos oriundos dos Orçamentos da União, quanto ao nível de execução das metas e objetivos estabelecidos e à qualidade do gerenciamento;

- Avaliar a execução dos orçamentos da União;

- Fornecer informações sobre a situação físico-financeira dos projetos e das atividades constantes dos orçamentos da União;

- Realizar auditoria sobre a gestão dos recursos públicos federais sob a responsabilidade de órgãos e entidades públicos e privados; e

- Avaliar o desempenho da auditoria interna das entidades da administração indireta federal.

Tanto o TCU como a SFC exercem regularmente auditorias e fiscalizações nos órgãos, entidades e demais recebedores de recursos da União a fim de avaliarem a aplicação de tais recursos.

2.3. A IMPORTÂNCIA DA AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO

Como demonstrado neste capítulo, a Tecnologia da Informação tornou-se parte estratégica para as organizações e, diante deste quadro no qual os processos passam a ficar

altamente dependentes da TI, a realização de auditorias por parte dos órgãos de controle mostra-se essencial para se garantir que a Gestão de TI esteja colaborando efetivamente para o atendimento dos objetivos da organização e para a mitigação das fragilidades que coloquem em risco a confiabilidade, integridade, efetividade, eficiência, confidencialidade (quando for o caso), disponibilidade e conformidade (com normas e legislação) das informações mantidas nos sistemas de informação da organização.

Os sistemas informatizados são realidade em toda a APF e ajudam a otimizar as atividades administrativas e gerenciais do Estado. Entretanto, como dito anteriormente, a tecnologia não deve ser implantada de modo desordenado e nem de forma desvinculada dos objetivos finalísticos da APF. Além disso, a informação, agora mais acessível, deve ser protegida das vulnerabilidades de segurança que esta situação a expõe.

Diante deste novo contexto, a TI também precisa ser objeto de ações de controle do Sistema de Controle da Administração Pública, de forma a garantir que os critérios da informação (serão detalhados no capítulo seguinte) sejam atendidos, contribuindo para a eficácia, eficiência e economicidade dos serviços públicos e para a prevenção de irregularidades, desvios e perdas de recursos públicos.

A Auditoria de TI já está presente no controle interno de diversas instituições públicas, sendo mais atuantes, estruturadas e maduras 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 especializados em controle, 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.

Por fim, outro fator complicador é a abrangência desse tipo de auditoria. O termo Auditoria de TI é muito amplo e envolve diversas áreas da Tecnologia, das quais se pode destacar:

- **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 Infra-Estrutura** - 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, sistemas e informações 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.

Essa diversidade de áreas exige que o auditor possua amplos conhecimentos ou que se tenha uma equipe com membros com conhecimentos nas áreas que integram o escopo da auditoria a ser realizada.

Portanto, as principais necessidades que podem ser identificadas em uma metodologia de Auditoria de TI são:

- Padronização da metodologia dentro de toda a entidade auditora;

- Linguagem comum entre auditor e auditado; e

- Modelagem de procedimentos de auditoria que possam abranger a diversidade de assuntos da área de TI.

Para solucionar tais questões, propomos, neste trabalho, o desenvolvimento de projetos de auditoria de TI baseada em uma metodologia que se utilize de padrões, métodos, modelos, normas e boas práticas conhecidas e bem aceitas no mercado nacional e internacional.

A principal base utilizada para a metodologia são as publicações do COBIT. Já para o desenvolvimento dos procedimentos específicos, propõe-se a utilização das boas práticas propostas na biblioteca ITIL, normas técnicas da ISO, técnicas de gerenciamento de projeto como PMBOK e PRINCE2, legislação brasileira, CMMI, entre outros.

Para tanto, necessita-se compilar tais melhores práticas e adaptá-las às necessidades e especificidades da Administração Pública de forma que sejam aplicáveis na prática.

A fim de demonstrar o modelo proposto, criamos procedimentos específicos para uma Auditoria de Controle de Acesso à informação (sub-área da Auditoria de Segurança) dentro dos órgãos da APF.

2.4. A AUDITORIA DE TI DENTRO DA APF

Todavia, antes de ser apresentado o modelo proposto, uma crítica ao atual contexto legal e infra-legal da Auditoria de TI deve ser feita. Por melhores que sejam as referências e metodologias implementadas, os órgãos de auditoria de TI enfrentam um problema maior do que sua própria infra-estrutura e capacidade fiscalizatória. Uma das grandes dificuldades é a sustentação nas recomendações das auditorias de que essas melhores práticas devem ser seguidas, já que não existem instruções normativas ou legislação dentro da APF que obrigue a utilização dessas práticas. O mais próximo disso são os vários acórdãos do TCU que fazem recomendações baseadas nesses padrões e modelos.

Dessa forma, por mais bem estruturado que seja o processo de auditoria, ela 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.

A mais recente iniciativa em direção à normatização de processos de TI dentro da APF pode ser visto nos Acórdãos 796/2006 – Plenário e 1480/2007 – Plenário do TCU. O primeiro recomenda que a Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MP elabore um modelo de licitação e contratação de serviços de informática para a Administração Pública Federal. O segundo consiste na análise da minuta de instrução normativa encaminhada pela SLTI relativa a este modelo solicitado. Em sua análise, o TCU faz diversas ressalvas ao modelo com a finalidade de que este esteja alinhado com os valores da Governança de TI e, em suas recomendações, sugere o uso das melhores práticas do mercado relacionadas a *outsourcing*, como ITIL, COBIT, MPS.BR e etc.

Outra importante iniciativa é o Projeto de Lei PLS-76/2000 que está no Congresso Nacional e que dispõe sobre crimes cometidos na área de informática, tipifica condutas que envolvam o uso de redes de computadores e internet, ou praticados contra sistemas informatizados. O Projeto já foi aprovado na Câmara dos Deputados e na Comissão de Educação do Senado. Atualmente, encontra-se na Comissão de Constituição e Justiça.

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.

3. BASE TEÓRICA

3.1. GOVERNANÇA DE TI

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.

A Governança de TI é responsabilidade da Direção da Organização e permite à Instituição satisfazer os requisitos de qualidade, confiança e segurança de suas informações e ativos relacionados. Além disso, permite à Gestão Corporativa otimizar o uso dos recursos, incluindo-se nestes dados, sistemas de aplicação, tecnologias, instalações e pessoal.

A Governança de TI não é uma disciplina isolada, ela é parte integral da governança corporativa. O aumento da demanda por a 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 estratégicas de TI sustem e cubram as estratégias e objetivos da empresa.

As responsabilidades na Governança de TI fazem parte do *framework* de governança corporativo e devem fazer parte da agenda de planejamento estratégico dos diretores da empresa. De forma mais simples, quando houver dependência crítica sobre os sistemas de TI, a governança deve ser efetiva, transparente e responsável. Desta forma, é possível assegurar que as expectativas sobre TI sejam alcançadas e os riscos sobre TI sejam gerenciados.

Atualmente, é impossível imaginar uma empresa sem uma forte área de sistemas de informações para manipular os dados operacionais e prover informações gerenciais aos executivos para tomadas de decisões.

Entretanto, a criação e manutenção de uma infra-estrutura de TI, incluindo profissionais especializados, requerem altos investimentos. Por isso, algumas vezes, a alta direção da empresa coloca restrições aos investimentos de TI por duvidarem dos reais benefícios da tecnologia. Entretanto, a ausência de investimentos em TI pode ser o fator chave para o fracasso de um empreendimento em mercados cada vez mais competitivos ou para a ineficácia de uma gestão, tanto no meio privado como na Administração Pública. Além disso, alguns gestores de TI não possuem habilidade para demonstrar os riscos associados ao negócio sem os corretos investimentos em TI. E, na extremidade oposta, existem os gestores de TI que conseguem recurso para o investimento, mas não conseguem aplicá-los de forma a trazer benefícios reais para a organização.

Para melhorar o processo de análise de riscos e tomada de decisão, é necessário um processo estruturado para gerenciar e controlar as iniciativas de TI nas empresas, para garantir o retorno de investimentos e adição de melhorias nos processos organizacionais.

Uma Governança de TI efetiva visa responder adequadamente as questões a seguir:

- **Princípios básicos para a TI:** Declarações de alto nível sobre como a TI deve ser usada na organização.

- **Arquitetura de TI:** Escolhas técnicas, políticas, regras, planos de migração (inclui dados, tecnologias e aplicações).

- **Estratégias para a Infra-estrutura de TI:** estratégias para os recursos e competências de TI compartilhadas na organização (pessoal, rede, dados, *help desk*, etc.)

- **Necessidades das aplicações aos negócios:** Especificar necessidades de negócio para comprar ou desenvolver aplicações de TI.

- **Investimentos em TI e suas prioridades:** decisões sobre quanto e onde investir em TI. Aprovação e justificação de projetos.

Neste cenário, a Governança de TI aparece como de importância vital para o negócio e tem como princípios:

- **Direção e Controle:** A Direção fornece as diretrizes necessárias para a implementação de uma mudança. Já o Controle assegura que o objetivo dessa mudança seja alcançado e que nenhum incidente indesejado ocorra ou, pelo menos, que seja mitigado. A Figura 3.1 demonstra as relações entre Direção e Controle.

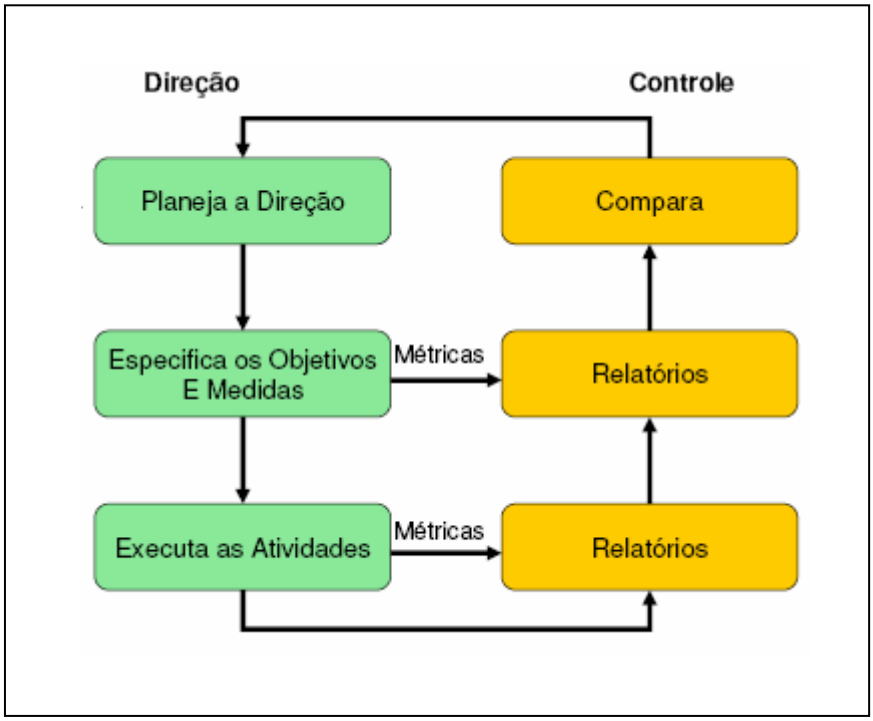

Figura 3.1 - Relações entre Direção e Controle

- **Responsabilidade:** O Alta Administração deve determinar a responsabilidade para o estabelecimento do Controle Interno. No caso dos Ministérios na Administração Pública Federal, existe a figura do Assessor de Controle Interno, responsável pelo Controle dentro do Órgão. Entretanto, o Controle Interno é de responsabilidade de todos em uma organização e pode ser uma função explícita ou implícita.

- **Prestação de Contas:** Os colaboradores têm a obrigação de prestar contas, fornecer relatórios ou explicar suas ações sobre o uso de recursos que lhes são transmitidos. Os diretores prestam contas à quem for hierarquicamente superior que, por sua vez, deve

fornecer governança, direção e monitoração. Para cada um, é essencial conhecer como suas ações contribuem para alcançar os objetivos da organização.

- **Atividades:** As atividades de TI são eficientes quando existe uma boa Governança de TI. Normalmente, os Departamentos de TI nas empresas funcionam como se fossem o motor de um automóvel, onde trabalham conforme ações realizadas pelo motorista, que neste caso se equivale à Alta Administração.

O Escopo de Governança de TI pode ser classificado em cinco áreas, conforme apresentado na Figura 3.2.

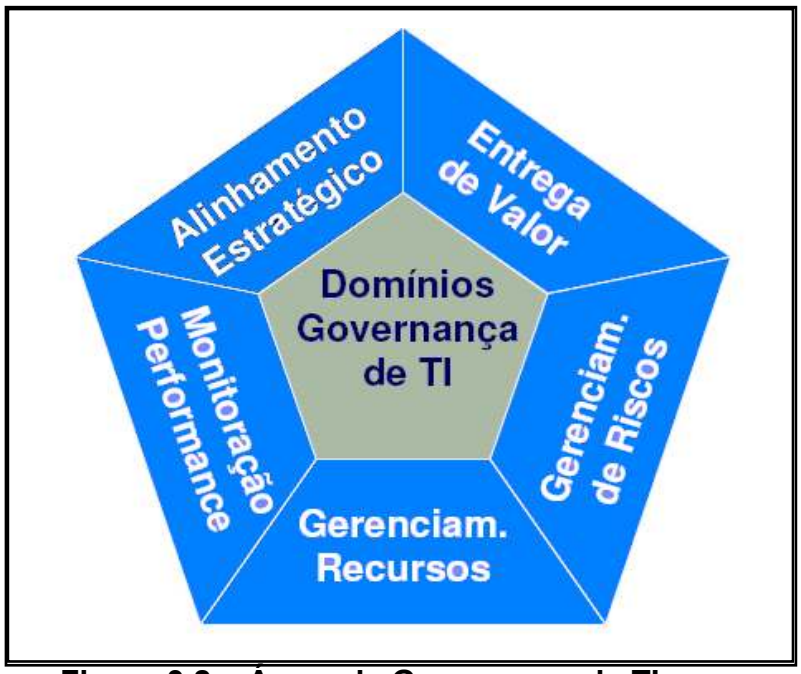

Figura 3.2 – Áreas de Governança de TI
Adaptado do *IT Governance Institute*

O Alinhamento Estratégico refere-se à garantia da ligação entre o negócio e os planos de TI, manutenção e validação da proposição de valor da TI, e alinhamento das operações da empresa com as de TI.

A Entrega de Valor (ou agregação de valor) refere-se à execução da proposição de valor através do tempo, assegurando que a TI entregue os benefícios prometidos de acordo com a estratégia, concentrando-se em otimizar custos e comprovar o valor intrínseco da TI.

O Gerenciamento de Riscos refere-se ao conhecimento dos riscos por parte da alta administração, ao entendimento claro dos requisitos de conformidade e das tendências da organização para os riscos, à transparência acerca dos riscos significativos para a empresa e à incorporação de responsabilidades para o gerenciamento dos riscos na organização.

O Gerenciamento de Recursos refere-se à otimização dos investimentos e da gestão adequada dos recursos críticos de TI, essenciais para fornecer os subsídios de que a organização necessita para alcançar seus objetivos.

A Monitoração de *Performance* refere-se ao acompanhamento e monitoração das atividades por meio de medições convencionais e indicadores de desempenho que traduzem a estratégia em ações para atingir objetivos mensuráveis.

3.2. CONTROLE INTERNO

Controles internos são definidos pela totalidade das políticas, procedimentos e práticas instituídas pela Administração, para assegurar que os riscos inerentes às atividades da instituição sejam identificados e gerenciados adequadamente, com a finalidade maior de fornecer razoável garantia à Administração de que os objetivos de negócio estão sendo continuamente alcançados. São, portanto, mecanismos de gestão que devem permear as operações e atividades críticas de forma ampla, gerenciada e eficaz, e devem ser adaptáveis às necessidades próprias de cada organização.

Estruturar, implementar e manter eficaz um Sistema de Controles Internos passou a ser fator fundamental para o sucesso das instituições, quer para a identificar e gerenciar os riscos operacionais, quer para adequar políticas e procedimentos internos para atenderem às regulamentações respectivas.

A seleção de um *framework* de controle interno depende, fundamentalmente, de quais tipos de objetivos a instituição visa alcançar de uma forma gerenciada.

Dentre as opções de *framework*, destacam-se soluções voltadas para alcançar os objetivos de negócio ou para alcançar os objetivos de áreas de conhecimento específicas, como a área de Segurança da Informação. A Tabela 3.1 resume e exemplifica alguns dos *frameworks* reconhecidos pelo mercado e seus focos:

Tabela 3.1 – Exemplos de *Frameworks*

Para objetivos de negócio	**Para objetivos de negócio focando em TI**	**Para objetivos de Segurança da Informação**
COSO	COBIT	NBR ISO/IEC 17799
CoCo	ITIL	

Independente dos objetivos específicos que mobilizam a escolha da instituição, o primeiro e mais tangível benefício em se adotar qualquer dessas estruturas é garantir que haja uma linguagem comum entre as diversas áreas envolvidas mais diretamente com a gestão de riscos, geralmente as área de Auditoria Interna, *Compliance* (conformidade com regulações), risco e a própria Administração.

Como conseqüência, os resultados obtidos para a definição, avaliação e implementação dos controles internos podem ser comunicados adequadamente a partir das camadas estratégicas para as operacionais e vice-versa, configurando-se essa estrutura (*framework*) como uma referência global para o processo de gestão de riscos corporativos. O resultado desse entendimento contribui positivamente para que todas essas funções desempenhem o seu papel efetivo nesse processo, tornando a gestão de riscos um verdadeiro pilar para a Governança Corporativa.

O COSO [20][80] e o CoCo [79] são metodologias de Governança Corporativa distantes do nível operacional e requerem a complementação com outros modelos de gestão.

A metodologia CoCo foi criada pelo *Canadian Institute of Chargered Accountants (CICA)*, para auxiliar a alta administração das organizações a implementar e avaliar um ambiente de controle, de modo a atingir seus objetivos operacionais e estratégicos. O CoCo não será tratado neste trabalho, mas mais informações podem ser encontradas em [79].

A metodologia publicada pelo COSO - *Committee of Sponsoring Organizations of the Treadway Commission* - identifica os objetivos essenciais do negócio de uma dada instituição e define o Controle Interno e seus componentes, fornecendo critérios a partir dos quais os sistemas de controle podem ser avaliados.

Segundo o COSO, Controle Interno é um processo, que se torna efetivo através das pessoas, as quais devem assegurar com razoável grau de segurança que os seguintes objetivos, fundamentais a qualquer negócio, serão atingidos:

- Economia e eficiência das operações, incluindo o alcance dos objetivos em termos de *performance* e segurança dos ativos contra perdas;

- Veracidade das demonstrações financeiras;

- *Compliance* com as normas e legislação locais.

O Ambiente de Controle representa a filosofia da instituição com relação a evitar riscos e assimilar a cultura de controle. Ele é tanto melhor quanto mais bem definidas estão as responsabilidades individuais, a clareza do que é devido e como se deve agir em caso de violação dos princípios éticos e de conduta, pois os sistemas de Controle Interno dependem, para serem efetivos, da aceitação, do comprometimento e da boa comunicação dos colaboradores envolvidos nos processos operacionais.

Com a implementação de um Sistema de Controles Internos, existe a necessidade de se verificar, sistematicamente, se esses controles estão implementados e são eficazes para os propósitos da instituição.

Denominamos Análise de Riscos ao mecanismo de verificação dos controles como parte do processo de gerenciamento dos riscos da instituição. As análises são instrumentos de planejamento do Sistema de Controles Internos, permitindo avaliar e propor controles adequados aos requisitos de segurança e *compliance* com políticas internas e normativas externas aplicáveis.

Uma vez implementados, os controles irão reduzir ou transferir riscos, sendo necessário avaliar sua eficácia em relação aos objetivos de controle e, devido às mudanças de estratégia e organizacionais, se eles continuam efetivos ao longo do tempo.

Essa função fica a cargo das Auditorias de Controles, processos investigativos que visam gerar indicadores de *compliance* com as políticas internas e normativas externas. Como resultado, os relatórios deverão mostrar as não conformidades e as respectivas relevâncias desses pontos para o cumprimento dos objetivos de negócio. Por esta perspectiva, as auditorias são instrumentos de monitoração da *performance* do Sistema de Controles Internos.

Já quando se foca na Governança em TI, diretrizes de melhores práticas como a *IT Infrastructure Library* – ITIL e *Control Objectives for Information and Related Technology* – COBIT estão no mercado há anos. Em sua maioria, esses *frameworks* deveriam trazer consistência e eficiência aos vários aspectos da TI, como desenvolvimento de aplicações, *help desk*, operações de redes, segurança e entrega e suporte a serviços. Com uma implantação bem feita dessas práticas, a TI alinha-se com a área de negócios, de maneira que os gerentes de TI traduzem seus serviços em termos de negócios e colocam prioridades também de negócios em suas listas de prioridades.

A maioria desses *frameworks* não são exclusivos e são mais efetivos quando utilizados em combinação. O caminho para um *framework* compreensivo de governança envolve o entendimento das diferenças entre eles e como tais medidas podem ser aplicadas.

Uma abordagem interessante na adoção dos *frameworks* de melhores práticas pode ser feita em três fases: começar com um *framework* como COBIT e ITIL; embasar o nível operacional em um padrão que pode ser certificado como ISO; e promover melhorias que possam ser medidas, como CMMI e Six Sigma.

Neste trabalho, serão utilizados conceitos de controle interno referentes ao COSO, mas o enfoque será dado na área de TI. Portanto, trabalharemos com COBIT e outros *frameworks* mais específicos, como a ABNT NBR ISO/IEC 17799.

3.3. MELHORES PRÁTICAS E NORMAS

O ideal é que, dentro da Administração Pública, adotem-se melhores práticas e normas nacionais e internacionais já bem aceitas no mercado. Assim, pode-se ter Governança de TI em todos os órgãos e seus conseqüentes benefícios.

Neste item, listaremos algumas das melhores práticas e normas conhecidas e bem aceitas no mercado. Cada uma delas pode trazer benefícios diferenciados para a Administração Pública e podem ser adotadas em conjunto pelo gestor.

1) **COBIT –** ***Control Objectives for Information and related Technology***

Trata-se de um modelo abrangente aplicável para a auditoria e controle de processos de TI, desde o planejamento da tecnologia até a monitoração e auditoria de todos os processos. Será detalhado no item **Erro! Fonte de referência não encontrada.**.

2) **ITIL –** ***Information Technology Infrastructure Library***

A ITIL [67][68][69][70][72][74] 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.

O ITIL surgiu em 1986 com o desenvolvimento do conjunto de mais de 40 livros que abordavam uma variedade de melhores práticas de TI.

A partir de 1999, ITIL versão 2 acrescentou sete livros principais que tratam os processos amplamente aceitos como um *framework* de melhores práticas para Gerenciamento de Serviços de TI (*IT Service Management* - ITSM). É a versão globalmente aceita como uma estrutura de boas práticas para a gestão de serviços de TI, sendo seus principais livros:

- Suporte de Serviços;
- Entrega de Serviços;
- Planejando a implementação da gestão de serviços;
- Gestão da infra-estrutura de Tecnologia de Informação e Comunicações;
- Perspectivas de negócio (Volumes I e II);
- Gerenciamento de aplicações; e
- Gerenciamento de segurança.

Em 2007, transcorridos 21 anos, surge o ITIL Versão 3 [74], que consiste de cinco livros principais e um livro oficial de introdução. Baseados em ciclos de vida das boas práticas de serviços, eles incorporam o que há de mais importante nas versões 1 e 2 e melhores práticas atuais para a gestão de serviços de TI. Cinco títulos de ciclo de vida formam o núcleo das práticas do ITIL:

- Estratégias de Serviços;
- Desenho de Serviços;

- Transição de Serviços;
- Operação de Serviços; e
- Melhoria Contínua de Serviços.

3) PMBOK – *Project Management Body Of Knowledge*

Trata-se de uma base de conhecimento em gestão de projetos e será melhor descrito no item 3.6.

4) PRINCE2 – Projects in Controlled Environments 2

Trata-se de uma metodologia de gerenciamento de projetos também mantida pelo atual OGC (*Office of Government Commerce*). Esta metodologia encontra-se em sua quarta versão, lançada em 2005, e é o padrão usado atualmente pelo governo britânico.

O modelo PRINCE2 [66][71] é composto por oito processos gerenciais distintos, oito componentes e três técnicas que buscam fornecer um método que possa ser repetido e ensinado, que assegure a previsão do que esperar dos projetos (onde, como e quando), que permita que o gerente de projeto seja proativo e que forneça um guia consistente que facilite planejamento, controle e comunicação no âmbito do projeto.

5) ABNT NBR ISO/IEC 27001:2006

Sob o título de "Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos", esta norma [10] é a tradução literal da norma ISO/IEC 27001 que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Esta norma é detalhada no item 3.7.1.

6) ABNT NBR ISO/IEC 17799:2005

Sob o título de Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, esta norma [9] é a tradução literal da ISO/IEC 17799:2005 (atualmente ISO/IEC 27002) e estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. Esta norma é detalhada no item 3.7.2.

7) ISO/IEC 15408:2005

Sob o título de *Common Criteria for Information Technology Security Evaluation* (Critérios comuns para avaliação de segurança da tecnologia da informação), esta norma [38][39][40], dividida em três partes, define critérios para a avaliação de segurança de produtos e sistemas de TI, auxilia análise de risco e tomada de decisão de consumidores.

Funciona com um guia o desenvolvimento de produtos e sistemas seguros, sendo aplicável a medidas de segurança em *hardware*, *firmware* ou *software*, abrangendo, entre outros, sistemas operacionais, redes, sistemas distribuídos e aplicações.

Assim, pode ser utilizada como detalhamento de implantação de controles relativos ao desenvolvimento de sistemas estabelecidos na ISO/IEC 17799, embora não abranja todos os aspectos desta última.

8) CMMI – Capability Maturity Model Integration

O CMMI [16][17][18] foi criado em 2002 pelo *Software Engineering Institute* (SEI) e tem como objetivo fornecer diretrizes para a melhoria dos processos e habilidades organizacionais, com foco no gerenciamento do desenvolvimento, aquisição e manutenção de produtos e serviços. Para isso, propõe a avaliação da maturidade da organização ou da capacidade das suas áreas de processo, o estabelecimento de prioridades e a implementação de ações de melhoria.

Este modelo possui duas abordagens de implementação: por estágios e contínua. Além disso, possui publicações direcionadas para disciplinas específicas: Engenharia de *Software* (CMMI-SW), Engenharia de Sistemas (CMMI-SE/SW), Desenvolvimento Integrado de Produto e Processo (CMMI-IPPD) e Terceirização (CMMI-SS).

9) NBR ISO/IEC 12207

Sob o título de "Tecnologia da Informação - Processos de ciclo de vida de *software*", esta norma [1] estabelece uma estrutura comum para os processos de ciclo de vida de *software*, com terminologia bem definida, que pode ser referenciada pela indústria de *software*. A estrutura contém processos, atividades e tarefas que servem para ser aplicadas durante a aquisição de um sistema que contém *software*, de um produto de *software* independente ou de um serviço de *software*, e durante o fornecimento, desenvolvimento, operação e manutenção de produtos de *software*.

10) NBR ISO/IEC14598

A NBR ISO/IEC14598-1 [3], sob o título de "Tecnologia da Informação - Avaliação de produto de *software* - Parte 1: Visão geral", esta norma define os termos técnicos utilizados nas demais partes, contém requisitos gerais para especificação e avaliação da qualidade de *software* e esclarece os conceitos gerais. Adicionalmente, também fornece uma estrutura para avaliar a qualidade de quaisquer produtos de *software* e estabelece os requisitos para métodos de medição e avaliação de produtos de *software*.

A NBR ISO/IEC14598-2 [4], sob o título de "Engenharia de *software* - Avaliação de produto - Parte 2: Planejamento e gestão", esta norma fornece requisitos, recomendações e diretrizes para uma função de apoio responsável pela gestão da avaliação de produto de software e pelas tecnologias necessárias para a avaliação de produto de *software*. O papel dessa função de apoio inclui: motivação e treinamento das pessoas para as atividades de avaliação; preparação de documentos e métodos de avaliação adequados e resposta a consultas sobre tecnologias de avaliação.

A NBR ISO/IEC14598-3 [5], sob o título de "Engenharia de *software* - Avaliação de produto - parte 3: Processo para desenvolvedores", esta norma destina-se ao uso durante o desenvolvimento de *software*. Ela é aplicável a todas as atividades de desenvolvimento de *software* que requeiram um processo disciplinado.

A NBR ISO/IEC14598-4 [6], sob o título de "Engenharia de *software* - Avaliação de produto - Parte 4: Processo para adquirentes", esta norma contém requisitos, recomendações e orientações para a medição, julgamento e avaliação sistemática da qualidade de produto de software durante a aquisição de produtos de *software* de prateleira, produtos de *software* sob encomenda ou modificações em produtos de software existentes.

A NBR ISO/IEC14598-5 [7], sob o título de "Tecnologia de informação - Avaliação de produto de software - Parte 5: Processo para avaliadores", esta norma fornece requisitos e recomendações para a implantação prática de avaliação de um produto de *software*, quando várias partes envolvidas necessitam entender, aceitar e confiar nos resultados da avaliação.

A NBR ISO/IEC14598-6 [8], sob o título de "Engenharia de *software* - Avaliação de produto - Parte 6: Documentação de módulos de avaliação", esta norma define a estrutura e o conteúdo da documentação a ser usada para descrever um Módulo de Avaliação (MA).

11) NBR ISO/IEC9126-1

Sob o título de "Engenharia de software - Qualidade de produto - Parte 1: Modelo de qualidade", esta norma **Erro! Fonte de referência não encontrada.** descreve um modelo de qualidade do produto de software, composto de duas partes: a) qualidade interna e qualidade externa e b) qualidade em uso. Sugere a avaliação dos atributos da qualidade do software relacionados a funcionalidade, usabilidade, confiabilidade, eficiência, portabilidade e manutenibilidade.

Esta norma é aplicável para quem faz aquisição e/ou desenvolvimento de software, para usuários e para quem fornece suporte, manutenção ou realiza auditoria de software.

12) MPS.BR

O MPS.BR [101] é um programa para Melhoria de Processo do *Software* Brasileiro coordenado pela Associação para Promoção da Excelência do *Software* Brasileiro (SOFTEX), contando com apoio do Ministério da Ciência e Tecnologia (MCT), da Financiadora de Estudos e Projetos (FINEP) e do Banco Interamericano de Desenvolvimento (BID). Este modelo pode ser exigido em contratos de *outsourcing* junto a pequenas e médias empresas desenvolvedoras de *software*.

O MPS.BR baseia-se nos conceitos de maturidade e capacidade de processo para a avaliação e melhoria da qualidade e produtividade de produtos de *software* e serviços correlatos.

O MPS.BR está dividido em três componentes: Modelo de Referência (MR-MPS), Método de Avaliação (MA-MPS) e Modelo de Negócio (MN-MPS). Cada componente é descrito por meio de guias e/ou de documentos do MPS.BR.

13) BSC – *Balanced Scorecard*

O *Balanced Scorecard* [87] é um sistema de gestão estratégica focado em quatro perspectivas: financeira, cliente, processos internos e aprendizado e crescimento. O BSC auxilia o alinhamento de todas as iniciativas de todos os níveis da empresa com os objetivos e estratégias do negócio e tem como objetivos a tradução da estratégia da empresa em termos operacionais, o alinhamento da organização à estratégia, a transformação da estratégia em tarefas, a conversão da estratégia em processo contínuo e a mobilização da mudança por meio da liderança executiva.

As iniciativas e investimentos necessários são guiados por mapas estratégicos que representam as relações de causa e efeito entre os objetivos estratégicos nas quatro perspectivas envolvidas.

14) Seis Sigma

A metodologia Seis Sigma [73] é uma metodologia de melhoramento da qualidade de processos testada e comprovada para direcionar e obter uma transformação organizacional, reduzindo a variação dentro dos limites definidos pelo cliente. Seis Sigma é, ainda, um processo de melhoria continua que faz com que a organização esteja focada nas necessidades dos clientes, alinhamento de processos, rigor analítico e execução dentro do prazo.

O Seis Sigma tem como meta que um processo apresente não mais do que 3,4 defeitos sobre um milhão de oportunidades, o que equivale a 99,9997% (6 sigmas) de resultados dos processos isentos de defeitos.

15) eSCM

O *eSourcing Capability Model* [92] é um modelo de *outsourcing* criado pelo *Information Technology Services Qualification Center* da *Carnegie Mellon University* que prevê diversos processos, desde a estratégia de negócio até a gestão da contratação. Apresenta três dimensões: ciclo de terceirização, áreas de capacidade e níveis de capacidade. Este modelo está dividido em duas publicações: eSCM-SP para provedores de serviços e eSCM-CL para clientes.

16) Sarbanes-Oxley e Basiléia II

A lei Sarbane-Oxley [90][93] e o Acordo da Basiléia II [19] são regulamentações internacionais com forte impacto na área de TI. A primeira atinge empresas de capital aberto e que têm ações nas bolsas de valores norte-americanas. Já a segunda atinge instituições financeiras.

Motivada por escândalos financeiros corporativos, a lei Sarbanes-Oxley (também conhecida por Sarbox ou SOX) foi assinada em 30 de julho de 2002 e foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores, causada pela aparente insegurança a respeito da governança adequada das empresas.

As seções mais importantes para a TI são a 302 e a 404 que tratam de controles internos. Segundo o livro Implantando a Governança de TI [29], para atender aos requisitos do SOX, as informações financeiras sobre os resultados devem atender aos seguintes princípios:

- O conteúdo da informação deve ser apropriado;
- A informação deve estar disponível no momento em que for necessária;
- A informação é atual ou pelo menos a última disponível;
- Os dados e as informações estão corretos;
- A informação é acessível aos usuários interessados;
- Há um sistema de controle interno sobre relatórios financeiros que garante todos os demais itens anteriores.

Esses requisitos afetam diretamente a TI e a Governança de TI em uma grande variedade de processos.

Já o Acordo da Basiléia II estipula requisitos de capital mínimo para as instituições financeiras, em função de seus riscos de créditos e operacionais. Do ponto de vista da governança corporativa e de TI, o Acordo Basiléia II se aplica à exigência da criação de políticas de gerenciamento de riscos para garantir total segurança, confidencialidade e integridade dos dados de clientes.

17) Normas Internacionais de Auditoria Governamental

As Normas Internacionais de Auditoria costumam abordar os seguintes assuntos:

- Qualificação da equipe;

- Independência dos auditores;
- Zelo profissional;
- Controle de qualidade;
- Planejamento de auditoria;
- Escopo de trabalho;
- Elaboração de relatório.

No âmbito da Auditoria Governamental [91], existem três normas de auditoria desenvolvidas por organismos internacionais:

1) *International Standards for the Professional Practice of Internal Auditing (ISPPIA ou Red Book)* [34] – Padrões Internacionais para a Prática Profissional da Auditoria Interna pelo Instituo de Auditores Internos dos EUA.

2) *International Organization of Supreme Audit Institutions (INTOSAI)* [37]– Organização Internacional de Instituições Superiores de Auditoria. O INTOSAI foi fundado em 1953 e congrega atualmente 170 entidades em todo o mundo. A estrutura geral das normas de auditoria da INTOSAI baseou-se nas Declarações de Lima e de Tóquio, nas declarações e relatórios aprovados pela INTOSAI em vários Congressos e no relatório do Grupo de Especialistas em Contabilidade e Auditorias Públicas dos países em desenvolvimento junto às Nações Unidas.

3) *Generally Accepted Government Auditing Standards (GAGAS ou Yellow Book)* [30]– Padrões de Auditoria Governamental aceitos, editado pelo

Controlador-Geral dos EUA, executivo máximo do GAD (*Government Accountability Office*).

18) Acórdão 1480/2007

Apesar de não ser uma norma, o Acórdão 1480/2007 – Plenário [ANEXO III: ACÓRDÃOS DO TCU] do TCU, publicado no Diário Oficial da União em 03/08/2007, apresenta papel de destaque no processo atual de conscientização da importância do alinhamento da TI ao negócio.

Trata-se de um exame da minuta de instrução normativa encaminhada pela Secretaria de Logística de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MP relativa a modelo de licitação e contratação de serviços de informática em resposta a recomendação do TCU, no Acórdão 786/2006 [ANEXO III: ACÓRDÃOS DO TCU], de que esta Secretaria elaborasse tal modelo voltado para a APF.

A análise realizada pelo TCU é claramente voltada para a Governança de TI e recomenda o uso dos modelos de melhores práticas como: MPS.BR, eSCM-CL, COBIT, ITIL, PMBOK, CMMI, entre outros.

3.4. COBIT

O COBIT - *Control Objectives for Information and Related Technology* (Diretrizes de Controle para Informação e Tecnologia Relacionada) - foi desenvolvido pelo ISACF - *The Information Systems Audit and Control Foundation*, tendo como base a metodologia COSO. Posteriormente, o COBIT passou a ser mantido pelo ITGI - *IT Governance Institute*.

Atualmente, o COBIT encontra-se na versão 4.1. Trata-se de uma estrutura conhecida mundialmente que busca garantir que a Tecnologia de Informação esteja

alinhada aos objetivos corporativos, que os seus recursos sejam usados com responsabilidade e os seus riscos gerenciados apropriadamente.

As atualizações no COBIT 4.1 incluem medida de desempenho aperfeiçoada, melhores objetivos de controle e melhor alinhamento dos negócios e das metas de TI.

A versão 4.1 é baseada nas melhores práticas e padrões reconhecidos internacionalmente, como PMBOK:2000, ITIL:1999-2004, CMM:1993, CMMI:2000, ISO/IEC 17799:2005, entre outros, como pode ser observado na Figura 3.3.

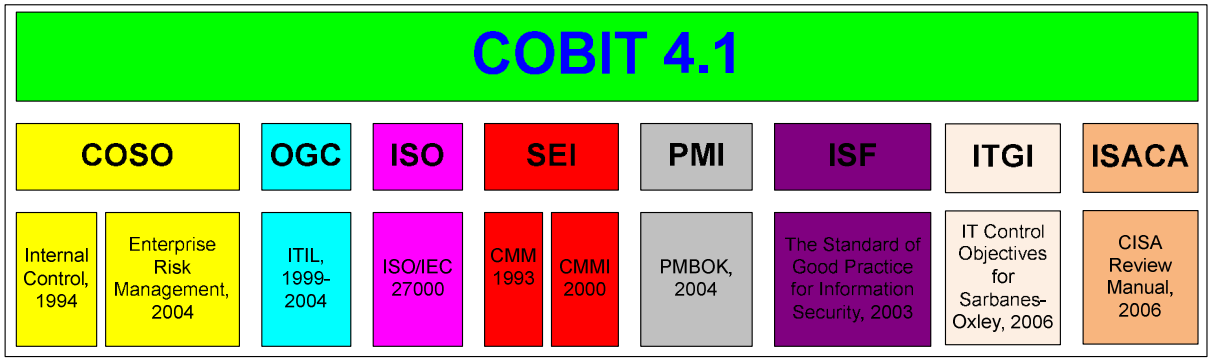

Figura 3.3 – Melhores práticas e padrões abrangidos pelo COBIT.

O ITGI possui várias publicações complementares ao COBIT 4.0 / COBIT 4.1 [44][45][61][42][58][59], sendo que as principais do ponto de vista deste trabalho são:

- *COBIT Control Practices*, (Práticas de Controle COBIT) 2a Edição [46]: Este livro contém prática de controle que melhora e é alinhada ao COBIT 4.1. As práticas de controle são direcionadas para ação e fornecem argumentos de "por que fazê-lo", na forma de valor a ser obtido e riscos a serem evitados.

- *IT Governance Implementation Guide: Using COBIT and Val IT*, (Guia de Implementação da Governança de TI: Usando COBIT e VAL IT) 2a Edição [62]: fornece um mapa detalhado para estabelecer Governança de TI eficiente em uma organização.

- *IT Assurance Guide: Using COBIT* (Guia de Garantia de TI: Usando COBIT)[60]: oferece um guia sobre como o COBIT pode suportar uma grande variedade de atividades de garantia e como a revisão de uma garantia pode ser realizada para cada um dos processos de TI. Esta publicação é detalhada no item 3.5.

- *COBIT Security Baseline*, 2nd Edition [57]: Em fase de atualização, estará disponível apenas em setembro de 2007. Esta publicação foca os passos principais para a implementação da segurança da informação em uma empresa.

- *COBIT Quickstart, 2nd Edition* [56]: Em fase de atualização, estará disponível apenas em setembro de 2007.Esta publicação fornece uma base de controle para pequenas organizações e orienta organizações maiores em seus primeiros passos na direção do controle de seus processos.

A estrutura do COBIT busca atender às necessidades de controle relacionadas à Governança de TI e tem como características:

- Foco nos requisitos de negócio;

- Orientação para uma abordagem de processo;

- Base em controle; e

- Direcionamento para análise de medições e indicadores de desempenho.

3.4.1. Foco nos Requisitos de Negócio

De acordo com o COBIT, a fim de se obter a informação necessária ao atendimento dos objetivos da organização, é necessário que os recursos de TI sejam gerenciados e

controlados, utilizando-se de um conjunto estruturado de processos para garantir a entrega dos serviços de TI requeridos. Os recursos de TI são:

- **Aplicações:** são os sistemas automatizados e procedimentos manuais que processam a informação.

- **Informação:** é o dado em todas as suas formas, como entrada, processado ou como saída de um sistema informatizado, em qualquer forma utilizada pelo negócio.

- **Infra-estrutura:** é a tecnologia e facilidades (isto é, hardware, sistemas operacionais, sistemas de gerenciamento de banco de dados, rede, multimídia, e ambiente) que possibilita o processamento de aplicações.

- **Pessoas:** é o pessoal necessário para planejar, organizar, adquirir, implementar, entregar, dar suporte, monitorar e avaliar os sistemas de informação e serviços. Eles devem ser internos, terceirizados e/ou contratados como necessário.

Esses quatro recursos, juntamente com os processos, formam a arquitetura de TI representada na Figura 3.4. Assim, os processos de TI usam infra-estrutura e pessoal para serem realizados e executam aplicações com a finalidade de entregar informação na forma necessária para atingir os objetivos de negócio.

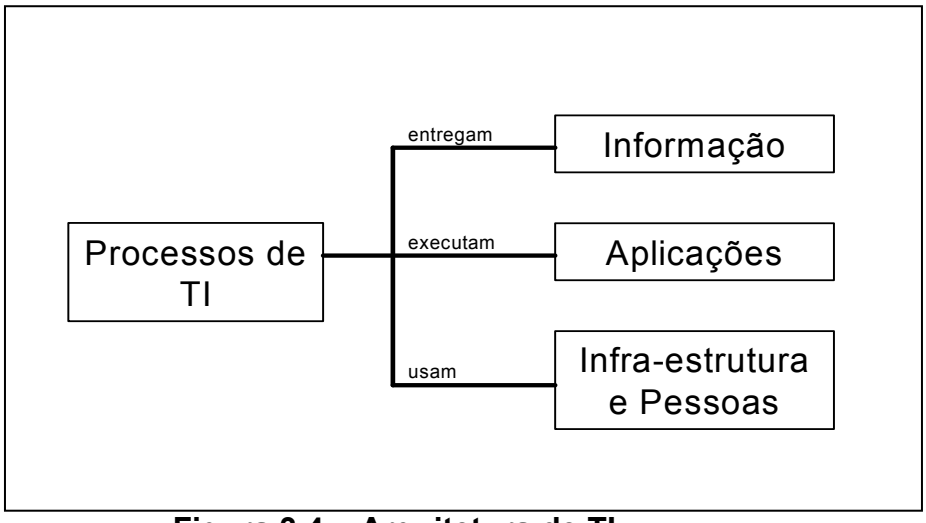

Figura 3.4 – Arquitetura de TI.
Fonte: COBIT 4.1

Os processos do COBIT são constituídos por alguns princípios (Qualidade, Confiança e Segurança) que representam os requisitos de negócio para a informação. Eles são chamados de Critérios da Informação:

- **Efetividade:** Trata-se da capacidade da informação de ser relevante e pertinente ao processo do negócio, bem como de ser entregue de um modo oportuno, correto, consistente e útil.

- **Eficiência:** Diz respeito à provisão da informação através do uso ótimo (mais produtivo e econômico) dos recursos.

- **Confidencialidade:** Diz respeito à proteção da informação sigilosa contra a divulgação não autorizada.

- **Integridade:** Relaciona-se à exatidão e à completeza da informação bem como à sua validade de acordo com os valores e expectativas do negócio.

- **Disponibilidade:** Relaciona-se à disponibilização da informação quando requerida pelo processo de negócio. Também diz respeito à salvaguarda dos recursos necessários e potencialidades associadas.

- **Conformidade:** Trata-se do cumprimento das leis, dos regulamentos e arranjos contratuais aos quais o processo de negócio está sujeito, i.e., critérios de negócio impostos externamente bem como políticas internas.

- **Confiabilidade:** Relaciona-se à provisão de informação apropriada para a gerência operar a entidade e exercer suas responsabilidades fiduciárias e de governança.

O grau de importância de cada um desses critérios é uma função do negócio e do ambiente em que a organização opera. Numa avaliação de riscos, esses critérios atribuem

pesos diferentes aos processos do COBIT, em função da importância no alcance dos respectivos Objetivos de Controle.

3.4.2. Orientação para Processos

Os componentes do COBIT são utilizados para fazer com que a TI seja orientada aos objetivos do negócio e cumpra seu papel na instituição. Para tanto, as boas práticas do COBIT são organizadas em processos, cada qual visando um Objetivo de Controle.

O COBIT identifica um conjunto de 210 Objetivos Controles, organizados em 34 Processos que são agrupados em 4 Domínios, aplicáveis aos sistemas e à Tecnologia da Informação.

Um objetivo de controle é definido como uma declaração de um propósito ou resultado desejado a ser alcançado, por meio da implementação de controles em determinada atividade de TI. Esses objetivos de controle, se atingidos por meio da implementação eficaz dos respectivos controles, garantem o alinhamento da TI aos objetivos do negócio e que eventos indesejáveis sejam prevenidos, apagados ou corrigidos. A responsabilidade pelo sucesso dos sistemas de controles é, portanto, da alta direção, a qual deve torná-los efetivos. Assim, são responsáveis por:

- Selecionar os objetivos de controle aplicáveis;
- Balancear o investimento necessário para implementar as práticas de gerenciamento necessárias para alcançar cada objetivo de controle com o risco de não alcançá-lo.
- Decidir quais práticas de controle implementar; e
- Escolher como implementar cada prática de controle.

Os mais de 200 objetivos de controle do COBIT definem o que é necessário ser gerenciado em cada processo de TI para mapear requisitos de negócio e riscos de gerenciamento. Eles ajudam a definir políticas claras, adotar boas práticas para controles de TI e encorajar a posse dos processos. Eles também provêm um ponto de referência para ligar boas práticas aos requisitos de negócio, podendo ser integrado a outros padrões e práticas que focam em área específicas.

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.

Na Figura 2.1, podem ser identificados os domínios do COBIT (Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, e Monitoramento), que integram um ciclo de vida repetível no sistema de gestão de TI.

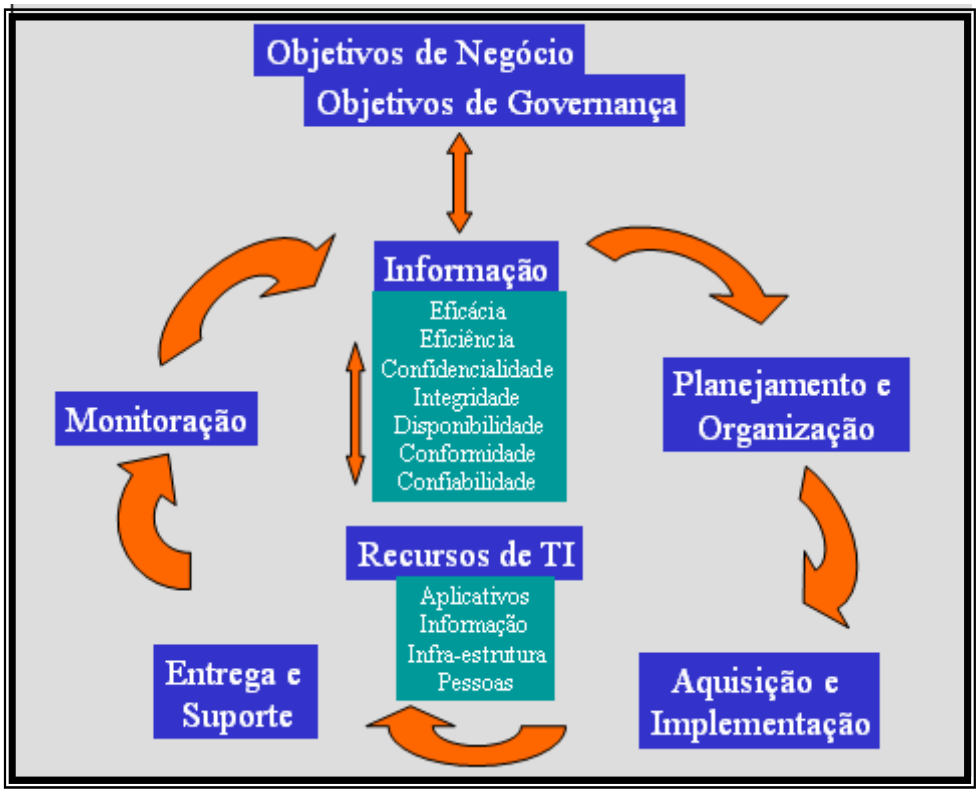

Figura 3.5 - *Framework* do COBIT
Adaptado do Cobit 4.1

Os 34 processos que fazem parte destes domínios são identificados na tabela do ANEXO V: TABELA COBIT. Esta tabela também possui um mapeamento relativo aos critérios de informação e recursos de TI envolvidos nos processos.

Cada processo possui um mapa demonstrando os critérios da informação e recursos de TI envolvidos, o domínio a que pertence, a área de Governança de TI focada, os principais objetivos e a métrica usada para medição. A Figura 3.6 mostra a forma de navegação no mapa de cada processo.

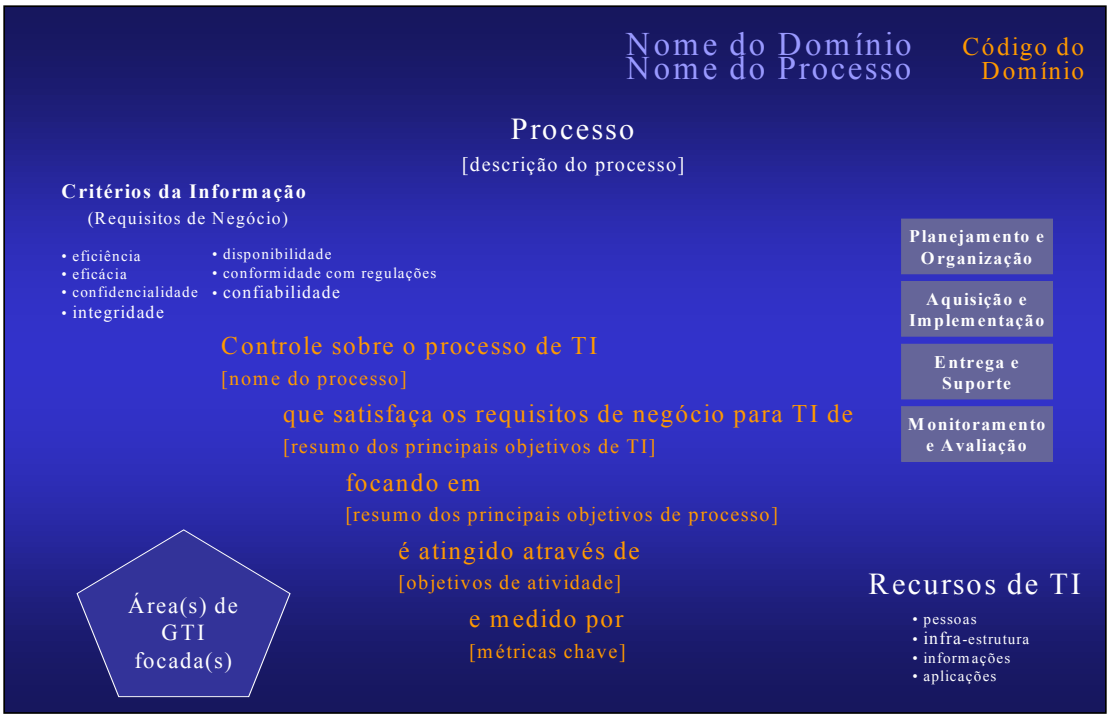

Figura 3.6 – Navegação na descrição dos Processos do COBIT

3.4.3. Base em Controle

Para cada processo são definidos objetivos de controle que definem um resultado esperado ou um propósito a ser atingido pela implementação de procedimentos de controle em uma atividade de TI específica. Os objetivos de controle do COBIT representam os requisitos mínimos necessários para que se possam controlar os processos de TI de forma eficaz.

Assim, colhem-se informações de controle da operação de cada processo de TI e as compara aos objetivos de controle. Caso haja necessidade, são tomadas medidas preventivas ou corretivas.

A fim de ajudar neste processo de avaliação de controles, para cada processo, o COBIT detalha os objetivos de controle, informa as entradas e saídas do processo e define a matriz RACI de papéis e responsabilidade.

3.4.4. Direcionamento para Medições e Indicadores

A análise de medições e o uso de indicadores de desempenho são necessários para que a organização conheça sua situação atual, compare com padrões de mercado ou com organizações similares, identifique as melhorias necessárias e monitore tais melhorias.

Esse processo de autoconhecimento e melhoria da organização pode ser subsidiado pela análise de maturidade dos processos e pela avaliação de indicadores.

O Modelo de Maturidade de Governança (Figura 3.2) 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 de acordo com os níveis apresentados na

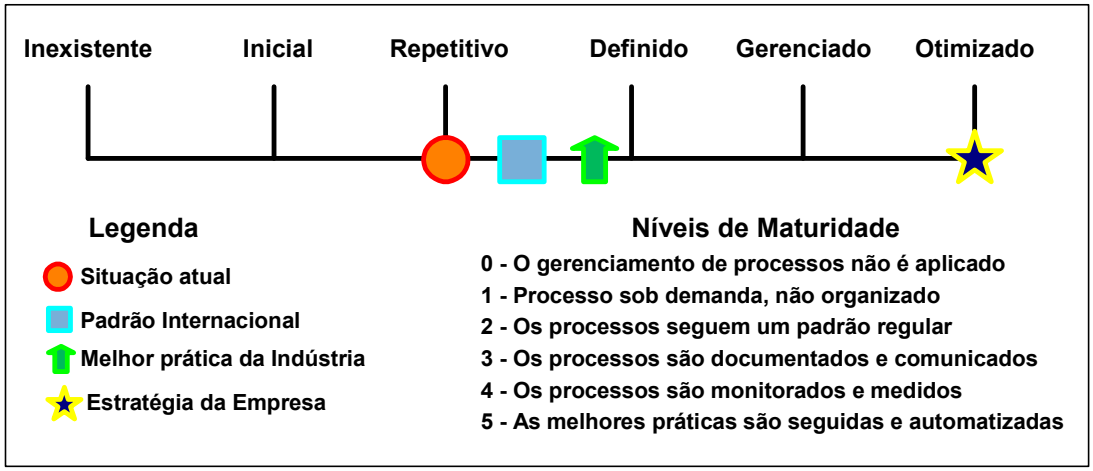

Figura 3.7:

Figura 3.7 – Modelo de Maturidade do COBIT
Adaptado do Cobit 4.1

A maturidade deve ser avaliada em cada um dos processos. O nível ótimo correspondente é determinado individualmente, de acordo com a natureza da instituição, ameaças e oportunidades viabilizadas por TI. O COBIT fornece orientações específicas para cada processo do que deve ser trabalhado para atingir determinado nível de maturidade.

O COBIT também oferece métricas para a medição dos objetivos. Existem dois tipos de métricas:

- Medidas de saídas: Indicam se os objetivos foram alcançados, podendo ser usada somente após o acontecimento do fato.

- Indicadores de desempenho: Indicam a probabilidade de se alcançar os objetivos por medições realizadas antes da geração de saídas.

Esses dois tipos de métricas podem ser usados para analisar objetivos de negócio, de TI, de processo e de atividade, medindo suas saídas e desempenhos.

3.5. IT ASSURANCE GUIDE

O *IT Assurance Guide* [60] é uma publicação que substitui o *COBIT Audit Guidelines* (Diretrizes de Auditoria do COBIT) [43]. Trata-se de um guia de atividades de garantia e revisão de processos de TI. O termo garantia é usado, pois é uma publicação que pode ser usada não apenas por auditores, mas por quaisquer profissionais que necessitem fazer avaliações e revisões de processos. Entretanto, neste trabalho, a utilizaremos apenas com o foco de auditoria.

O objetivo deste guia não é prover um programa detalhado de garantia que possa ser usado como é e executado. A intenção é que um profissional de garantia com alguma experiência use este manual como base para um desenvolvimento eficiente de programas de garantia customizados que possam ser usados e executados por membros da equipe com menos experiência. Dessa forma, antes de ser utilizado, os passos de teste devem ser adequados para a realidade da organização e para os objetivos da iniciativa de garantia.

Este guia é organizado acerca dos 34 processos COBIT e contém os seguintes componentes mostrados na Figura 3.8:

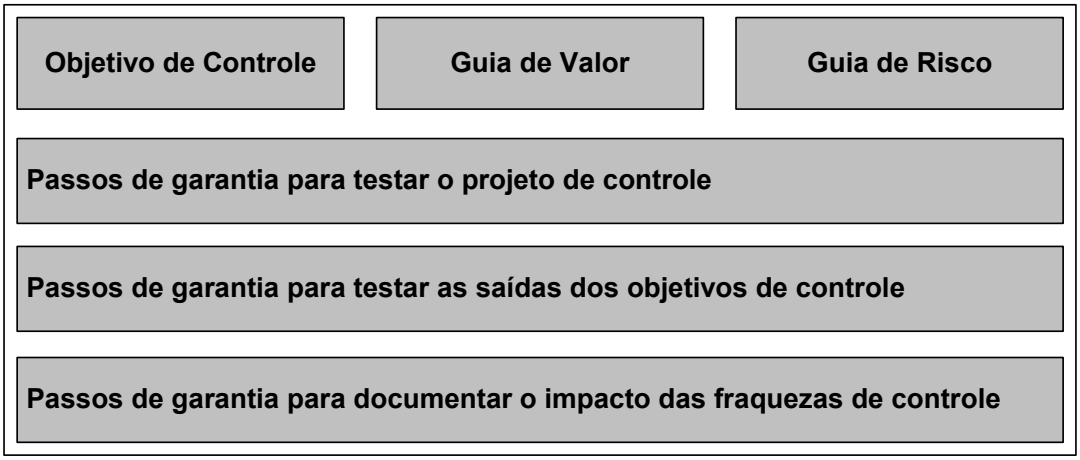

Figura 3.8 – Componentes do *IT Assurance Guide*

a) Objetivos de Controle

Objetivos de Controle de TI são os objetivos levantados pelo COBIT 4.0 e referem-se aos requisitos e finalidades a serem alcançados pela implementação de práticas de controle em um processo de TI e geralmente diretamente relacionado a atividades específicas dentro do processo.

b) Guias de Valor e de Risco

Os Guias de Risco e de Valor provêm entradas valiosas para profissionais usarem na comunicação de justificativas de negócio para alcançar objetivos de controle específicos

e implementar as práticas de controle associadas a eles. O Guia de Valor destaca os pontos importantes de valores que podem ser agregados com a implementação do controle. Já o Guia de Risco destaca riscos que podem ser evitados com tal implementação.

c) Passos de testes de garantia

Os passos de testes de garantia provêm um guia em nível de objetivos de controle para a condução de um processo de auditoria (ou qualquer outra atividade de garantia). Os passos são derivados das práticas de controle que, por sua vez, são derivados de cada objetivos de controle. Tais passos permitem a avaliação do projeto de controles, a confirmação de que são colocados em operação e a estimativa da efetividade operacional de cada controle.

Passos de garantia genéricos cobrem a existência e efetividade de projeto do projeto de controle proposto bem como as responsabilidades associadas. Os passos de garantia específicos testam a efetividade operacional dos controles e estão no nível de objetivo de controle. Além disso, passos de garantia são providos para testar as fraquezas e falhas das saídas dos controles.

A combinação de todos os componentes de garantia provê um método de teste para ajudar a formar opiniões acerca dos objetivos de garantia. Entretanto, este método não provê descrições de soluções específicas. Por isso, guias mais detalhados devem ser obtidos de padrões e melhores práticas específicos e relevantes, como o ITIL e normas ISO.

3.6. PMBOK

O *Project Management Body of Knowledge* - PMBOK (2004) [95], elaborado pelo *Project Management Institute* (PMI), é um conjunto de conhecimentos em gestão de projetos amplamente reconhecidos como boas práticas. 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.

O modelo é constituído de nove áreas de conhecimento em gerenciamento de projetos distribuídas em cinco processos. As áreas de conhecimento ao agrupamento de atividades correlacionadas em relação ao conteúdo de suas atividades.

As áreas de conhecimento podem ser visualizadas na Figura 3.9:

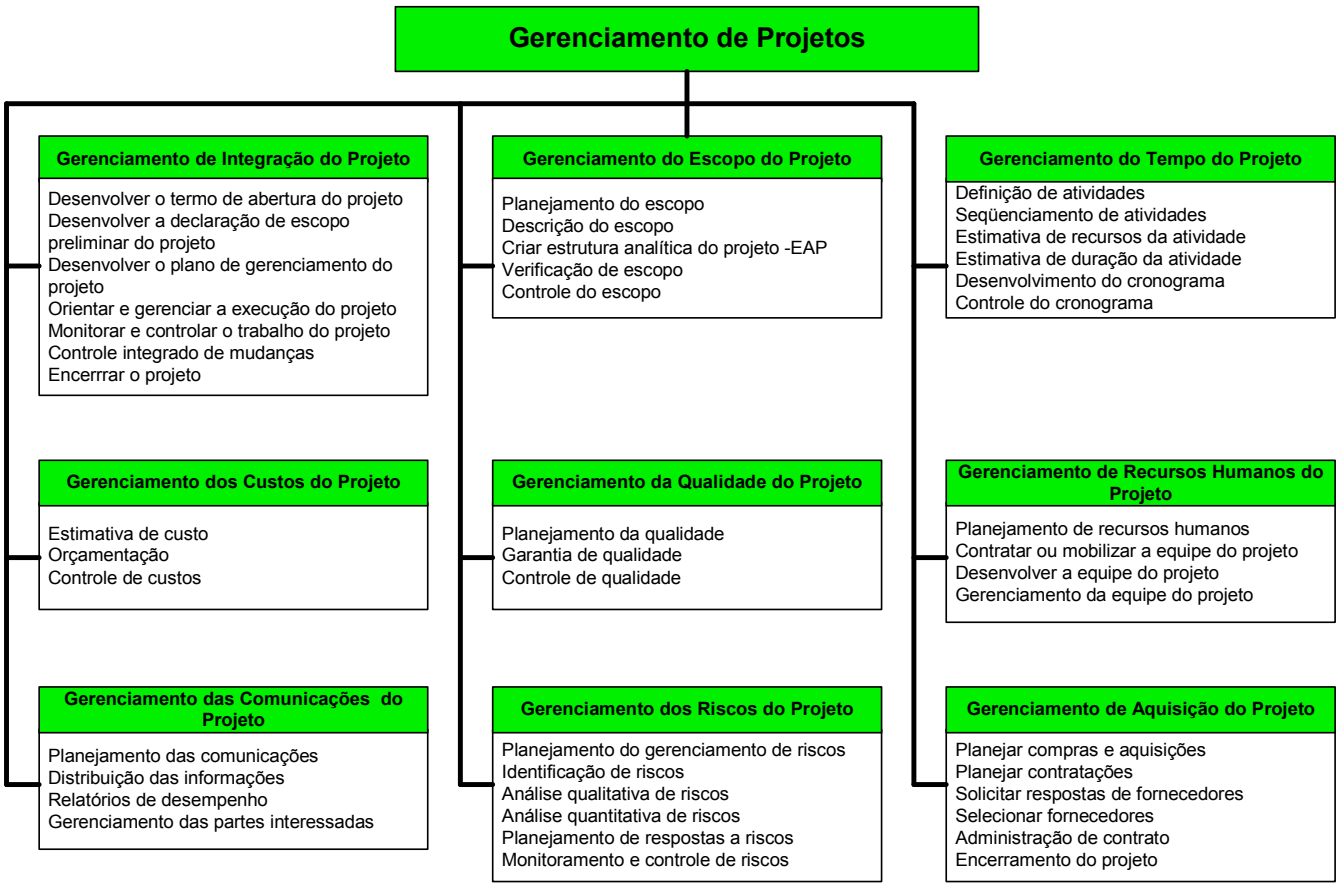

Figura 3.9 – Áreas de Conhecimento do PMBOK
Fonte: PMBOK

Já os processos de gerenciamento de projetos referem-se ao agrupamento das mesmas atividades, mas em relação à etapa em que elas ocorrem. O conjunto de cinco grupos refere-se a todas as etapas de um projeto ou de uma fase de projeto, ou seja, ao

mesmo tempo em que cada grupo é aplicado ao projeto como um topo, também é recomendável que sejam aplicados em cada fase do projeto. A definição de cada grupo é apresentada na Tabela 3.2.

Tabela 3.2 – Grupos de Processos de Gerenciamento de Projetos

Grupo de Processos	Definição
INICIAÇÃO	Conjunto de atividades que define e autoriza formalmente o início do projeto ou de uma fase.
PLANEJAMENTO	Conjunto de atividades que define e refina os objetivos e possibilita o planejamento de que cada área de conhecimento a fim de alcançar os objetivos e escopo do projeto ou fase. Esta fase tem como saídas artefatos importantes como: o plano de gerenciamento do projeto; os planos de gerenciamento de escopo, riscos, qualidade, comunicações, aquisições, recursos humanos etc.
EXECUÇÃO	Conjunto de atividades voltadas para a realização do trabalho definido pelo plano de gerenciamento do projeto por meio da integração de pessoas e outros recursos e sempre observando os requisitos de produto e de projeto.
MONITORAMENTO E CONTROLE	Conjunto de atividades responsáveis pela medição e monitoramento do desempenho do projeto quando comparada ao seu plano de gerenciamento, de forma a realizar ações corretivas quando necessárias e garantir a implantação de mudanças aprovadas.
ENCERRAMENTO	Conjunto de atividades destinadas à finalização formal do projeto ou de uma fase, de forma a entregar o produto terminado ou encerrar um projeto cancelado.

A relação entre os grupos pode ser visualizada na Figura 3.10:

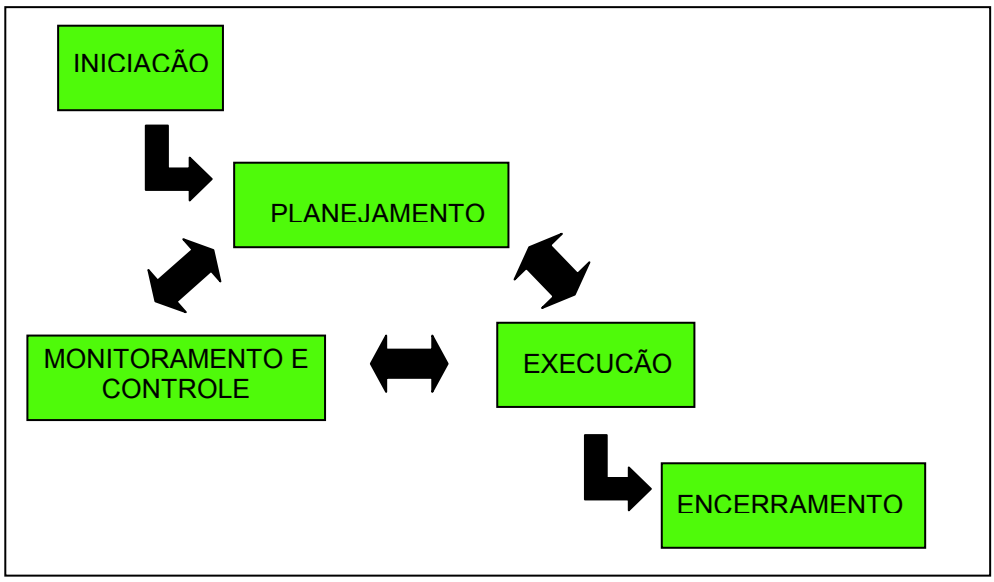

Figura 3.10 - Relação entre os Grupos de Processos

3.7. SEGURANÇA DA INFORMAÇÃO

As principais normas internacionais relacionadas à segurança da informação são a ISO/IEC 27001:2005 e a ISO/IEC 17799:2005.

Estas normas se originaram da norma do Governo Britânico *British Standard* (BS) 7799. Em 1995, foi publicada a primeira versão da BS 7799-1 (BS 7799-1:1995 - Tecnologia da Informação - Código de prática para gestão da segurança da informação). Em 1998, foi publicada a primeira versão da BS 7799-2 (BS 7799-2:1998 - Sistema de gestão da Segurança da Informação - Especificações e guia para uso). A partir daí, estas normas passaram por processos de revisão, se tornaram normas ISO/IEC 17799 e ISO/IEC 27001, respectivamente, e evoluíram até a versão atual.

Em setembro de 2005, foi publicada, no Brasil, a segunda versão da norma NBR ISO/IEC 17799 (Tecnologia da Informação - Código de prática para gestão da segurança da informação), tradução literal da norma ISO.

Em Outubro de 2005, foi publicada a norma ISO 27001 (ISO/IEC 27001:2005 - Tecnologia da Informação - Técnicas de segurança - Sistema de gestão da Segurança da Informação - Requisitos).

Neste ano, a ISO (*International Organization for Standardization*) e o IEC (*International Eletrotechnical Comission*) lançaram a série 27000, em que, além da ISO/IEC 27001, contempla a ISO/IEC 27002 (em substituição à ISO 17799) e a ISO/IEC 27004 (que focará a melhoria contínua do sistema de gestão da segurança da informação).

Neste trabalho, faremos um pequeno resumo da ISO/IEC 27001 e da NBR ISO/IEC 17799:2005. Entretanto, apenas esta será usada no desenvolvimento de procedimentos deste trabalho.

3.7.1. NBR ISO/IEC 27001:2005

A NBR ISO/IEC 27001 [10] visa prover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão da Segurança da Informação - SGSI (ISMS – *Information Security Management System*). Utiliza uma abordagem de processo para a gestão da segurança da informação.

O texto da norma é subdividido em cinco seções:

- O Sistema de Gestão da Segurança da Informação;
- A responsabilidade da administração;
- As auditorias internas do SGSI;
- A revisão do SGSI; e
- A melhoria do SGSI.

A seção sobre **O Sistema de Gestão da Segurança da Informação** (Figura 3.11) trata do ciclo PDCA (Plan/Planejar – Do/Fazer – Check/Checar – Act/Agir) e dos requisitos da documentação por meio de algumas diretrizes divididas nos seguintes tópicos: o estabelecimento do SGSI, a implementação e operação do SGSI, monitoramento e revisão do SGSI, manutenção e melhoria do SGSI e requisitos de documentação.

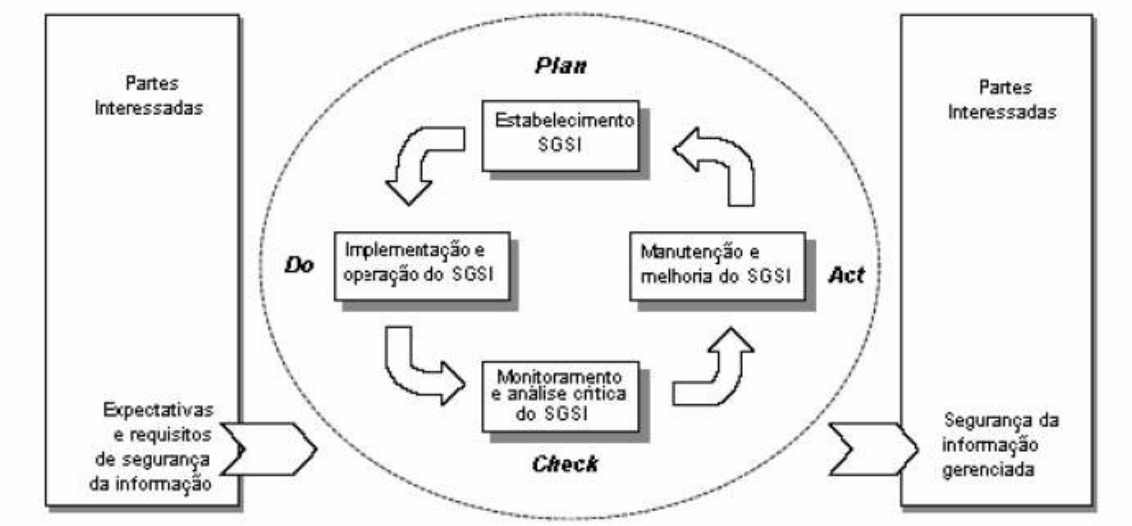

Figura 3.11 – Sistema de Gestão da Segurança da Informação
Fonte: NBR ISO/IEC 27001

A Tabela 3.3, retirada da norma, traz uma breve descrição de cada tópico:

Tabela 3.3 – Descrição das fases do SGSI
Fonte: NBR ISO/IEC 27001

Plan (Planejar) (estabelecer o SGSI)	Estabelecer política do SGSI, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação para entregar resultados conforme as políticas globais de uma organização e objetivos.
Do (Fazer) (implementar e operar o SGSI)	Implementar e operar a política do SGSI, controles, processos e procedimentos.
Check (Checar) (monitorar e revisar o SGSI)	Avaliar e, onde aplicável, medir o desempenho de um processo contra a política do SGSI, objetivos e experiência prática e relatar os resultados para a gerência para revisão.
Act (Agir) (manter e melhorar o SGSI)	Tomar as ações corretivas e preventivas, baseado nos resultados da auditoria interna do SGSI e revisão gerencial ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Já em **A responsabilidade da administração**, aborda-se a necessidade de haver evidência do compromisso da administração com o estabelecimento, implementação, operação, monitoramento, revisão e manutenção e melhoria do SGSI.

De acordo com a seção **As auditorias internas do SGSI**, a organização deve conduzir as auditorias internas do SGSI de forma a verificar a conformidade (com a norma e demais requisitos), a implementação e manutenção efetivos e o desempenho das atividades de controle, dos controles, dos processos e dos procedimentos do sistema.

A revisão do SGSI estabelece que a administração deve rever, pelo menos uma vez por ano, o SGSI para assegurar sua contínua adequação e eficácia. Nesta seção, são definidas as entradas da revisão e as saídas esperadas.

Na seção **A melhoria do SGSI,** define-se que a organização deve melhorar continuamente a eficácia do SGSI, por meio de ações corretivas e preventivas, revisões gerenciais, resultados de auditoria, entre outras atividades.

3.7.2. NBR ISO/IEC 17799:2005

A NBR ISO/IEC 17799 **Erro! Fonte de referência não encontrada.** estabelece diretrizes e princípios gerais para iniciar, manter e melhorar a gestão da segurança da informação em uma organização.

O objetivo da norma não é detalhar procedimentos de configuração, mas identificar os pontos de partida para a constituição de uma gestão de segurança da informação eficaz por meio de recomendações que se traduzem sob a forma de controles. Assim, servindo como um guia prático para desenvolver os procedimentos de segurança da informação e práticas eficientes de gestão de segurança para a organização.

Esta norma contém 11 seções de controles de segurança da informação, que juntas totalizam 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos.

Cada seção contém um número de categorias principais de segurança da informação. Cada categoria principal de segurança da informação contém um objetivo de controle que define o que deve ser alcançado e um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

As descrições dos controles estão estruturadas da seguinte forma:

i. Controle

Define qual o controle específico para atender ao objetivo do controle.

ii. Diretrizes para a implementação

Contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. Algumas destas diretrizes podem não ser adequadas em todos os casos e assim outras formas de implementação do controle podem ser mais apropriadas.

iii. Informações adicionais

Contém informações adicionais que podem ser consideradas, como, por exemplo, considerações legais e referências a outras normas.

A Tabela 3.4 apresenta as 11 seções e seus respectivos assuntos:

Tabela 3.4 – Controle de Segurança da Informação

Seção	Assunto
Política de Segurança	Descreve a estrutura do documento de Política de Segurança, análise crítica e avaliação.

Segurança Organizacional	Aborda a infra-estrutura de segurança, o controle de acesso dos prestadores de serviço e o estabelecimento de responsabilidades e caso de terceirização.
Classificação e Controle de Ativos de Informação	Detalha a contabilização e o registro de ativos e a classificação de informação.
Segurança de Pessoas	Foca o risco decorrente de atos intencionais ou acidentais realizados por pessoas. Além disso, aborda a inclusão de responsabilidades relativas à segurança da informação na descrição de cargos, a forma de contratação e o treinamento em segurança.
Segurança Física e Ambiental	Define áreas de segurança, segurança dos equipamentos e controles gerais.
Gerenciamento das Operações	Aborda procedimentos e responsabilidades operacionais, planejamento e aceitação dos sistemas, proteção contra *softwares* maliciosos, salvamento e recuperação de dados, gerenciamento de rede, segurança e tratamento de mídias, troca de informações e software.
Controle de Acesso	Aborda requisitos do negócio para controle de acesso, gerenciamento de acessos de usuários, responsabilidade do usuário, controle de acesso à rede, controle de acesso ao sistema operacional, controle de acesso às aplicações, monitoração do uso e acesso aos sistemas, computação móvel e acesso remoto.
Desenvolvimento e Manutenção de Sistemas	Aborda requisitos de segurança de sistemas, segurança de sistemas de aplicação, controles de criptografia, segurança de arquivos do sistema.
Gestão de Incidentes de Segurança	Aborda a notificação de fragilidades e eventos de segurança da informação e a gestão de incidentes de segurança da informação e melhorias.
Gestão de Continuidade do Negócio	Aborda processo de gestão, continuidade de negócio e análise de impacto, documentação e implementação do plano de continuidade, estrutura do plano de continuidade dos negócios, testes, manutenção e reavaliação dos planos de continuidade.
Conformidade	Aborda a necessidade de conformidade com requisitos legais, análise crítica da política de segurança e da conformidade técnica, considerações quanto à auditoria de sistemas.

4. METODOLOGIA DE AUDITORIA DE TI

Uma metodologia completa de Auditoria de TI dá parâmetros para a realização da Auditoria em todas as suas fases e funciona como um facilitador para o desenvolvimento de práticas e procedimentos a serem aplicados durante a execução do processo.

Para que se tenha como resultado essa metodologia, devem-se conciliar as melhores práticas e normas de TI conhecidas no mercado, a legislação brasileira e as normas de auditoria. A partir daí, deve-se compilar e adaptar todas essas variáveis à necessidade da Administração Pública e seus princípios, de forma a gerar uma metodologia simples e aplicável na prática. Este modelo pode ser visualizado na Figura 4.1.

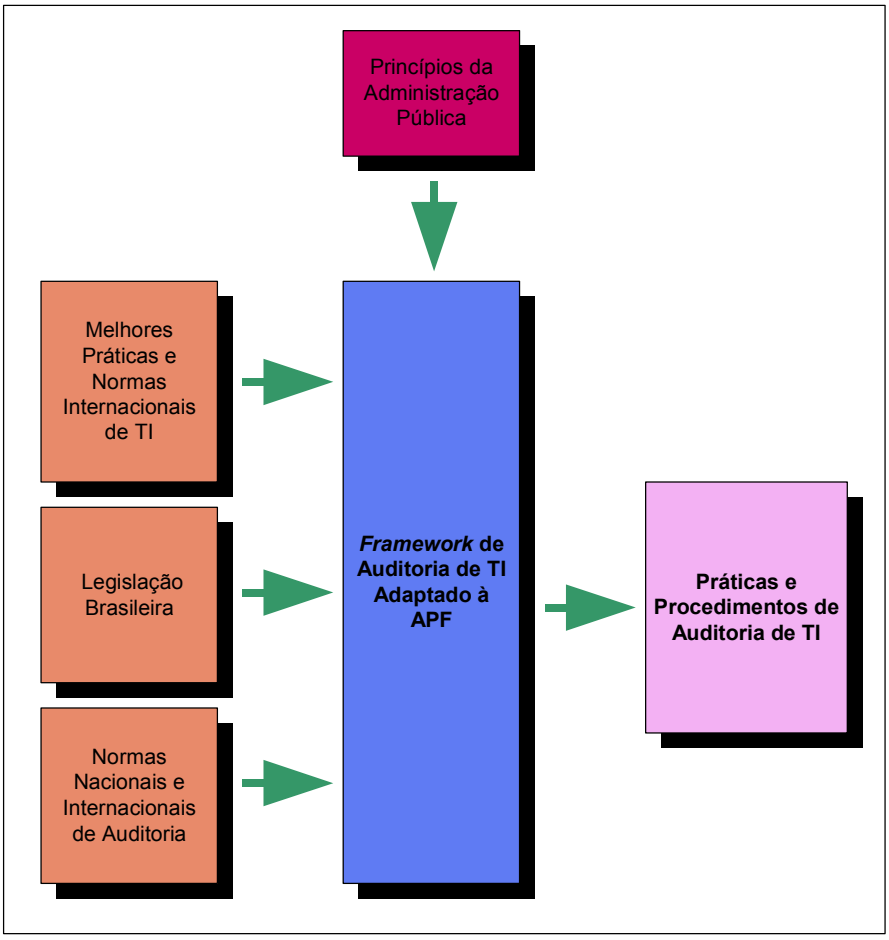

Figura 4.1 – Metodologia de Auditoria de TI

As melhores práticas do mercado foram descritas no capítulo anterior e são detalhadas, de acordo com a necessidade, no decorrer da descrição da metodologia.

A legislação brasileira utilizada refere-se tanto às normas relacionadas ao Sistema de Controle Interno e Externo brasileiro (ANEXO I: LEGISLAÇÃO DE CONTROLE) quanto às normas pertinentes ao uso da informação e da tecnologia relacionada (ANEXO II: LEGISLAÇÃO APLICÁVEL À TI).

As normas nacionais e internacionais específicas de auditoria **Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.Erro! Fonte de referência não encontrada.** também são entradas deste processo, mas não serão diretamente abordadas neste trabalho. Apesar de utilizadas em vários momentos, as normas de auditoria interna **Erro! Fonte de referência não encontrada.** e independente **Erro! Fonte de referência não encontrada.** não serão detalhadas, mas podem ser facilmente compreendidas com uma breve leitura e devem ser utilizadas, no que couber, para conduzir uma auditoria.

Os principais princípios da Administração Pública são explicados item 2.2 deste trabalho e consistem em legalidade, moralidade, impessoalidade, publicidade, eficiência, supremacia do interesse público, indisponibilidade, continuidade dos serviços públicos e autotutela.

O *Framework* de Auditoria de TI adaptado à Administração Pública Federal é uma adaptação de melhores práticas de auditoria nacionais e internacionais voltadas à TI de forma a produzir um guia de práticas de auditoria e de desenvolvimento de procedimentos simplificados e aplicáveis à prática.

Utilizamos os conceitos de Gerência de Projetos para melhor gerenciar os trabalhos de auditoria. Entretanto, a espinha dorsal desse *Framework* é o COBIT 4.1 e o Guia de

Auditoria do COBIT (*IT Assurance Guide*) que são detalhados no item **Erro! Fonte de referência não encontrada.** deste trabalho.

Neste capítulo, fazemos uma apresentação geral de conceitos, técnicas e práticas utilizados em auditorias de TI e dividimos o processo em fases, detalhando cada uma. As atividades de cada fase tiveram como base principal o *IT Assurance Guide*. Já divisão das fases foi feita de forma a atender melhor a necessidade da APF e se adaptar à forma de auditorias comuns já realizadas pela Administração.

A metodologia de desenvolvimento de Procedimentos de Auditoria de TI, resultado deste trabalho e detalhada no Capítulo 5, é uma proposta que visa:

a) Dar direção ao trabalho do auditor: o uso do Cobit como base possibilita que o auditor deixe de abordar algum controle por vontade própria e não por desconhecimento ou esquecimento.

b) Contribuir para a padronização do processo dentro da organização: a metodologia, por obrigar que se escolham padrões e modelos conhecidos nacional e internacionalmente, faz com que a organização auditora tenha que definir e decidir por tais padrões.

c) Gerar uma linguagem comum entre auditor e auditado: como já dito anteriormente, a escolha de padrões e modelos ajuda na criação de uma linguagem comum, já que o auditado também tem acesso no mercado aos controles utilizados pelo auditor.

d) Demonstrar como os padrões podem ser relacionados para serem usados nas auditorias: o excesso de padrões e modelos muitas vezes traz dificuldades para o auditor escolhê-los e usá-los. O modelo mostra como eles podem ser relacionados a partir de um nível mais abstrato e genérico a um nível mais técnico.

4.1. AUDITORIA DE TI SOB A VISÃO DE PROJETO

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.

Devido à diversidade das áreas de Auditoria de TI (vide item 2.3), às peculiaridades de cada ambiente auditado e à vasta possibilidade de definição de escopos, sugerimos que cada auditoria seja tratada como um projeto.

Segundo o PMBOK 2004, "um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo". Na mesma linha, de acordo a ABNT, na norma NBR 10006, 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".

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 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 analisarmos 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.

A elaboração progressiva é uma característica de projetos que integra os conceitos detemporário e exclusivo. Elaboração progressiva significa desenvolver em etapas e

continuar por incrementos. Por exemplo, o escopo de uma auditoria é descrito de maneira geral no início do projeto e se tornará mais explícito e detalhado conforme a equipe do projeto desenvolve um entendimento mais completo do objeto auditado, dos pontos críticos e dos objetivos de controle essenciais.

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 [95][66].

Além disso, pode ser criado, dentro da organização auditora, um escritório de projetos (*Project Management Office* - PMO) de Auditoria de TI.

De acordo com o PMBOK, um escritório de projetos (PMO) é uma unidade organizacional que centraliza e coordena o gerenciamento de projetos sob seu domínio. 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.

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 *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 ocorrem 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 departamentos isolados, e facilitaria a padronização de diretrizes e linguagem dentro do órgão de controle.

4.2. DIRETRIZES GERAIS DE AUDITORIA

4.2.1. Atividades Essenciais da Auditoria

Todo o processo de auditoria resume-se à obtenção de entendimento do objeto auditado de forma a conhecer os riscos relacionados e as medidas de controle relevantes, avaliação da adequação de tais controles, avaliação do funcionamento destes controles e substanciação do risco destes objetivos de controle não serem atingidos e suas potenciais e reais conseqüências, conforme Figura 4.2.

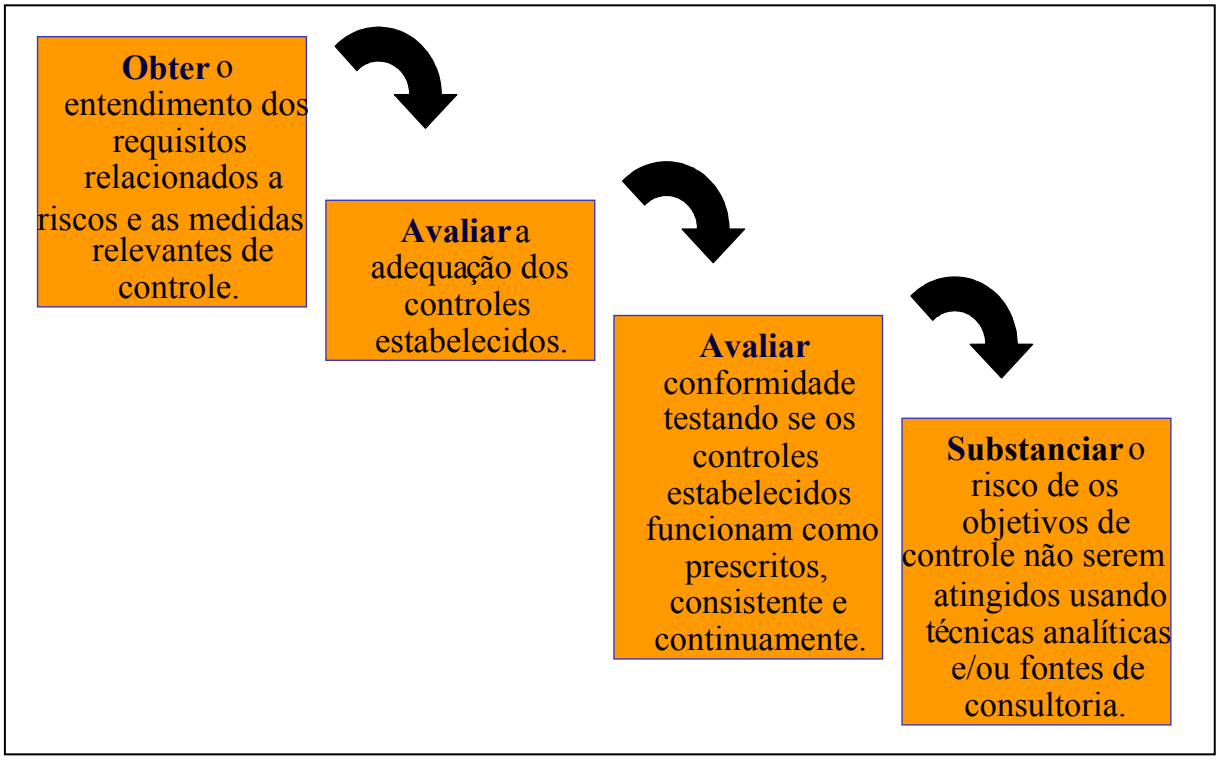

Figura 4.2 – Atividades Essenciais da Auditoria

4.2.2. Análise de Riscos

O "Livro Laranja" [105] define Risco como sendo um resultado incerto, que pode ser uma oportunidade positiva ou uma ameaça negativa, de ações e eventos. O risco deve ser avaliado no que diz respeito à combinação entre a probabilidade de ocorrência e o impacto resultando no caso do evento realmente acontecer.

As organizações devem ser capazes de gerenciar riscos, ou seja, identificá-los, avaliá-los e dar a eles o tratamento mais adequado. O *Risk Management Guide for Information Technology Systems* [102] é um guia de gerenciamento de riscos para Sistemas de TI publicado pelo Instituto Nacional de Padrões e Tecnologias (*NIST – National Institute of Standards and Technology*) dos Estados Unidos que pode ser usado no auxílio desta atividade dento das organizações.

A auditoria interna deve emitir uma opinião independente para a Administração da organização informando se os riscos estão sendo gerenciados a níveis aceitáveis. Há uma metodologia denominada *Risk Based Internal Auditing* – RBIA (Auditoria Interna Baseada em Risco) [31] voltada exclusivamente para a avaliação de riscos pelo controle interno. Tal metodologia pode ser adaptada à necessidade de qualquer auditor. Além das citadas, há inúmeras outras publicações que podem ser usadas na análise de riscos [15][35][102][28][12][103].

Há dois tipos de avaliação de riscos a ser executada por um auditor:

a) **Risco do objeto:** é o risco a que o objeto a ser auditado está submetido.

A avaliação de riscos é uma técnica utilizada para examinar unidades auditáveis dentro do universo da auditoria e selecionar as áreas para avaliação que apresentam maior exposição a riscos para serem incluídas no planejamento. Os planos e objetivos estratégicos da entidade auditada e a estrutura de gestão de riscos corporativos devem ser considerados parte integrante da avaliação de riscos quando disponíveis ao auditor.

Ainda sobre o mesmo conceito, segundo Imoniana[33], “a análise de risco é uma metodologia adotada pelos auditores de TI para saber, com antecedência, quais as ameaças puras ou prováveis em um ambiente de tecnologia da informação de uma organização. Essas ameaças puras ou prováveis constituem eventos futuros não desejáveis ou incertos, cuja ocorrência resulta em perdas.”.

O risco associado a cada área de TI não pode ser determinado pela análise da TI isoladamente, mas em conjunto com os processos e objetivos da organização.

Para melhor entendimento desta questão, vamos analisar duas situações:

i. O Portal da Transparência [81] é um canal pelo qual o cidadão pode acompanhar a execução financeira dos programas de governo, em âmbito federal. Estão disponíveis informações sobre os recursos públicos federais transferidos pelo Governo Federal a estados, municípios e Distrito Federal – para a realização descentralizada das ações do governo – e diretamente ao cidadão, bem como dados sobre os gastos realizados pelo próprio Governo Federal.

ii. A página do Banco do Brasil [78] é um canal na *Internet* que possibilita que seus clientes realizem consultas e transações financeiras online.

No primeiro caso, o foco do problema é a integridade da informação que está sendo mostrada para o cidadão. O dado precisa estar íntegro e correto para se visualizado por qualquer pessoa. Entretanto, o dado não é confidencial, ou seja, não precisa de direitos de acesso para ser consultado.

Já no segundo caso, além dos dados ser íntegro e correto, ele é confidencial, ou seja, cada cliente tem acesso apenas aos dados e transações de sua própria conta.

Portanto, quando não se conhece o objetivo da organização, não se podem determinar os riscos de um processo de TI. Certos critérios da informação nem sempre são necessários para um aplicativo estar em conformidade com seu objetivo.

O Risco possui dois grandes atributos: probabilidade e impacto. Estes atributos devem ser equacionados de uma forma padronizada dentro das auditorias para que a organização auditora possua uma mesma base paramétrica para se guiar.

O *IT Assurance Guide* apresenta uma abordagem para análise de risco. Entretanto, do ponto de vista de um órgão de controle, que é distinto do órgão executor, apenas alguns passos são aplicáveis. Os passos utilizados em nossa abordagem podem ser visualizados na Figura 4.3.

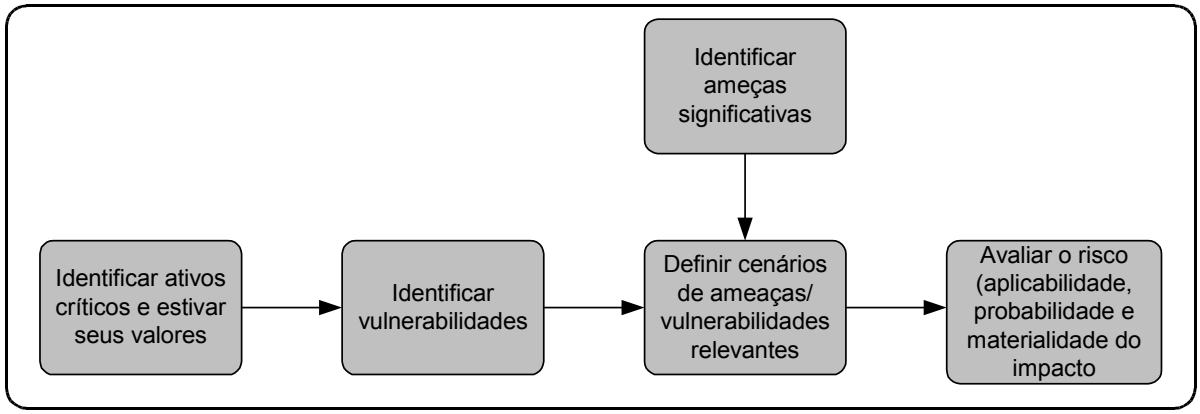

Figura 4.3 – Passos de uma análise de riscos

b) **Risco de auditoria:** é a possibilidade de o auditor vir a emitir uma opinião tecnicamente inadequada sobre situações com incorreções materialmente relevantes. Pode decompor-se em risco inerente, risco de controle e risco de detecção.

Risco Inerente é a possibilidade de a informação estar errada devido à inexistência ou inadequação de controles internos.

Risco de Controle é a possibilidade de a informação estar errada e isto não ser detectado pelo sistema de controle interno. Este está ligado à eficácia dos procedimentos do controle interno (ao contrário, o risco inerente está mais ligado à inexistência do controle interno).

Risco de Detecção é a possibilidade de a informação estar errada e, em função dos procedimentos de auditoria, isto não ser detectado. Nenhum risco de detecção pode ser dimensionado por métodos de amostragem. O risco de detecção é determinado a partir da eficiência dos procedimentos de auditoria. Assim, abrange aspectos não relacionados com o processo de amostragem.

Os riscos inerentes e de controle podem ser avaliados pelo auditor juntos ou separadamente, pois ambos referem-se ao sistema de controle interno. Estes riscos sempre existem já que não há sistema de controle interno perfeito. Já o risco de detecção é função dos procedimentos de auditoria, isto é, dos testes substantivos. A existência deste tipo de erro pode ser devido a procedimentos de auditoria inadequados, equipe de auditoria inapta, interpretação errônea do resultado do teste, entre outras razões.

Estabelecido no SAS nº 47, "Audit Risk and Materiality in Conductin an Audit" **Erro! Fonte de referência não encontrada.**, o Modelo de Risco do AICPA, ou Risco Final, é o produto entre risco inerente (RI), risco de controle (RC) e risco de detecção (RD). Assim, temos:

$$\mathbf{RF = RI \times RC \times RD}$$

O auditor deve efetuar os testes de modo que o resultado obtido seja menor que o risco (final) que ele está disposto a assumir. É importante que a organização possua um procedimento padronizado de análise de risco, de forma que estas variáveis possam ser uniformemente medidas com o uso de parâmetros pré-determinados.

4.2.3. Procedimentos de Auditoria

Os procedimentos de auditoria são o conjunto de técnicas que permitem ao auditor obter evidências ou provas suficientes e adequadas para fundamentar sua opinião sobre o objeto auditado. São compostos por:

Testes de observância: visam à obtenção de razoável segurança de que os procedimentos de controle interno, estabelecidos pela administração, estão em efetivo funcionamento e cumprimento.

Teste substantivos: visam à obtenção de evidência quanto à suficiência, exatidão e validade dos dados produzidos pela entidade.

Na fase de testes, diferentes testes podem ser aplicados. Cinco métodos genéricos, citados pelo *IT Assurance Guide*, incluem:

→ **Investigar e confirmar:**

- Procurar por exceções/desvios e examiná-los;

- Investigar transações/eventos não usuais ou rotineiras;

- Checar/determinar se algo ocorreu (ou não) (amostra);

- Corroborar instruções da gerência a partir de fontes diferentes;

- Entrevistar funcionários e avaliar seus conhecimentos.

- Reconciliar transações;

- Fazer perguntas à gerência e obter respostas para confirmar os achados.

→ **Inspeção:**

- Revisar planos, políticas e procedimentos;

- Procurar por trilhas de auditoria, *logs* de problemas, etc.

- Investigar transações através de um processo/sistema;

- Inspecionar existência física;

- Andar por instalações;

- Comparar achados reais com o esperado.

→ **Observação:**

- Observar e descrever os processos;

- Observar e descrever os procedimentos;

- Comparar comportamento real com o esperado.

→ **Re-execução e Recálculo:**

- Desenvolver independentemente e estimar a saída esperada;

- Testar o que é prevenido;

- Re-executar o que é detectado por controles detectores;

- Re-executar transações, procedimentos de controle, etc.;

- Recalcular independentemente;

- Comparar valores esperados com valores reais;

- Investigar transações através de processos/sistemas.

→ **Examinar coleta automática de evidências:**

- Coletar amostra de dados;

- Usar módulos de auditoria;

- Analisar dados usando CAATs;

- Extrair exceções e transações-chave.

4.2.4. Aplicação de Técnica de Auditoria Assistida por Computador

As Técnicas de Auditoria Assistida por Computador (TAAC) ou, em inglês, *Computer Assisted Audit Technique* (CAAT) podem ser aplicadas em testes de controles gerais, testes de detalhes de transações, testes analíticos e substantivos e amostragem.

As ferramentas de TAAC auxiliam na extração, sorteio, seleção de dados e transações, atentando para discrepâncias, duplicidades e desvios.

De acordo com [33][35], as ferramentas de TAAC podem ser classificadas em *softwares* generalistas, *softwares* especialistas e *softwares* utilitários.

Os *softwares* generalistas de Auditoria de TI são aplicativos que possuem funções variadas de auditoria como extração de dados, sumarização, testes globais, apontamento de duplicidades, seleção de amostras, entres outras. Há também aqueles voltados para os processos e fases da auditoria, sendo capazes de dar suporte a todas as etapas de processo, desde o planejamento até a geração de relatório. São exemplos de softwares especialistas: SAS [86], ACL [82], IDEA [84], Galileo [83] e Pentana [85].

Os *softwares* especialistas são aqueles desenvolvidos pelo auditor ou, decorrente da necessidade destes, por terceiros, com a finalidade de realizar tarefas específicas. Deve ser feita uma análise custo/benefício para o desenvolvimento deste tipo software.

Os *softwares* utilitários são aqueles que não foram desenvolvidos especificamente para auditoria, mas auxiliam no processo, como os bancos de dados.

4.2.5. Papéis de Trabalho

Os papéis de trabalho são documentos que formalizam as informações obtidas nos trabalhos de auditoria, desde o planejamento até o encerramento. São produzidos pelo auditor ou colhidos por ele, mas produzidos por outras fontes. Podem estar em papel, meios eletrônicos ou em qualquer outra forma a que assegurem o objetivo a que se destinam.

Devem ter abrangência e grau de detalhamento suficiente para fundamentar a opinião do auditor, seguir um padrão definido e claro, ser limpos, objetivos, corretos, completos, concisos e elaborados de forma sistemática e racional.

Segundo a NBC T 11.3, os papéis de trabalho devem ser conservados em boa guarda pelo período de cinco anos a partir da data de emissão do parecer pelo auditor.

Os papéis de trabalho podem ser de dois tipos: permanente e corrente.

Os permanentes não são resultado de exames realizados, mas referem-se aos documentos, registros e informações gerais consolidados sobre o objeto da auditoria e sobre as unidades auditadas. Por isso, poderão ser utilizados em mais de uma auditoria. Como exemplo, tem-se os regimentos internos e a legislação específica aplicáveis às entidades auditadas.

Os correntes referem-se a informações e documentos gerados, obtidos e utilizados na realização das auditorias e têm por finalidade documentar os testes realizados, auxiliar a execução dos exames, evidenciar as conclusões emitidas e possibilitar a avaliação do processo de auditoria em si.

4.2.6. Ambiente de Auditoria

O ambiente de auditoria é o local onde será realizado o trabalho de campo. Em auditorias, a preocupação com segurança é sempre fundamental.

O grau de proteção e implementação de controles de segurança devem estar de acordo com o valor do objeto de auditoria para a organização auditada. Ao avaliar este valor devem ser considerados aspectos financeiros, de imagem (o que a organização quer aparentar para o público), criticidade da informação tratada e quantidade de indícios de problemas graves.

Entretanto, independente desta avaliação, um nível básico de segurança é obrigatório, assim como a obediência a questões relacionadas a normas profissionais de auditoria, como as relacionadas nas Normas Brasileiras de Profissionais de Auditor Interno e Independente [22][23] e as Normas Internacionais para o Exercício da Auditoria Interna [65].

O ambiente de trabalho de campo deve ser cuidadosamente estudado e algumas medidas básicas devem ser sempre tomadas, como:

- Controlar o acesso de pessoas que não pertençam à equipe de auditoria na sala destinada a esta e nunca permitir a permanência de terceiros sem nenhum membro da equipe de auditoria;

- Não deixar anotações sobre exames da auditoria à vista do auditado;

- Zelar pela segurança de *notebooks*, mídias, *pen drives* e demais fontes de informação;

- Tomar cuidados relacionados à segurança da informação quando usarem a conexão de rede da entidade auditada;

O uso de redes *ad hoc* é uma boa opção em tais ambientes, pois permite compartilhamento de conexão na Internet (pontos de redes disponíveis são sempre poucos) e compartilhamento de dados, sem a necessidade de uma estrutura física organizada. Assim, qualquer sala de reunião que tenha pelo menos um ponto de rede pode ser usada e oferecer um mínimo de estrutura de trabalho.

Entretanto, nem sempre é necessário realizar o exame do objeto no ambiente do auditado. Este é o caso, por exemplo, de Auditoria de Dados, em que o importante é estar de posse dos dados, independente do ambiente. Ressalta-se que, muitas vezes, a organização auditora possui uma estrutura melhor para tratamento de dados dentro de seu ambiente do que em trabalho de campo. Nestes casos, outros tipos de cuidado com a segurança devem ser tomados, como a proteção dos dados retirados da entidade auditada, já que geralmente são confidenciais e a garantia da integridade da cópia do banco de dados em relação ao original.

4.3. ELABORAÇÃO DO PLANO DE AUDITORIAS

A organização auditora deve elaborar semestralmente ou anualmente (ou outro período que julgar conveniente) um Plano de Auditorias previstas para o período. No caso das organizações que possuírem um Escritório de Projetos de Auditoria de TI, esse planejamento é gerenciado por este escritório, mesmo que as demais áreas da entidade precisem ser consultadas.

Este planejamento pode ser dividido nas seguintes etapas:

4.3.1. Mapeamento

A entidade auditora deve fazer um levantamento de todas as áreas de TI, sob sua jurisdição, passíveis de auditoria e que possuam relevância na operacionalização de ações governamentais.

A determinação do universo da auditoria deve ser feita com base no conhecimento do plano estratégico de TI da organização auditada, das suas operações e discussões com a gestão responsável.

4.3.2. Hierarquização

Nesta etapa, todos os itens mapeados devem ser hierarquizados de acordo com critérios de relevância, materialidade e criticidade.

A relevância leva em consideração a importância do objeto selecionado para dar suporte a políticas governamentais. A importância de tais políticas também deve ser considerada.

A materialidade refere-se ao volume de recursos financeiros investidos ou a ser investidos no objeto.

A criticidade é definida a partir de uma análise de risco potencial ou factual global, ou seja, devem ser classificados em um grau mais alto da hierarquização aqueles objetos possam trazer ou que já trazem maiores prejuízos (financeiros ou não) no caso de seu mau funcionamento. Nesta etapa, a análise de risco realizada é simples e básica.

O uso da avaliação de riscos na seleção de projetos de auditoria permite que o auditor quantifique e justifique a quantidade de recursos de auditoria necessários para concluir o plano de auditoria de TI. Além disso, o auditor pode dar prioridade a revisões programadas a objetos já auditados com base na percepção de riscos.

4.3.3. Priorização

A partir do universo de objetos passíveis de auditoria hierarquizados, devem-se priorizar as auditorias a serem realizadas de acordo com critérios de prioridades institucionais, capacidade operacional da instituição auditora e oportunidade de atuação.

4.3.4. Escopo básico dos itens priorizados

Os objetos selecionados na priorização devem ter seu escopo especificado e pontos críticos definidos em um nível macro. O detalhamento aprofundado de cada objeto será realizado durante o Planejamento específico de cada auditoria.

4.3.5. Cronograma de previsão de auditorias

As auditorias selecionadas devem ser distribuídas em um cronograma dentro do período compreendido pelo Plano de Auditorias. Quanto melhor estimado o cronograma, menores os riscos de não se conseguir cumprir o planejado.

4.3.6. Plano de Auditorias

Nesta etapa, são consolidadas, em um único Plano, a ordem de priorização dos objetos de auditoria, o cronograma de auditorias para o período escolhido (semestre, ano ou outro período de tempo utilizado), o escopo de cada objeto e o cronograma de previsão de auditorias.

Este plano deve ser usado como guia de execução de auditorias dentro do período selecionado e todo desvio do previsto deve ser registrado para que, ao final do período, uma análise do Plano de Auditorias seja feito a fim de que os problemas que geraram os

desvios na execução sejam evitados ou considerados quando da elaboração de outros Planos.

Cabe ressaltar que, apesar da existência de um cronograma, pode haver também a necessidade da realização de auditorias especiais que não tenham sido previamente planejadas. No caso governamental, elas podem acontecer pela existência de denúncias ou acontecimento de fatos relevantes ou mudanças de políticas governamentais que tornem prioritária tal auditoria.

4.4. FASES DA AUDITORIA DE TI

Um Projeto de Auditoria é divido em fases para facilitar seu gerenciamento, controle e execução. O importante é que as atividades sejam divididas em fases e controladas, independente do grau de divisão e do nome que se dê a cada uma, pois isto varia entre os modelos propostos no mercado. Neste trabalho, trabalharemos com as fases mostradas na Figura 4.4.

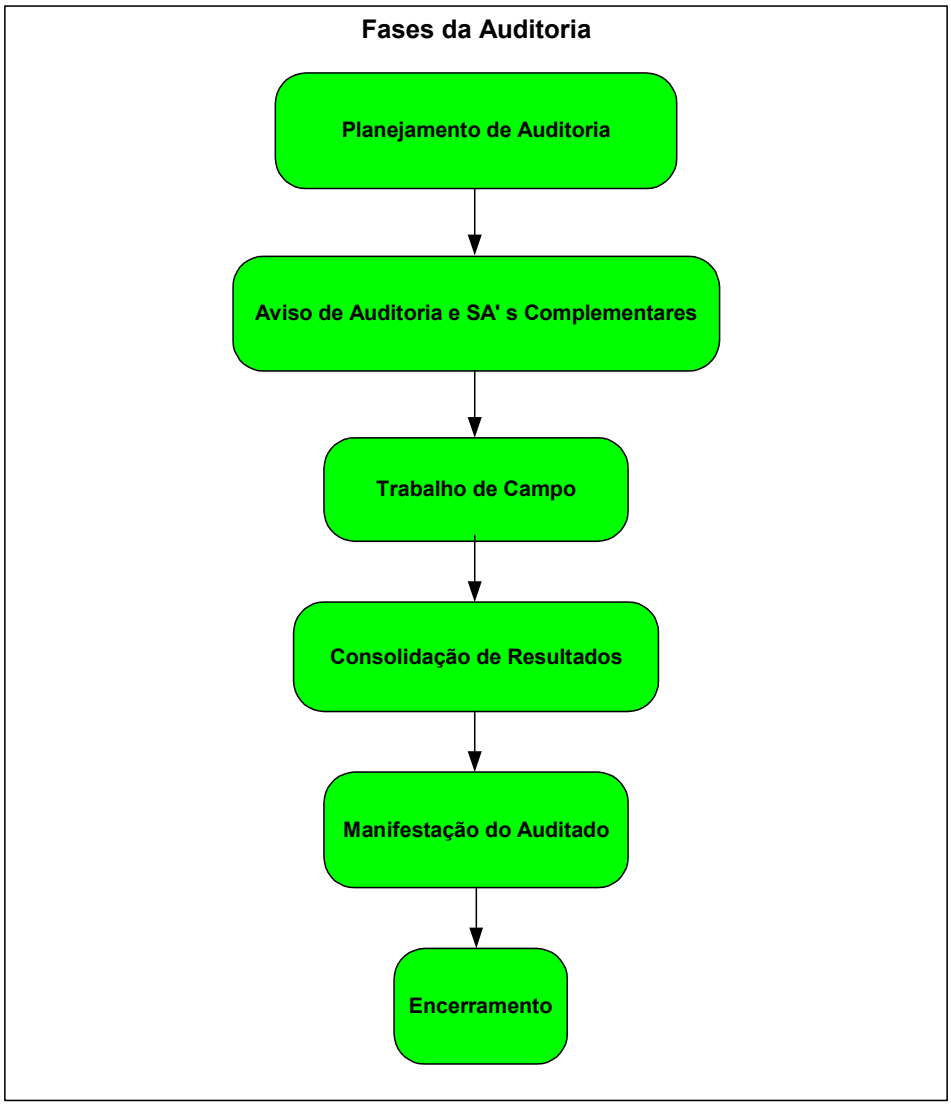

Figura 4.4 – Fases da Auditoria

4.4.1. Planejamento de Auditoria

O Planejamento é a fase base da auditoria. Quando bem realizado, o risco de auditoria é controlado, o retrabalho é evitado e os resultados são mais bem embasados.

É no Planejamento que se define **quando**, **como** e **o quê** será analisado e verificado. Nesta fase, devem ser considerados todos os fatores relevantes na execução dos trabalhos.

A falta de definição do escopo da auditoria faz com que o auditor vá a campo sem um direcionamento sobre o que procurar. Com isso, suas análises podem ser superficiais e

sem um foco consistente. Muitas vezes, ele pode desconfiar da existência de uma constatação só após a análise de seus achados. Entretanto, já pode ser tarde demais para se conseguir material suficiente para o embasamento do fato detectado.

O planejamento pressupõe adequado nível de conhecimento sobre as atividades, os fatores econômicos, legislação aplicável e as práticas operacionais da entidade, e o nível geral de competência de sua administração.

O auditor deve documentar seu planejamento geral e preparar programas de trabalho por escrito, detalhando o que for necessário à compreensão dos procedimentos que serão aplicados, em termos de natureza, oportunidade e extensão, de forma a servir como guia e meio de controle de sua execução.

O planejamento e os programas de trabalho devem ser revisados e atualizados sempre que novos fatos o recomendarem.

Esta fase divide-se nas seguintes etapas, conforme Figura 4.5:

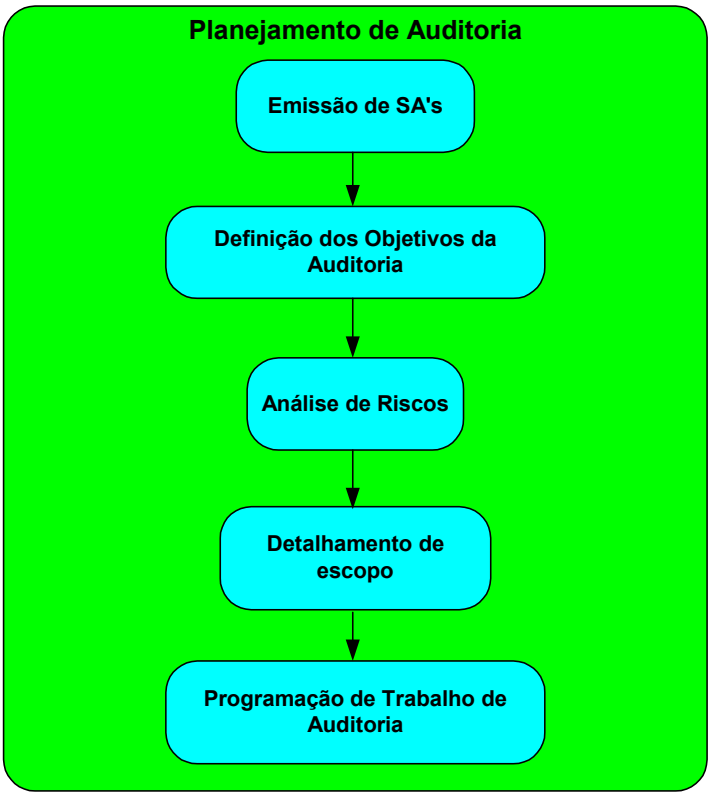

Figura 4.5 – Planejamento de Auditoria

→ Passo 1: Emissão de Solicitações de Auditoria prévias

Como as auditorias realizadas pelos órgãos de controle (interno ou externo da APF) acontecem sobre os órgãos de execução de programas e políticas de governo, antes do detalhamento do escopo, é necessário que sejam solicitadas informações sobre o objeto a ser auditado. Dentro da APF, são inúmeras as possibilidades de objeto, que pode ir desde uma licitação para aquisição de software a uma avaliação total da Governança de TI dentro de determinado órgão.

A obtenção de informações deve bordar todos os assuntos relacionados com os objetivos e alcance da auditoria, desde informações da própria estrutura da unidade auditada (como regimentos e planos) como dados gerais do objeto a ser auditado. Devem ser colhidas as informações necessárias para que se faça uma análise de riscos a fim de se identificar os pontos críticos do objeto. O órgão auditado é obrigado a fornecer as informações necessárias ao trabalho de auditoria.

Algumas informações a seguir podem ser solicitas nesta etapa ou, de acordo com decisão do coordenador da auditoria, deixar para levantá-las durante o trabalho de campo:

- Requisitos de negócio e riscos associados;

- Estrutura organizacional;

- Papéis e Responsabilidades (importante no momento de responsabilização);

- Políticas e procedimentos;

- Legislação aplicável e demais regulações;

- Medidas de controle implementadas;

- Relatórios da gerência;

- Recomendações anteriores e ações corretivas implementadas;

- Questões atuais.

As recomendações anteriores e ações corretivas implementadas serão solicitadas caso o mesmo objeto já tenha sido analisado pelo órgão auditor anteriormente, ou se tenha conhecimento de solicitações realizadas por outros órgãos de controle. Esse tipo de atividade é denominada de *Follow-up* e seu objetivo é verificar o cumprimento das solicitações.

A partir dos papéis e responsabilidades dentro da organização, é possível fazer um diagrama RACI. Este diagrama é uma ferramenta que ajuda a identificar quem é responsável (*Responsible*) pelas atividades desenvolvidas, a quem o responsável deve prestar contas (*Accountable*), quem é consultado (*Consulted*) e quem é informado (*Informed*), dentro uma equipe de trabalho, de um departamento ou de um órgão.

Por meio da análise RACI [107] é possível estabelecer a responsabilidade pelas decisões e pela execução das atividades; identificar o tipo ou grau de participação de cada agente (pessoa, órgão ou departamento) em cada decisão; tornar mais clara a relação entre as partes envolvidas; e conhecer a distribuição de poder. Com isso, se houver necessidade de responsabilização de algum agente por dolo ou culpa em ato que gere alguma constatação, basta consultar o diagrama.

→ Passo 2: Definição dos Objetivos Gerais da Auditoria

Nesta etapa, devem ser definidos os objetivos gerais da auditoria em questão. Em termos genéricos, detalhar o que se deseja avaliar. Por exemplo, o objeto da auditoria pode ser um software adquirido. O objetivo da auditoria pode ser avaliar o processo de aquisição do software sobre o ponto de vista legal. Já se o objeto for o ambiente de gerenciamento de dados sensíveis de uma organização, o objetivo pode ser analisar a segurança da informação em tal ambiente em todos os seus aspectos: confidencialidade, integridade e disponibilidade.

Os objetivos gerais de uma auditoria guiarão a escolha dos pontos críticos e objetivos de controle a serem analisados.

→ Passo 3: Análise de Riscos

De posse das informações sobre o objeto a ser auditado, deve ser realizada uma análise de risco detalhada sobre os riscos relevantes a que esse objeto está sujeito e sobre os riscos da auditoria em TI.

O escopo da realização da auditoria de TI deve refletir os resultados de tal avaliação de riscos.

Nesta etapa, além da bibliografia já citada como subsídio, o auditor de TI pode consultar diretriz G13 [ANEXO IV: NORMAS, DIRETRIZES E PROCEDIMENTOS DA ISACA] de auditoria de Sistemas de Informação - SI, "Uso da avaliação de riscos no planejamento da auditoria", e o procedimento P1 de auditoria de SI, "Medição da avaliação de riscos". Ambos os documentos são encontrados no sítio da ISACA [75].

Com base nessas informações, algumas análises preliminares já podem ser feitas, gerando alguns indícios a serem verificados no trabalho de campo.

→ Passo 4: Detalhamento de escopo

Com base nas informações recebidas, em análise de risco sobre o objeto e nos pontos críticos observados, detalhar o escopo da auditoria. Nesta etapa, se define a extensão e a profundidade de cada exame.

Neste trabalho, utilizamos como base os objetivos de controle do COBIT e as diretrizes do *IT Assurance Guide* para definir o escopo. Como já dito anteriormente, isso permite que exista uma linguagem comum dentro da organização auditora e entre a auditora e a auditada.

Segundo o *IT Assurance Guide*, o processo de detalhamento de escopo pode ser feito de três formas diferentes:

1. A abordagem mais detalhada de definição de escopo começa pela definição dos objetivos de negócio e de TI para o ambiente em análise e identificação do conjunto de processos e recursos de TI (universo a ser examinado) necessários para atingir tais objetivos. Os objetivos que são objeto da auditoria podem ser detalhados, por exemplo, em objetivos de controle customizados para a organização.

2. A abordagem mais geral de escopo utiliza diretrizes genéricas no que se refere a objetivos de negócio, objetivos de TI e processos de TI, como descritos no COBIT. A partir desta cascata genérica, um escopo mais detalhado voltado para o ambiente específico pode ser definido.

3. A abordagem híbrida de definição de escopo combina as duas abordagens anteriores, iniciando por uma cascata genérica de objetivos e processos, mas é adaptado e modificado para o ambiente específico antes da definição de escopo em um nível mais detalhado.

A escolha da abordagem mais adequada depende do nível de conhecimento do ambiente a ser analisado.

Neste trabalho, propõe-se que se utilize uma abordagem híbrida, porém um pouco modificada em relação à proposta acima. Isto se justifica pelo contexto onde a auditoria de TI será aplicada. Os objetivos de negócio apresentados pelo COBIT, desenvolvidos principalmente para empresas do setor privado, em sua maioria, possuem um ângulo de visão diferente daquele usado dentro da Administração Pública, salvo no caso de empresas públicas. Os objetivos de negócio da Administração Pública estão muito mais ligados aos Princípios que regem tal Administração do que ao alcance de lucro.

Portanto, uma abordagem para detalhamento de escopo neste tipo de auditoria deve começar com a definição dos objetivos de negócio específicos do objeto auditado. Em seguida, devem ser mapeados em objetivos de TI, tomando como base os objetivos de TI do COBIT, mas com as adaptações necessárias para os objetivos de negócio da Administração Pública.

Para ajudar no Planejamento de auditoria, o COBIT provê uma cascata detalhada partindo dos objetivos de negócio relacionados com TI, passando pelos objetivos de TI e chegando aos processos de TI. O COBIT define 17 objetivos de negócio genéricos, que englobam guias e serviços de negócio que impactam a TI diretamente. Eles são traduzidos em objetivos de TI que são relacionados a objetivos de processos de TI. Esta cascata de objetivos de negócio, TI e processo é particularmente útil quando da análise dos guias de

auditoria e de como eles impactam o universo auditado. Entretanto, como dito anteriormente, nem sempre esses objetivos são aplicáveis à Administração Pública e, grande parte das auditorias, terá objetivos de negócio próprios e não os apresentados pelo COBIT.

Apesar das adaptações necessárias, essa cascata de objetivos pode ajudar a guiar o planejamento de trabalho de auditoria. Como mostrado na Tabela 4.1, se o trabalho da auditoria focar em uma função específica de negócio, objetivos de negócios relacionados a TI e objetivos de TI podem ser valiosas entradas para o planejamento de trabalho. O trabalho de auditoria que foca em componentes organizacionais (por exemplo, um processo) pode usar objetivos e processos de TI como fonte de informação para o planejamento.

Tabela 4.1 – Relação entre foco e planejamento da auditoria.
Fonte: COBIT 4.1

	OBJETO DE AUDITORIA				
	Função de Negócio	**Aplicação Principal**	**Componente Importante de Infra-estrutura**	**Componente Organizacional**	**Uma Grande Mudança**
Objetivos de Negócio	**Principal**	**Secundário**			**Principal**
Objetivos de TI	**Secundário**	**Principal**	**Principal**	**Secundário**	**Secundário**
Objetivos de Processos de TI		**Secundário**	**Secundário**	**Primário**	**Secundário**

Este passo pode ser dividido nas seguintes atividades:

i) Documentar a arquitetura de TI da organização

Nesse passo, a arquitetura de TI (item 3.4.1) da organização é documentada. Essa arquitetura pode ser validada por meio de entrevistas com funcionários-chave da TI.

ii) Seleção de *frameworks* de controle

Nesse passo, *frameworks* de controle são selecionados. Como padrão, adotaremos o COBIT em combinação com *frameworks* mais específicos, dependendo das características do objeto auditado.

iii) Identificação de processos de TI

Depois da escolha apropriada dos *frameworks* de controle, os processos apropriados de TI são selecionados e relacionados com os recursos de TI apropriados (atividade iv). Os processos de TI que farão parte do escopo podem ser identificados pela análise de relacionamento com objetivos de negócio, objetivos de TI e processos de TI.

iv) Seleção de componentes de TI

Os recursos de TI são formados por: Aplicações, Informação, Infra-estrutura e Pessoas.

O número de entradas pode ser usado para determinar os recursos de TI que são relevantes. Esse levantamento pode ser completo, pois a análise de risco subseqüente determina os itens que podem ser excluídos do escopo. Entretanto, deve-se levar em conta a eficiência para manter a matriz em um tamanho trabalhável e razoável.

v) Refinar a seleção de componentes de TI

No processo de relacionamento inicial de processos com recursos, o auditor deve ter redigido uma larga lista, entretanto, maior do que é possível se analisar. Neste passo, o auditor deve refinar esta seleção de forma a garantir que os recursos tenham uma relação direta com os processos relevantes da auditoria.

vi) Seleção de Objetivos de Controle

O auditor faz uma primeira seleção dos objetivos de controle do COBIT que sejam relevantes para os processos de TI que estão no escopo da auditoria. Freqüentemente, os objetivos de controle precisam ser customizados para a realidade particular da entidade auditada. Para a maioria das auditorias, o levantamento dos recursos de TI não precisa de análises substanciais, porque começa de uma situação específica da situação da entidade auditada. Entretanto, o levantamento dos objetivos de controle exige uma análise mais detalhada porque esse processo se inicia de *frameworks* genéricos. O COBIT provê suporte pela descrição de guias de risco e valor para cada objetivo de controle, demonstrando porque os controles específicos são necessários. Mapeamentos são necessários para a customização dos objetivos de controle selecionados para o ambiente da organização auditada.

vii) Refinar a seleção de Objetivos de Controle

Finalmente, o auditor relaciona a lista refinada de recursos de TI com a lista de objetivos de controle selecionados no passo anterior. Em um processo interativo, o auditor refina e, muitas vezes, reduz a lista de objetivos de controle que são relevantes para a auditoria.

Nesse passo, o auditor deve fazer a análise de risco de não alcançar o objetivo de controle selecionado para o recurso de TI escolhido e descartar os recursos de TI e objetivos de controle que não têm relevância se não forem alcançados.

Como resultado desta etapa, tem-se todos os objetivos de controle escolhidos para serem analisados, que devem guardar relação com os pontos críticos do objeto. A cada ponto escolhido, chamaremos de ponto de controle.

b) Programação de Trabalho de Auditoria

Os Programas de Trabalho de Auditoria devem ser detalhados de forma a servir como guia e meio de controle de sua execução.

O detalhamento de escopo permite ao auditor conhecer os pontos de controle a serem verificados.

Esta etapa pode ser dividida nos seguintes passos, conforme Figura 4.6:

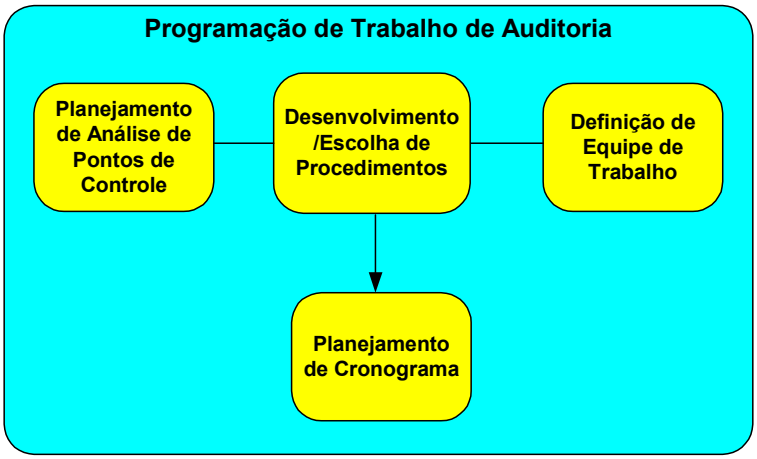

Figura 4.6 – Programação de Trabalho de Auditoria

Passo1: Planejamento de Análise de Pontos de Controle

As etapas i, ii e iii são desenvolvidas concomitantemente, pois guardam grande dependência entre si.

Para cada um dos pontos de controle a serem avaliados, devem ser definidos: a quantidade de horas-homem necessária, os itens a serem analisados, a estratégia de seleção destes itens (prova seletiva ou amostragem) e as técnicas a serem utilizadas.

A quantidade de horas-homem necessária para auditoria é a previsão de quantas horas serão necessárias para todo o processo de auditoria, mas especificado por atividade. A partir disso, define-se a quantidade de servidores necessários na auditoria.

Os pontos de controle a serem analisados já foram definidos quando do detalhamento do escopo. Entretanto, nesta etapa, eles são listados juntamente com as

informações complementares de cada item, como horas necessárias, estratégia de seleção dos itens a serem examinados, técnicas e procedimentos.

A estratégia de seleção de itens pode ser por prova seletiva em que há critérios a serem seguidos pelos elementos selecionados ou por amostragem probabilística ou não probabilística. Ao usar métodos de amostragem estatística ou não estatística, o auditor deve projetar e selecionar uma amostra de auditoria, aplicar a essa amostra procedimentos de auditoria e avaliar os resultados da amostra, de forma a proporcionar evidência de auditoria suficiente e apropriada.

As técnicas previstas referem-se às técnicas convencionais de auditoria a serem utilizadas na avaliação dos itens.

Passo 2: Definição de Equipe de Trabalho

A partir das necessidades técnicas e operacionais observadas no detalhamento de escopo e no planejamento de análise de pontos de controle e com base na disponibilidade de servidores, deve-se definir o número de membros e o perfil da equipe de trabalho do projeto de auditoria.

Este é o momento de se alocar os recursos humanos para o projeto, definindo o coordenador (gerente de projeto) e os membros da equipe de trabalho.

Passo 3: Desenvolvimento/Escolha de Procedimentos

Os procedimentos a serem usados nas auditorias podem ser desenvolvidos para cada projeto ou específico ou escolhidos a partir de um banco de dados de procedimentos. O capítulo 5 deste trabalho traz uma metodologia para desenvolvimento de procedimentos

que pode ser aplicado para projetos específicos ou para fazer procedimentos gerais que serão armazenados para uso geral.

Passo 4: Planejamento de Cronograma

Nesta etapa, conhecendo-se as atividades a serem realizadas e a equipe de trabalho disponível somados às lições aprendidas em definições de escopos de projetos anteriores, deve-se fazer uma previsão de cronograma para a realização da auditoria. Esta previsão deverá conter o período de tempo total a ser utilizado para planejamento, o período de tempo a ser utilizado para o trabalho de campo, o período referente à análise de resultados e produção de parecer e relatório e, por fim, o período total planejado, que consiste da soma de todos os outros períodos.

4.4.2. Aviso de Auditoria e SA' s Complementares

Nesta etapa, um aviso de auditoria oficial é enviado ao órgão auditado. Este aviso deve conter o escopo a ser analisado, a equipe responsável pelo trabalho e o período de tempo do trabalho de campo.

Além disso, podem ser enviadas SAs complementares, como forma de adiantar o trabalho de levantamento de dados que serão usados na auditoria, caso se observe que o órgão terá que fazer levantamento de informações não disponíveis a qualquer momento.

4.4.3. Trabalho de Campo

No Trabalho de Campo, a equipe de auditoria vai aplicar tudo o que foi planejado.

A correta aplicação dos procedimentos constantes no Programa de Trabalho busca garantir que tudo o que foi planejado seja realizado e de forma controlada.

Durante o Trabalho de Campo, o auditor deve anotar os resultados de cada análise, bem como colher as informações que julgar importantes para o embasamento de evidências, como cópias de papel, cópias digitais, fotos, entre outros. A partir das evidências colhidas durante os trabalhos, o auditor aprofunda seus exames de forma a obter novas evidências para dar mais embasamento aos fatos observados.

As informações coletadas no trabalho de campo devem ser suficientes, adequadas, relevantes e úteis no fornecimento de evidências às conclusões e recomendações da auditoria interna.

A aplicação dos procedimentos de auditoria deve ser realizada, em razão da complexidade e volume das operações, por meio de provas seletivas, testes e amostragens, cabendo ao auditor, com base na análise de riscos de auditoria e outros elementos de que dispuser, determinar a amplitude dos exames necessários à obtenção dos elementos de convicção que sejam válidos para o todo.

O auditor deve documentar, através de papéis de trabalho, todos os elementos significativos dos exames realizados e que evidenciam ter sido a auditoria executada de acordo com as normas aplicáveis.

Os papéis de trabalho devem ter abrangência e grau de detalhe suficientes para propiciar o entendimento e o suporte da auditoria executada, compreendendo a documentação do planejamento, a natureza, oportunidade e extensão dos procedimentos de auditoria, bem como o julgamento exercido pelo auditor e as conclusões alcançadas.

Essa etapa pode ser dividida nos seguintes passos, conforme a Figura 4.7:

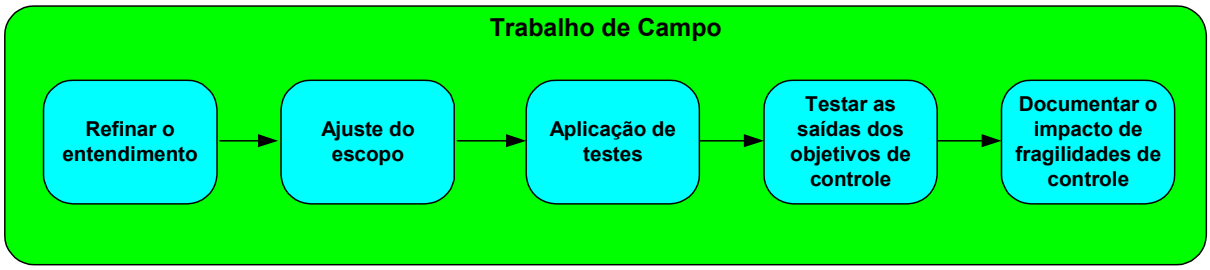

Figura 4.7 – Trabalho de Campo

→ Passo 1: Refinar o entendimento

O primeiro passo da etapa de execução é refinar o entendimento da organização auditada e do ambiente onde os testes serão realizados. O objetivo deste passo é documentar as atividades que sustentam os objetivos de controle selecionados para exame na fase de planejamento e identificar medidas/procedimentos de controle implementados.

Nesta etapa coleta-se e analisa-se documentação relativa a descrição de processos, políticas, entradas/saídas, questões gerais, minutas de reuniões, relatórios anteriores de auditoria, recomendações anteriores de auditoria, relatórios de negócio que não tenha sido examinada durante a fase de planejamento.

A saída deste passo consiste na documentação de evidências relativas a:

- Quem executa as tarefas, onde e quando são executadas. Essa tarefa pode ser realizada por entrevistas e utilização de diagramas RACI.

- As entradas necessárias para executar as tarefas e as saídas geradas por elas.

- Os procedimentos da organização para executar as tarefas.

→ Passo 2: Ajuste do escopo

Com base nas informações colhidas no passo anterior, caso se verifique necessidade, o auditor deve ajustar o escopo de forma a atender questões relevantes não detectadas no planejamento ou descartar questões percebidas como irrelevantes.

Neste passo, as seguintes atividades devem ser realizadas:

i) Análise dos objetivos de negócio e de TI

Os objetivos da auditoria e a abordagem dos objetivos de negócio atuais devem ser realinhados, e o entendimento dos processos de negócio, os objetivos de negócio, e a relevância da TI para os processos e objetivos devem ser atualizados. Os objetivos de TI precisam ser ajustados, tendo em mente os requisitos da última auditoria e a organização da TI.

ii) Seleção dos processos e controles

A seleção de processes, objetivos de controle e recursos de TI deve ser revisada e refinada para estabelecer os limites da auditoria. Esta seleção é feita por meio da avaliação da probabilidade de ocorrência de fatos indesejados e prejuízos (não necessariamente financeiro) em conseqüência do não alcance dos objetivos de controle.

iii) Análise de Riscos

O escopo deve ser ainda ajustado com base em uma avaliação de risco dos objetivos de controle não serem alcançados. Esse ajuste de escopo baseado em risco determina a quantidade de exames e testes necessários na auditoria.

iv) Finalização do escopo

O Programa de Trabalho da Auditoria deve ser atualizado, quando houver necessidade, baseado no último entendimento dos objetivos, melhor abordagem de testes e análise de risco, como descrito nos passos anteriores. A documentação necessária e a abordagem de teste devem ser determinadas para garantir a cobertura mais eficiente e eficaz dos objetivos da auditoria.

→ Passo 3: Aplicação de Testes

Os testes aplicados no trabalho de campo são executados cobrindo os seguintes objetivos principais:

i) Avaliar o *design* de controles;

ii) Confirmar se os controles estão em operação;

iii) Estimar a efetividade operacional dos controles.

As atividades de auditoria a serem realizadas avaliam a adequação dos *designs* de controles. Para essa avaliação, deve-se:

- Observar/inspecionar e revisar a abordagem de controle e testar o *design* sob o ponto de vista de completeza, relevância, oportunidade e capacidade de ser medido.

- Investigar e confirmar se as responsabilidades para as práticas de controle e todas as prestações de conta foram determinadas. Testar quando responsabilidades e *accountability* são entendidos e aceitos. Verificar se as habilidades certas e os recursos necessários estão disponíveis.

- Investigar por entrevistas com funcionários-chave se mecanismos de controle, suas finalidades, e *accountability* e responsabilidades são entendidos.

Para realizar tais atividades, utilizam-se técnicas de auditoria. Algumas delas estão citadas no item 4.3.3 deste trabalho.

Em resumo, neste passo, o auditor deve:

i) Determinar se os processos de controle documentados existem;

ii) Colher e documentar evidências apropriadas acerca da existência de processos de controle;

iii) Verificar se responsabilidades e accountability são claros e efetivos.

→ Passo 4: Testar as saídas dos objetivos de controle

O objetivo deste passo é verificar se as medidas de controle estabelecidas estão funcionando como descritas, consistente e continuamente, e concluir sobre adequação (ou não) do ambiente de controle.

Para testar as saídas ou efetividade dos controles, o auditor deve procurar por evidências diretas e indiretas de impactos dos controles sobre a qualidade das saídas dos processos.

→ Passo 5: Documentar o impacto de fragilidades de controle

Quando fragilidades de controle são encontradas, elas devem ser propriamente documentadas. Deve ser tomado um cuidado particular para analisar e estimar a gravidade das fragilidades observadas e potencial impacto nos negócios (sentido amplo) da entidade auditada.

O objetivo deste passo é conduzir os testes necessários para avaliar a realização de um dado processo de negócio e objetivos de controle relacionados. Análises mais detalhadas devem ser realizadas quando:

i) Não há medidas de controle implementadas;

ii) Controles não funcionam como esperado;

iii) Controles não são consistentemente aplicados.

Este processo deve resultar em um entendimento profundo sobre os potenciais impactos e sobre as fragilidades de controle e conseqüentes ameaças e vulnerabilidades.

As seguintes atividades podem ser usadas para documentar o impacto de não se alcançar os objetivos de controle:

a) Relatar o impacto de não se alcançar o objetivo de controle;

b) Ilustrar o que pode ser afetado com o impacto;

c) Descrever as vulnerabilidades e ameaças mais prováveis com os controles não funcionando efetivamente;

d) Apontar as conseqüências de não estar conforme requisitos regulatórios, legislação aplicável e acordos contratuais.

e) Documentar o custo de erros que poderiam ser evitados com o controle efetivo;

f) Medir e documentar o preço do retrabalho gerado pela fragilidade de controle.

O COBIT provê suporte a essas atividades nos seguintes aspectos:

- Os objetivos de negócio e de TI, os processos de TI e critérios de informação indicam os valores de negócio a serem alcançados e o risco a ser evitado pela melhoria de controles;

- Para cada objetivo de controle, existem guias de valor e risco que indicam os benefícios a serem ganhos e os riscos a serem evitados pela melhoria de controles.

Recomenda-se que o auditor realize seus trabalhos em conformidade com padrões e diretrizes de auditoria. No ANEXO IV: NORMAS, DIRETRIZES E PROCEDIMENTOS DA ISACA, são citados as normas, diretrizes e procedimentos já desenvolvidos pelo ISACA em Auditoria de Sistemas da Informação.

4.4.4. Consolidação de Resultados

Esta fase inclui a consolidação de resultados das fases anteriores, o desenvolvimento de conclusões acerca das fragilidades de controle e a comunicação de ações recomendadas para mitigar o impacto das fragilidades de controle, comparações com desempenhos de padrões e boas práticas para uma visão relativa de resultados e a posição do risco em relação ao processo.

Os fatos observados no trabalho de campo, quando indesejáveis, dão origem a constatações.

Nesta etapa, a equipe de auditoria consolida os resultados procurando identificar os nexos entre os fatos detectados, quando houver, e determina o tipo de constatação.

Durante a análise dos dados coletados em trabalho de campo, o auditor pode concluir por constatações que envolvam falhas, excessos, desperdícios, prejuízos, desvios e fraudes.

A responsabilidade primária na prevenção e identificação de fraude e erros é da administração da entidade auditada, por meio da implementação e manutenção de adequado sistema contábil e de controle interno. Por isso, ao detectar erros relevantes ou fraudes no decorrer dos seus trabalhos, o auditor deve comunicá-los, por meio de Notas ou Solicitações de Auditoria, à administração da entidade, pedindo justificativas e, quanto possível, medidas corretivas para os fatos. Caso sejam encontrados danos ao Erário, eles devem ser quantificados e inseridos no relatório.

A partir de todas as evidências encontradas e informações que a equipe de auditoria julgar relevantes, gera-se um Relatório Preliminar da Auditoria de TI.

O relatório deve conter o objetivo da auditoria, as áreas cobertas por ela, a base teórica e legal utilizada nos exames, as constatações e fatos identificados, as recomendações para ação corretiva das constatações e o prazo dado para colocá-las em prática.

As constatações devem ser embasadas e ter indicação da legislação vigente pertinente e das normas utilizadas para exame. Também podem ser utilizados alguns acórdãos do TCU como referência [ANEXO III: ACÓRDÃOS DO TCU]. Além disso, a utilização da indicação dos objetivos de controle do COBIT que não estão sendo satisfeitos adequadamente permite utilizar uma linguagem padrão em todas as auditorias e estabelecer uma linguagem comum que pode ser entendida pelo auditado.

4.4.5. Manifestação do Auditado

O Relatório Preliminar de Auditoria, após ser revisado pela equipe e pelo Escritório de Projetos (ou Coordenação ou Diretoria responsável), deve ser enviado ao gestor do órgão auditado. Este terá um tempo definido para se manifestar sobre as constatações, dando as justificativas que julgar necessárias.

4.4.6. Encerramento

Esta etapa tem como principais produtos o Relatório Final e o Parecer.

Com base nas justificativas do gestor, o relatório é revisto e, quando a justificativa for aceita, a constatação é retirada. Caso contrário, mantida, inserindo-se também um resumo (ou íntegra, quando necessário) da justificativa do gestor.

O Parecer traz um breve resumo dos problemas encontrados e a opinião geral emitida pelo auditor sobre o objeto examinado.

Além destes produtos, há produtos secundários, porém, obrigatórios: organização dos papéis de trabalho, análise do que foi planejado em detrimento do que foi executado e documentação de lições aprendidas.

5. PROCEDIMENTOS DE CONTROLE DE ACESSO

Como visto no capítulo anterior, os procedimentos utilizados na auditoria podem ser feitos para o projeto específico ou escolhidos a partir de um banco de dados de procedimentos.

Neste capítulo, será apresentada uma metodologia para se produzir procedimentos acerca da verificação dos controles de acesso físico e lógicos dentro de uma organização. Nem todos os procedimentos aqui produzidos deverão ser utilizados obrigatoriamente em uma Auditoria de TI que inclua Controle de Acesso, subconjunto dos controles relacionados à Segurança da Informação. Essa escolha depende da extensão do escopo e da estrutura da organização auditada. Cabe à equipe de auditoria fazer essa avaliação e eventuais adaptações às necessidades reais.

O capítulo está dividido em quatro subitens: o item 5.1 apresenta a motivação de se abordar a Segurança da Informação em uma auditoria de TI, o item 5.2 apresenta conceitos básicos de Controle de Acesso, o item 5.3 demonstra a metodologia utilizada e o item 5.4 apresenta os procedimentos propriamente ditos.

5.1. SEGURANÇA DA INFORMAÇÃO E AUDITORIA

Para alcançar seus objetivos de negócio, a organização precisa investir, gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos de forma a prover serviços que geram a informação necessária ao negócio.

Tais processos e recursos de TI constituem a arquitetura de TI da organização. Por meio das habilidades das pessoas e da infra-estrutura tecnológica para executar as aplicações automatizadas de negócio, as informações necessárias são geradas. O COBIT divide esses recursos em quatro tipos: Aplicações, Informação, Infra-estrutura e Pessoas.

Para satisfazer os objetivos de negócio, a informação precisa estar em conformidade com certos critérios de controle da informação aos quais o COBIT se refere como requisitos de negócio para a informação: efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabiliadade.

A dependência crescente dos objetivos de negócio nas informações geradas pelos processos de TI tem acentuado a importância destes critérios. Por isso, seja qual for a forma na qual a informação se apresentada ou o meio pelo qual é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segundo a NBR ISO/IEC 17799:2005, Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Segundo a publicação de segurança do ITIL, segurança é o meio de se alcançar um nível aceitável de riscos residuais. O valor da informação deve ser protegido e este valor é medido em termos dos três critérios da informação relacionados à segurança: confidencialidade, integridade e disponibilidade.

Assim, a Segurança da Informação não é apenas uma meta de TI, mas um meio de se alcançar os objetivos de negócio. Por isso, nem toda informação ou todo serviço é igualmente importante dentro de uma organização. O nível de segurança da informação deve ser compatível com a importância da informação para a organização. O Decreto n.º 4.553 [ANEXO II: LEGISLAÇÃO APLICÁVEL À TI] dispõe sobre a classificação da informação dentro da Administração Pública.

Segundo a NBR ISO/IEC 17799:2005, a segurança das informações é obtida através da implementação de um conjunto adequado de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software. Esses controles precisam ser estabelecidos para assegurar que os objetivos de segurança específicos da organização sejam alcançados.

A Segurança da Informação é importante para os negócios e para a proteção das infra-estruturas críticas do setor público, evitando ou reduzindo os riscos mais relevantes. O aumento da dependência da Tecnologia da Informação na esfera governamental tem aumentado a necessidade da implementação de controles no que se diz respeito à segurança. Dois momentos devem ser considerados quando se analisa a Segurança da Informação na esfera pública:

1) Prevenção: Deve haver um esforço das entidades públicas de se implantar as diretrizes e controles de segurança da informação de forma a evitar problemas de confidencialidade, disponibilidade e integridade da informação a fim de garantir que as informações estejam disponíveis apenas a quem permitido,

2) Responsabilização: No caso da impossibilidade de se evitar problemas com a Segurança da Informação, devem sem implementados controles que permitam a detecção do incidente ocorrido e a descoberta do responsável pelo fato, independente de dolo ou culpa.

Diante da deficiência observada na esfera pública em se responsabilizar agentes causadores de incidentes de Segurança da Informação, pretende-se desenvolver procedimentos de auditoria que visem verificar a situação das entidades auditadas e recomendar melhorias com o foco de possibilitar maior controle das ações dos agentes públicos (em sentido amplo), de forma que, caso haja algum incidente, seja possível se responsabilizar alguém.

O que se observa atualmente é que, em muitos casos, não é possível sequer detectar tais incidentes, muito menos provar como ocorreram e apontar um culpado. Este fato aliado ao aumento da dependência da Tecnologia da Informação em operações governamentais de toda espécie demonstram a necessidade imediata de conscientização e criação de estratégias para a proteção dos ativos da informação.

A conscientização deve abranger todo tipo de agente, em todos os níveis de cargos e tipos de atividades. Entender que a informação é um ativo de propriedade da organização, assim como uma cadeira ou uma pasta de documentos contábeis é o primeiro

passo para a conscientização de que manipular informações importantes indevidamente é tão grave quanto adulterar documentos contáveis impressos em papel e de que levar informações a conhecimentos de pessoas não autorizadas é como furtar um patrimônio da organização. Este é um assunto de fundamental importância nos dias de hoje e está relacionado ao Direito Digital [94].

Uma forma de incentivar essa conscientização é a realização de Auditorias de Segurança da Informação. Por isso, os procedimentos aqui desenvolvidos são voltados justamente para a proteção de ativos. Entretanto, os procedimentos apresentados aqui, devido à grande extensão do assunto, não objetivam cobrir todos os critérios de Segurança da Informação, mas apenas o Controle de Acesso.

5.2. CONTROLE DE ACESSO

Nos dias de hoje, a interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.

O controle de acesso à informação é uma questão crítica dentro da Segurança da Informação e da APF, pois se tem observado que, muitas vezes, sua importância é diminuída ou desconsiderada. A informação é um ativo estratégico de toda organização (pública ou privada) e deve ser protegida de acordo com o seu nível de importância, sigilo e criticidade.

A NBR ISO/IEC 17799 possui um capítulo específico sobre Controle de Acesso. Por se tratar de uma norma brasileira, baseada na norma internacional ISO 17799, ela pode ser utilizada como linguagem comum entre o auditor e o auditado. Com isso, a adequação à norma pode ser foco de recomendação, possibilitando uma atuação pró-ativa do Controle no sentido não só de se descobrir irregularidades, mas também de se evitá-las.

5.3. METODOLOGIA

As principais bases utilizadas no desenvolvimento dos procedimentos deste trabalho são as publicações do COBIT e a NBR ISO/IEC 17799:2005. O COBIT foi escolhido se por tratar do modelo de Governança de TI mais abrangente e conhecido no mercado nacional e internacional e por englobar os modelos e padrões mais aceitos no mercado, inclusive a norma de segurança em questão. Além dessas bases, também foram utilizados, como subsídio, o ITIL [72] e a legislação brasileira [ANEXO II: LEGISLAÇÃO APLICÁVEL À TI].

Os procedimentos de Auditoria de TI podem ser criados independentemente de um projeto de auditoria já programado ou para uma auditoria específica.

No primeiro caso, os procedimentos são criados dentro do passo 3 da Programação de Trabalho da Auditoria, como detalhado no capítulo anterior. A vantagem é que os procedimentos já são criados de acordo com as especificidades da auditoria e no grau de detalhe adequado, apesar de o planejamento precisar de um tempo maior para ser realizado

Já no segundo caso, os procedimentos são armazenados em um banco de dados e utilizados sempre que necessários, de acordo com o escopo dos projetos. A vantagem é que quando da realização de uma auditoria, se gasta tempo apenas escolhendo os procedimentos aplicáveis ao escopo e adaptando-os, detalhando-os em procedimentos mais específicos ou agrupando-os em procedimentos mais genéricos, de acordo com a necessidade do projeto.

A metodologia utiliza os objetivos de controle do COBIT como referência e direcionamento para definir o escopo da auditoria de TI e para servir de linguagem comum dentro da organização auditora e entre auditor e auditado. Outro instrumento usado são os mapeamentos do COBIT [48][49][50][51][52][53][54][55] com outros modelos, disponibilizados no site da ISACA[75].

Para se criar procedimentos para execução de Auditoria em TI, devem ser seguidos, não necessariamente na mesma ordem, os seguintes passos criados durante o desenvolvimento desta pesquisa e baseados em diretrizes do *IT Assurance Guide*:

1. Definição dos Objetivos da Auditoria

2. Identificação dos Objetivos de Negócio

3. Identificação dos critérios da informação a serem focados na auditoria.

4. Identificação dos recursos de TI a serem focados na auditoria.

5. Identificação dos Objetivos de TI.

6. Identificação dos processos de TI.

7. Seleção dos objetivos de controle detalhados.

8. Levantamento de legislação, normas e padrões específicos acerca dos objetivos de controle selecionados.

9. Descrição dos procedimentos.

Neste trabalho, demonstraremos a aplicação da metodologia criando exemplos de procedimentos para serem inseridos em um banco de dados e não para um projeto de auditoria específico. Entretanto, os mesmos passos podem ser utilizados quando se tratar de um caso específico. Inclusive, os passos 1,2, 4, 5, 6 e 7 já pertencem a etapas do Planejamento de Auditoria.

Dependendo do foco da auditoria, a ordem de execução destes passos pode variar. Quando a auditoria é focada nos objetivos de negócio, esses passos devem ser executados

na ordem direta. Entretanto, quando for focada em aspectos operacionais, a ordem muda para 1, 8, 7, 3, 4, 6, 5, 2 e 9.

Ressalta-se que alguns desses passos podem parecer irrelevantes quando do desenvolvimento de procedimentos genéricos aplicáveis a qualquer auditoria. Entretanto, em casos específicos, eles devem ser realizados, inclusive por já fazerem parte do processo de planejamento.

5.3.1. Definição dos Objetivos da Auditoria

O primeiro passo consiste na definição do que se espera averiguar na auditoria. Este é o momento de se decidir se a Auditoria será focada na Governança de TI como um todo, ou no desenvolvimento de software, ou em terceirização de TI, ou em Segurança da Informação, ou apenas em um item específico como Controle de Acesso.

5.3.2. Identificação dos Objetivos de Negócio

Nesta etapa, define-se que objetivos de negócio, dentro do escopo da auditoria, devem ser alcançados dentro da organização auditada.

Com o objetivo de negócio definido com clareza e objetividade, devem-se identificar, dentro dos objetivos de negócio disponíveis no COBIT, aqueles que envolvam no todo ou em parte os objetivos de negócio definidos. O quadro de objetivos de negócio do COBIT pode ser visualizado no ANEXO V: TABELA COBIT deste trabalho.

No caso da Administração Pública, os objetivos de negócio apresentam um foco diferenciado dos da iniciativa privada. A informação, muitas vezes não é apenas um meio para se produzir um resultado, mas sim o próprio produto desejado. Por isso, muitas vezes, não será possível mapear os objetivos de negócio escolhidos dentro da tabela de objetivos

de negócio que faz parte dos anexos do COBIT [ANEXO VI: RELAÇÃO ENTRE OBJETIVOS DE NEGÓCIO E DE TI].

5.3.3. Identificação dos critérios da informação a serem focados na auditoria.

De acordo com os objetivos principais da auditoria, selecionar os principais critérios da informação a serem abordados. Caso não haja foco em critérios específicos, esse passo pode ser pulado. Como dito anteriormente, os critérios da informação são: efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade.

5.3.4. Identificação dos recursos a serem focados na auditoria.

De acordo com os objetivos principais da auditoria, selecionar os principais recursos de TI a serem abordados. Caso não haja foco em critérios específicos, esse passo pode ser pulado. Como dito anteriormente, os recursos de TI são: aplicações, informação, infra-estrutura e pessoas.

5.3.5. Identificação dos Objetivos de TI.

A partir dos critérios de informação priorizados e dos objetivos de negócio abordados, tendo sempre em mente os objetivos principais da auditoria, são identificados os objetivos de TI. O COBIT apresenta uma tabela de mapeamento entre seus Objetivos de Negócio de Objetivos de TI. A tabela original é apresentada no ANEXO VI: RELAÇÃO ENTRE OBJETIVOS DE NEGÓCIO E DE TI.

5.3.6. Identificação dos processos de TI.

A partir dos processos relacionados aos objetivos de TI, dos critérios de informação focados, do objetivo da auditoria e dos recursos abordados, selecionar os processos de TI que serão usados como base para a auditoria. O COBIT apresenta uma tabela de mapeamento entre seus Objetivos e Processos TI. A tabela original é apresentada no ANEXO VII: RELAÇÃO ENTRE OBJETIVOS DE TI E PROCESSOS.

5.3.7. Seleção dos objetivos de controle detalhados.

Analisar cada objetivo de controle detalhado para verificar se é um controle que deve existir a fim de garantir que a organização auditada, dentro do escopo da auditoria, atinja os objetivos determinados. Quando os procedimentos forem desenvolvidos para uma auditoria específica essa seleção é feita por meio de análise de risco, como explicado no capítulo anterior.

5.3.8. Levantamento de legislação, normas e padrões específicos acerca dos objetivos de controle selecionados.

Com base nos objetivos de controle detalhados, fazer levantamento de normas, padrões, modelos e legislação que possam subsidiar e sustentar o desenvolvimento de procedimentos de auditoria.

5.3.9. Descrição dos procedimentos.

A descrição dos procedimentos deve ser realizada de forma a nortear as buscas do auditor no momento da execução de testes. Os procedimentos devem conter:

- A descrição do controle a ser avaliado (não coincide, necessariamente, com os objetivos de controle do COBIT, podendo ser mais específicos ou genéricos);

- A fundamentação dessa verificação com a citação da lei, norma ou modelo de onde foi tirado o objetivo de controle;

- O procedimento a ser realizado para avaliação do controle (pode ser mais genérico ou mais detalhado, dependendo da necessidade); e

- Observações adicionais que, porventura, sejam necessárias.

5.4. DESENVOLVIMENTO DE PROCEDIMENTOS

5.4.1. Foco no objetivo de negócio

Quando se diz que uma auditoria terá foco nos objetivos de negócio, significa que o escopo para a definição de procedimentos será definido a partir de um objetivo de negócio, como demonstrado abaixo:

1) Objetivo da Auditoria:

Verificar o grau de proteção da informação dentro do órgão auditado.

2) Objetivos de Negócio:

Garantir a segurança das informações da organização.

3) Critérios da Informação focados:

Confidencialidade e Integridade.

4) Recursos de TI focados:

Pessoas, informação, infra-estrutura e aplicações.

5) Objetivos de TI:

- Objetivo principal: Garantir que informações críticas e confidenciais sejam protegidas daqueles que não deveriam acessá-las (objetivo de TI número 19 do COBIT);

- Objetivo secundário: Proteger os ativos de TI (objetivo de TI número 14 do COBIT);

- Objetivo secundário: Manter a integridade da infra-estrutura da informação e processamento (objetivo de TI número 26 do COBIT).

6) Processos de TI:

- Processos referentes ao objetivo número 19: PO6, DS5, DS11 e DS12.

- Processos referentes ao objetivo número 14: PO9, DS5, DS9, DS12.

- Processos referentes ao objetivo número 126: AI6 e DS5.

Como os critérios que compõem o escopo são apenas integridade e confidencialidade, pela análise do ANEXO V: TABELA COBIT, os processos PO6 e DS9 já podem ser excluídos. Considerando que o processo ME2 aborda os critérios escolhidos de forma secundária, por decisão de projeto, ele também será excluído. Como o escopo engloba os quatro tipos de recursos de TI, eles não constituem filtro de exclusão de processos.

Além disso, ao considerarmos a importância dos objetivos de TI escolhidos, também por decisão de projeto, podemos escolher priorizar os processos do Objetivo de TI número 19, com exceção do PO6, já eliminado.

Portanto, os processos selecionados são:

→ DS5 Garantir a segurança dos sistemas;

→ DS11 Gerenciar dados; e

→ DS12 Gerenciar o ambiente físico.

7) Objetivos de controle detalhados:

A Tabela 5.1 mostra os objetivos de controle relativos a cada processo selecionado no passo anterior:

Tabela 5.1 – Objetivos de Controle

PROCESSOS	OBJETIVOS DE CONTROLE
DS5 Garantir a segurança dos sistemas	DS5.1 Gerenciamento de Segurança de TI DS5.2 Planejamento de Segurança de TI DS5.3 Gerenciamento de Identidade DS5.4 Gerenciamento de Contas de Usuário DS5.5 Teste, Inspeção e Monitoramento de Segurança DS5.6 Definição de Incidente de Segurança DS5.7 Proteção de Tecnologia de Segurança DS5.8 Gerenciamento de Chaves Criptográficas DS5.9 Prevenção, Detecção e Correção de *Softwares* Maliciosos DS5.10 Segurança de Rede DS5.11 Troca de Dados Sensíveis
DS11 Gerenciar dados	DS11.1 Requisitos de Negócio para Gerenciamento de Dado DS11.2 Arranjos de Retenção e Armazenamento DS11.3 Sistemas de Gerenciamento de Biblioteca de Mídias DS11.4 Descarte DS11.5 *Backup* e Restauração DS11.6 Requisitos de Segurança para gerenciamento de Dados
DS12 Gerenciar o ambiente físico	DS12.1 Seleção e *Layout* de Local DS12.2 Medidas de Segurança Física DS12.3 Acesso Físico DS12.4 Proteção contra Fatores Ambientais DS12.5 Gerenciamento de Facilidades Físicas

A partir destes objetivos de controle, em combinação com as normas, padrões e legislação aplicáveis, desenvolvem-se os procedimentos de auditoria. Se houvesse um projeto em questão, os pontos críticos do objeto seriam utilizados para nortear a escolho dos objetivos de controle a serem focados.

Neste momento, escolheremos o objetivo de controle DS5.3 do processo DS5 para usar como exemplo no desenvolvimento de procedimentos.

Primeiramente, é importante se conhecer uma descrição do processo, retirada do COBIT 4.1:

→ DS5 Garantir a Segurança dos Sistemas

A necessidade de manter a integridade da informação e de proteger os ativos de TI requer um processo de gerenciamento de segurança. Esse processo inclui o estabelecimento e manutenção de papéis e responsabilidades, políticas, padrões e

procedimentos de segurança de TI. Gerenciamento de segurança também inclui monitoramento de segurança, testes periódicos e implementação de ações corretivas para fragilidades e incidentes de segurança. Gerenciamento efetivo de segurança protege todos os ativos de TI para minimizar o impacto de negócio de vulnerabilidades e incidentes de segurança.

O *IT Assurance Guide* apresenta para os objetivos de controle de cada processo: descrição dos objetivos de controle, guias de valor, guias de risco, testes genéricos a serem aplicados para testar o *design* dos controles, passos genéricos (válidos para todos os objetivos de controle de um processo) para testar as saídas dos objetivos de controle e passos para a documentação do impacto das fragilidades de controle.

Os objetivos de controle definem o objetivo de se implantar o controle em questão, sendo as orientações que descrevem o que deve ser cumprido para governança de TI.

Os guias de valores indicam benefícios a serem agregados à organização com o aperfeiçoamento do controle em questão.

Os guias de risco indicam os riscos a serem evitados pelo aperfeiçoamento do controle em questão.

Os testes de *design*, passos para testes de saídas dos objetivos de controle e passos para documentação do impacto das fragilidades de controle não serão transcritos neste trabalho, mas podem ser usados como auxílio durante uma auditora.

8) Legislação, Normas e Padrões escolhidos:

O *site* da ISACA disponibiliza para associados mapeamentos entre o COBIT e outros padrões, modelos e normas de mercado [53][49][51][52][48][54][55][50][47][41].

A Tabela 5.2 mostra os controles da norma NBR ISO/IEC 17799 que dão subsídio para o alcance do objetivo de controle em questão.

Tabela 5.2 – Relação entre COBIT e NBR ISO/IEC 17799
Adaptada de [50]

Objetivo de Controle do Cobit		Requisitos (NBR ISO/IEC 17799)
DS5.3	Gerenciamento de identidade.	11.2.3 Gerenciamento de senhas do usuário 11.3.1 Uso de senhas 11.4.1 Políticas de uso dos serviços de rede 11.5.1 Procedimentos seguros de entrada no sistema (*log-on*) 11.5.2 Identificação e autenticação do usuário 11.5.3 Sistema de gerenciamento de senha 11.5.5 Desconexão de terminal por inatividade 11.5.6 Limitação de horário de conexão 11.6.1 Restrição de acesso à informação

De acordo com a extensão da auditoria, os procedimentos podem ser mais detalhados ou genéricos, podendo agrupar mais de um requisito um mesmo item de verificação.

Neste trabalho, apresentaremos procedimentos de forma detalhada, mas mostrando o que deve ser verificado e não a forma de verificação.

9) Modelo de Procedimentos:

Os procedimentos apresentados iniciam-se com a descrição do objetivo de controle, guias de valor e guias de risco, dados retirados do *IT Assurance Guide*. Em seguida, são listados os requisitos que devem ser observados para análise do objetivo de controle em questão. No caso deste trabalho, os requisitos são retirados da norma NBR ISO/IEC 17799, de forma a detalhar os controles do *IT Assurance Guide*. Assim, como base em tais requisitos, foram desenvolvidos os procedimentos propriamente ditos.

Este modelo de procedimentos refere-se ao objetivo de controle DS5.3 do COBIT 4.1.

Objetivo de Controle:

DS5.3 Gerenciamento de Identidades (Fonte: *IT Assurance Guide*)

- Garantir que todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicações de negócio, ambiente de TI, operações de sistemas, desenvolvimento e manutenção) sejam identificáveis de forma única.
- Disponibilizar identidades de usuários por mecanismos de autenticação.
- Confirmar que os direitos de acesso dos usuários a sistemas e dados estão em acordo com os requisitos de negócio definidos e documentados e que os requisitos de trabalho estão amarrados às identidades dos usuários.
- Garantir que os direitos de acesso dos usuários são solicitados pela gerência de usuários, aprovados pelos proprietários dos sistemas e implementados pelo pessoal responsável pela segurança.
- Manter as identidades e direitos de acesso dos usuários em repositório central.
- Desenvolver medidas técnicas e procedimentais de custo efetivo e mantê-las atualizadas para estabelecer identificação de usuário, implementar autenticação e reforçar direitos de acesso.

Guias de Valores (Fonte: *IT Assurance Guide*):

- Implementação efetiva de mudanças.
- Investigação apropriada de atividades de acesso impróprias.
- Comunicação segura garantindo transações de negócio aprovadas.

Guias de Risco (Fonte: *IT Assurance Guide*):
- Mudanças não autorizadas em hardware e software.
- Falhas de requisitos de negócio pelo gerenciamento de acesso e comprometimento de segurança de sistemas de negócio críticos.
- Falta de especificação de requisitos de segurança de segurança para todos os sistemas.
- Violação de segregação de responsabilidade.
- Comprometimento de informações de sistemas.

Requisitos de verificação:

Código: 001

Título: Gerenciamento de acesso do usuário: Gerenciamento de senha do usuário.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que a concessão de senhas seja controlada através de um processo de gerenciamento formal".

Procedimento:
- Verificar a existência de processo de gerenciamento formal de senhas e a sua aplicação prática com base em documentos e entrevistas com usuários e administradores.
- Analisar o processo a fim de averiguar se este possui os requisitos apresentados no item 11.2.3 da norma em questão.
- Verificar as formas de proteção das senhas armazenadas nos sistemas.

Fundamentação: Item 11.2.3 da norma NBR ISO/IEC 17799:2005.

Código: 002

Título: Responsabilidades dos usuários: Uso de senhas.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas".

Procedimento:
- Solicitar ao gestor comprovação (diretrizes internas, mensagens eletrônicas, ocorrência de palestras) de que os usuários são informados sobre as boas práticas de segurança da informação em relação à seleção e uso de senhas, de acordo com as diretrizes de implementação do item 11.3.1 da norma em questão.
- Entrevistar uma amostra de usuários questionando sobre a divulgação interna das boas práticas e sobre o conhecimento absorvido. Para tal entrevista, elaborar um questionário padrão para posterior consolidação das respostas dos entrevistados.

Fundamentação: Item 11.3.1 da norma NBR ISO/IEC 17799:2005.

Código: 003

Título: Controle de acesso à rede: Política de uso dos serviços de rede.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar".

Procedimento:
- Verificar a existência de política relativa ao uso de redes e serviços de redes e, caso exista, observar se as diretrizes do item 11.4.1 da norma referida estão contempladas.
- Verificar se não existem inconsistências entre as políticas de uso de serviço de rede e de controle de acesso do negócio.

Fundamentação: Item 11.4.1 da norma NBR ISO/IEC 17799:2005.

Código: 004

Título: Controle de acesso ao sistema operacional: Procedimentos seguros de entrada no sistema (*log-on*).

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que o acesso aos sistemas operacionais seja controlado por um procedimento seguro de entrada no sistema (*log-on*)".

Procedimento:
- Verificar se o procedimento de entrada no sistema (*log-on*) está de acordo com as diretrizes enumeradas no item 11.5.1 da norma em questão.

- Verificar a existência de históricos (*logs*) da última entrada bem sucedida e detalhes de qualquer tentativa de entrada sem sucesso desde a última entrada com sucesso.
- Verificar se as senhas não são transmitidas em texto claro pela rede.

Fundamentação: Item 11.5.1 da norma NBR ISO/IEC 17799:2005.

Código: 005

Título: Controle de acesso ao sistema operacional: Identificação e autenticação de usuário.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário".

Procedimento:
- Verificar se todos os usuários, inclusive os responsáveis pela manutenção da área tecnológica, possuem o seu identificador único.
- Avaliar a técnica usada para a validação da identidade alegada por um usuário (tais como senhas, cartões inteligentes, meios biométricos, entre outros), considerando sempre o nível de sensibilidade da informação.
- Verificar, também, se os identificadores de usuários podem ser usados para responsabilizar os usuários por suas atividades. Assim, em caso de atividades suspeitas, inadequadas ou maliciosas, o usuário pode ser identificado para iniciar a adoção de providências administrativas e legais, se for o caso. Considerar as diretrizes do item 11.5.2 da norma em questão para a avaliação deste controle.

Observações: Segundo o Decreto n.º 4.553, os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos. É importante verificar a existência de dados sigilosos no momento da análise deste controle.

Fundamentação: Item 11.5.2 da norma NBR ISO/IEC 17799:2005.

Código: 006

Título: Controle de acesso ao sistema operacional: Sistema de gerenciamento de senha.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade".

Procedimento:
- Verificar a qualidade do sistema de gerenciamento de senhas, observando se a senha é associada a um identificador de usuário individual, se as senhas não são mostradas na tela ao serem digitadas, se são transmitidas criptografadas pela rede, se o sistema obriga o usuário a escolher senhas de qualidade, entre outras diretrizes importantes citadas no item 11.5.3 da referida norma.

Fundamentação: Item 11.5.3 da norma NBR ISO/IEC 17799:2005.

Código: 007

Título: Controle de acesso ao sistema operacional: Desconexão de terminal por inatividade.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que terminais sejam desconectados após um período definido de inatividade".

Procedimento:
- Verificar se existe desconexão por tempo de inatividade e, caso exista, se seguem as diretrizes do item 11.5.5 da norma, considerando a sensibilidade das informações disponíveis e os riscos relacionados com as aplicações utilizadas e os riscos para usuário habitual do terminal.

Observações: Segundo o Decreto n.º 4.553, os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos. É importante verificar a existência de dados sigilosos no momento da análise deste controle.

Fundamentação: Item 11.5.5 da norma NBR ISO/IEC 17799:2005.

Código: 008

Título: Controle de acesso ao sistema operacional: Limitação de horário de conexão.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que restrições nos horários de conexão sejam utilizadas para proporcionar segurança adicional para aplicações de alto risco".

Procedimento:
- Verificar se as conexões de aplicativos de alto risco possuem horário limite de conexão, a fim de diminuir a exposição de tais aplicativos.

Fundamentação: Item 11.5.6 da norma NBR ISO/IEC 17799:2005.

Código: 009

Título: Controle de acesso à aplicação e à informação: Restrições de acesso à informação.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte seja restrito de acordo com o definido na política de controle de acesso".

Procedimento:

- Verificar se requisitos de restrição de acesso à informação e às funções dos sistemas de aplicações são aplicados e qual a adequação de tais requisitos em relação à política de controle de acesso da organização.
- Observar a aplicação dos controles enumerados no item 11.6.1 da norma.
Observações: A Lei n.º 9.983, de 14 de julho de 2000 altera o Código Penal de forma a prever penas específicas para crimes de inserção, alteração, exclusão e divulgação indevidas de dados nos sistemas informatizados ou bancos de dados da Administração Pública.

Fundamentação: Item 11.6.1 da norma NBR ISO/IEC 17799:2005.

5.4.2. Foco em aspectos operacionais

Quando se diz que uma auditoria terá foco em aspectos operacionais, significa que o escopo para a definição de procedimentos será definido a partir de questões operacionais específicas, como demonstrado abaixo. Entretanto, isto se refere apenas ao modo como os procedimentos de auditoria serão criados, ou seja, não deixa de existir a necessidade de que a TI do órgão auditado esteja alinhada com os objetivos de negócio do órgão.

Tais procedimentos, apesar de planejados com base em aspectos operacionais, só serão aplicados se a garantia da existência desses controles for importante para o alcance dos objetivos de negócio do órgão auditado.

1) Objetivo da Auditoria:

Avaliar a efetividade dos controles de acesso, tanto físico como lógico.

2) Legislação, Normas e Padrões escolhidos:

O sítio da ISACA disponibiliza para associados mapeamentos entre o COBIT e outros padrões, modelos e normas de mercado. A partir desse mapeamento, foi desenvolvido outro em que todas os requisitos da NBR ISO/IEC 17799 referentes a Controle de Acesso foram mapeados dentro dos processos e objetivos de controle do COBIT, como mostra a Tabela 5.3. Sob esta ótica, mapeia-se tudo que existe dentro do COBIT acerca de Controle de Acesso, mas a recíproca não acontece, pois estes requisitos, sozinhos, nem sempre cobrem por completo os objetivos de controle do COBIT envolvidos.

Tabela 5.3 – Mapeamento de Controle de Acesso
Adaptada de [50]

MAPEAMENTO DE CONTROLE DE ACESSO		
Objetivo de Controle do COBIT		**Requisitos (NBR ISSO/IEC 17799)**
PO2	**Definir a arquitetura da informação.**	
PO2.1	Modelo da arquitetura da informação da organização.	11.1.1 Política de Controle de Acesso
PO2.3	Esquema de classificação de dados.	11.1.1 Política de Controle de Acesso
PO4	Definir a organização de TI, seus processos e relacionamentos.	
PO4.14	Procedimentos e políticas de contratação de pessoal.	9.1.5 Trabalhando em Áreas Seguras
PO6	**Comunicar objetivos e direcionamentos gerenciais.**	
PO6.2	Framework de controle interno e risco de TI da organização.	8.3.2 Devolução de Ativos 9.1.5 Trabalhando em Áreas Seguras 9.2.7 Remoção de Propriedade 11.1.1 Política de Controle de Acesso 11.3.1 Uso de senhas 11.3.2 Equipamento de usuário sem monitoração 11.3.3 Política de mesa limpa e tela limpa 11.7.1Computação e comunicação móvel 11.7.2 Trabalho remoto
PO7	**Gerenciar os recursos humanos.**	
PO7.8	Término e mudança de tarefa.	8.3.2 Devolução de Ativos 8.3.3 Retirada de direitos de acesso
AI1	**Identificar soluções automatizadas.**	
AI1.2	Relato de análise de risco.	11.6.2 Isolamento de sistemas sensíveis
AI2	**Adquirir e manter software aplicativo.**	
AI2.4	Segurança e disponibilidade de aplicação.	11.6.2 Isolamento de sistemas sensíveis
AI3	**Adquirir e manter infra-estrutura tecnológica.**	
AI3.3	Manutenção de infra-estrutura.	9.1.5 Trabalho remoto em áreas seguras 9.2.4 Manutenção dos equipamentos

AI6	**Gerenciar mudanças.**	
AI6.3	Mudanças emergenciais.	11.5.4 Uso de utilitários de sistema
AI7	**Instalar e aprovar soluções e mudanças.**	
AI7.10	Distribuição de sistema.	9.1.6 Acesso do público, áreas de entrega e de carregamento
DS5	**Garantir a segurança dos sistemas.**	
DS5.2	Plano de Segurança de TI.	11.1.1 Política de Controle de Acesso 11.7.1 Computação e comunicação móvel 11.7.2 Trabalho remoto
DS5.3	Gerenciamento de identidade.	11.2.3 Gerenciamento de senhas do usuário 11.3.1 Uso de senhas 11.4.1 Políticas de uso dos serviços de rede 11.5.1 Procedimentos seguros de entrada no sistema (*log-on*) 11.5.2 Identificação e autenticação do usuário 11.5.3 Sistema de gerenciamento de senha 11.5.5 Desconexão de terminal por inatividade 11.5.6 Limitação de horário de conexão 11.6.1 Restrição de acesso à informação
DS5.4	Gerenciamento de contas de usuário.	8.3.3 Retirada de direitos de acesso 11.1.1 Política de Controle de Acesso 11.2.1 Registro de usuário 11.2.2 Gerenciamento de privilégios 11.2.4 Análise crítica dos direitos de acesso de usuário 11.3.1 Uso de senhas 11.5.1 Procedimentos seguros de entrada no sistema (*log-on*) 11.5.3 Sistema de gerenciamento de senha 11.6.1 Restrição de acesso à informação
DS5.7	Proteção de tecnologia de segurança.	9.1.6 Acesso do público, áreas de entrega e de carregamento 9.2.1 Instalação e proteção de equipamento 9.2.3 Segurança do cabeamento 11.3.2 Equipamento de usuário sem monitoração 11.3.3 Política de mesa limpa e tela limpa 11.4.3 Identificação de equipamento em redes 11.4.4 Proteção e configuração de portas de diagnóstico remotas 11.5.1 Procedimentos seguros de entrada no sistema (*log-on*) 11.5.4 Uso de utilitários de sistema 11.5.5 Desconexão de terminal por inatividade 11.5.6 Limitação de horário de conexão 11.6.2 Isolamento de sistemas sensíveis 11.7.1 Computação e comunicação móvel 11.7.2 Trabalho remoto
DS5.10	Segurança de Rede.	11.4.1 Políticas de uso dos serviços de rede 11.4.2 Autenticação para conexão externa do usuário 11.4.3 Identificação de equipamento em redes 11.4.4 Proteção e configuração de portas de diagnóstico remotas 11.4.5 Segregação de redes 11.4.6 Controle de conexão de rede 11.4.7 Controle de roteamento de redes

		11.6.2 Isolamento de sistemas sensíveis
DS5.11	Troca de dados sensíveis.	11.4.2 Autenticação para conexão externa do usuário
DS9	**Gerenciar configuração.**	
DS9.2	Identificação e manutenção de itens de configuração.	11.4.3 Identificação de equipamento em redes
DS11	**Gerenciar dados.**	
DS11.4	Descarte.	9.2.6 Reutilização e alienação segura de equipamentos
DS12	**Gerenciar o ambiente físico.**	
DS12.1	Seleção e *layout* de local.	9.1.1 Perímetro de segurança física 9.1.3 Segurança em escritórios, salas e instalações 9.1.6 Acesso do público, áreas de entrega e de carregamento
DS12.2	Medidas de segurança física.	9.1.1 Perímetro de segurança física 9.1.2 Controles de entrada física 9.1.3 Segurança em escritórios, salas e instalações 9.2.5 Segurança de equipamentos fora das dependências da organização 9.2.7 Remoção de Propriedade
DS12.3	Acesso físico.	9.1.2 Controles de entrada física 9.1.5 Trabalhando em Áreas Seguras 9.1.6 Acesso do público, áreas de entrega e de carregamento 9.2.5 Segurança de equipamentos fora das dependências da organização
DS12.4	Proteção contra fatores ambientais.	9.1.4 Proteção contra ameaças externas e do meio ambiente 9.2.1 Instalação e proteção de equipamento 9.2.2 Utilidades 9.2.3 Segurança do cabeamento
DS12.5	Gerenciamento de facilidades físicas.	9.2.2 Utilidades 9.2.4 Manutenção dos equipamentos
DS13	**Gerenciar operações.**	
DS13.5	Manutenção preventiva para *hardware*.	9.2.4 Manutenção dos equipamentos

De acordo com a extensão da auditoria, os procedimentos podem ser mais detalhados ou genéricos, podendo agrupar mais de um requisito um mesmo item de verificação.

3) Objetivos de controle detalhados:

Os objetivos de controle selecionado são todos os itens da norma NBR ISO/IEC 17799 que se encontram na coluna de requisitos da Tabela 5.3. Ressalta-se que os objetivos

de controle podem ser mapeados em vários níveis. Neste caso, são objetivos de controle operacionais, que são traduzidos, na mesma tabela, para os objetivos de controle do COBIT.

4) Critérios da Informação focados:

Confidencialidade e Integridade.

5) Recursos de TI focados:

Pessoas, informação, infra-estrutura e aplicações.

6) Processos de TI:

Os processos selecionados são resultantes do mapeamento de todos os controles da norma NBR ISO/IEC 17799 [50] referentes a controle de acesso junto aos processos do COBIT e Objetivos de controle do COBIT.

Entretanto, deve ficar claro que os objetivos de controle selecionados no item 3 são suficientes para atender ao objetivo da auditoria referente a Controle de Acesso, mas não quer dizer que eles garantem o funcionamento de todos os processos abaixo por inteiro, pois, na maioria das vezes, são apenas parte de um conjunto bem maior de controles necessários para atender ao processo.

Como resultado, apresentado na Tabela 5.3, tem-se os processos:

- PO2 Definir a arquitetura da informação;
- PO4 Definir a organização de TI, seus processos e relacionamentos;
- PO6 Comunicar objetivos e direcionamentos gerenciais;
- PO7 Gerenciar os recursos humanos;
- AI1 Identificar soluções automatizadas;
- AI2 Adquirir e manter software aplicativo;
- AI3 Adquirir e manter infra-estrutura tecnológica;
- AI6 Gerenciar mudanças;
- AI7 Instalar e aprovar soluções e mudanças;
- DS5 Garantir a segurança dos sistemas;
- DS9 Gerenciar configuração;
- DS11 Gerenciar dados;
- DS12 Gerenciar o ambiente físico; e
- DS13 Gerenciar operações.

7) Objetivos de TI:

- Objetivo principal: Garantir que informações críticas e confidenciais sejam protegidas daqueles que não deveriam acessá-las (objetivo de TI número 19 do COBIT);

- Objetivo secundário: Proteger os ativos de TI (objetivo de TI número 14 do COBIT);

- Objetivo secundário: Manter a integridade da infra-estrutura da informação e processamento (objetivo de TI número 26 do COBIT).

8) Objetivos de Negócio:

Garantir o acesso seguro às informações da organização.

9) Procedimentos:

Para efeito de exemplificação, neste trabalho, apenas detalharemos os procedimentos relativos aos requisitos relacionados ao objetivo de controle COBIT DS12.2 Medidas de Segurança Física, pertencente ao processo DS12 Gerenciar o ambiente físico, cuja descrição no COBIT 4.1 é:

→ Proteção para equipamentos e pessoal requer facilidades físicas bem planejadas e gerenciadas. O processo de gerenciamento do ambiente físico inclui a definição de requisitos do local físico, seleção de instrumentos apropriados e arquitetura de processos efetivos para monitoramento dos fatores ambientais e gerenciamento do acesso físico. Gerenciamento efetivo do ambiente físico reduz interrupções de negócio decorrentes de dano a equipamentos e pessoal.

Os procedimentos apresentados iniciam-se com a descrição do objetivo de controle, guias de valor e guias de risco. Em seguida, são listados os requisitos, retirados da NBR ISO/IEC 17799, que devem ser observados para análise do objetivo de controle em questão e são a base dos procedimentos propriamente ditos.

Objetivo de Controle
DS12 Gerenciamento de Ambiente Físico

DS12.2 Medidas de Segurança Física (Fonte: *IT Assurance Guide*)
- Definir e implementar medidas de segurança física alinhadas com os requisitos de negócio para dar segurança ao local e aos ativos físicos.
- Medidas de segurança física devem ser capazes de, efetivamente, prevenir, detectar e mitigar riscos relacionados a roubo, temperatura, fogo, fumaça, água, vibração, terror, vandalismo, fortes interrupções, químicas e explosivos.

Guias de Valores (Fonte: *IT Assurance Guide*)
- Proteção contra roubos físicos de sistemas de TI críticos.
- Implantação efetiva de medidas de segurança física.
- Promoção de conscientização dentro do grupo de trabalho e da gerência sobre os requisitos organizacionais para segurança física.

Guias de Risco (Fonte: *IT Assurance Guide*)
- Ameaças à segurança física não identificadas.
- Roubo de hardware por pessoas não autorizadas.
- Ataque físico ao local de TI.
- Dispositivos reconfigurados sem autorização.
- Informações confidenciais acessadas por dispositivos configurados para ler informações enviadas por computador por via aérea.

Requisitos de verificação:

Código: 001

Título: Áreas seguras: perímetro de segurança física.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que sejam utilizados perímetros de segurança (barreiras tais como parede, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação" e "convém que seja projetada e aplicada segurança física para escritórios, salas e instalações".

Procedimento:
- Verificar, de acordo com a criticidade e sensibilidade dos ativos e dos recursos de processamento de informação da organização, o nível de adequação das proteções físicas

implementados na organização de acordo com as diretrizes do item 9.1.1 e do item 9.1.3 da referida norma.

Fundamentação: Itens 9.1.1 e 9.1.3 da norma NBR ISO/IEC 17799:2005.

Código: 002

Título: Áreas seguras: Controle de entrada física.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso".

Procedimento:
- Verificar a adequação dos controles de entrada de pessoas na organização, principalmente nas áreas que armazenem e tratem informações sensíveis, de acordo com as diretrizes do item 9.1.2 da norma e com a classificação da informação dentro do órgão.
- Realizar testes, com autorização da alta administração da organização, para verificar se os controles são efetivamente implementados.
- Analisar os registros de entrada e saída de visitantes a fim de analisar sua adequação com o tipo de informação a ser protegida.

Observações: Segundo o Decreto n.º 4.553, os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos. É importante verificar a existência de dados sigilosos no momento da análise deste controle.

Fundamentação: Item 9.1.2 da norma NBR ISO/IEC 17799:2005.

Código: 003

Título: Segurança de equipamentos: Segurança de equipamentos fora das dependências da organização.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que sejam tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização".

Procedimento:
- Verificar se há autorização da gerência para trabalhos com equipamentos fora da organização e verificar se há diretrizes para sua utilização. Na avaliação destas, considerar as diretrizes do item 9.2.5 da referida norma.

Observações: Considerar que devem ser verificados os controles sobre todas as formas de armazenamento de informações que sejam retirados das dependências da organização: computadores, agendas, telefones celulares, *smart cards*, papéis, *pendrives*, mídias, entre outras.

Fundamentação: Item 9.2.5 da norma NBR ISO/IEC 17799:2005.

Código: 004

Título: Segurança de equipamentos: Remoção de propriedade.

Descrição do controle: Segundo a NBR ISO/IEC 17799:2005, "convém que equipamentos, informações ou *software* não sejam retirados do local sem autorização prévia".

Procedimento:
- Verificar se há procedimentos definidos para o controle de entrada e saída de equipamentos, informações ou *softwares* da organização e se tais procedimentos estão de acordo com as diretrizes do item 9.2.7 da norma.

Observações:
- O controle de saída protege a organização contra perdas e possibilita a identificação de responsável no caso de extravio de algum ativo. Já o registro de entrada permite o controle da organização da localização de seus ativos e protege a pessoa portadora do ativo de ser responsabilizada se ocorrer algum incidente com o ativo após a devolução.
- Considerar que devem ser verificados os controles sobre todas as formas de armazenamento de informações que sejam retirados das dependências da organização: computadores, agendas, telefones celulares, *smart cards*, papéis, *pendrives*, mídias, entre outras.
- A Lei n.º 9.983, de 14 de julho de 2000 altera o Código Penal de forma a prever penas específicas para crimes de inserção, alteração, exclusão e divulgação indevidas de dados nos sistemas informatizados ou bancos de dados da Administração Pública.

Fundamentação: Item 9.2.7 da norma NBR ISO/IEC 17799:2005

6. CONCLUSÃO

Objetivando alcançar os objetivos propostos na Introdução, neste trabalho, realizou-se um levantamento das melhores práticas, padrões e normas nacionais e internacionais relativos aos processos de TI. A partir daí, foi proposta uma metodologia de planejamento de Auditoria de TI, cuja espinha dorsal é o *framework* do COBIT.

Além disso, foi proposta uma metodologia de desenvolvimento de procedimentos para serem utilizados como subsídio nos trabalhos de campo também baseados nas diretrizes do COBIT e complementados pelas normas e padrões nacionais e internacionais.

O uso do COBIT como base, aliado às outras práticas de mercado, possibilita uma abordagem abrangente por envolver praticamente todas as áreas da Tecnologia da Informação. Já as melhores práticas do mercado possibilitaram dar maior detalhamento aos controles, descendo a níveis operacionais e técnicos.

Assim, a pesquisa aqui desenvolvida contribui para dar uma visão geral de como se implantar Auditoria de TI nos órgãos de controle governamental e de como se desenvolver procedimentos que visem a verificação dos controles de acordo com objetivos de negócio de cada órgão auditado, de forma que não sejam exigidos controles desnecessários ou que não se deixe de analisar algo essencial.

O uso de padrões e modelos bem conhecidos também possibilita que seja criada uma linguagem comum de auditoria que permita que o órgão auditor trabalhe de forma homogênea e padronizada, que possa ser entendido pelo órgão auditado e que este órgão possa tomar medidas preventivas de controle interno, antes mesmo de ser fiscalizado, por já serem de conhecimento público os controles exigidos na fiscalização.

Outra questão importante abordada, dada a facilidade de acesso à informação, foi a Segurança da Informação dentro dos órgãos da APF, especificamente Controle de Acesso.

É possível se observar, pelo tipo de procedimentos descritos, que há como se implantar controles que possibilitem proteger as informações e detectar incidentes de segurança. Uma Auditoria de Segurança da Informação bem realizada pode diminuir as chances de incidentes de segurança e garantir que sejam implantados controles que, na impossibilita de prevenção de incidente, identifiquem sua ocorrência e os seus responsáveis por meio das trilhas de auditoria.

Portanto, observa-se que existe uma vasta base de boas soluções que podem ser adaptadas para os órgãos da APF a fim de melhorar a Governança de TI e de possibilitar, por meio da metodologia proposta, o efetivo controle dos processos de TI por parte do Sistema de Controle da APF.

Além disso, é necessário um apoio da Alta Administração do governo, de forma que sejam tomadas medidas integradas e concretas no sentido de dar suporte e direcionamento aos gestores de TI e fortalecimento das Auditorias de TI dentro dos órgãos de controle.

Com isso, espera-se ter um Controle que ajude a Administração Pública a manter uma Tecnologia de Informação que torne os processos de negócio dos órgãos mais eficientes e eficazes, diminua o desperdício de recursos públicos, evite desvios e fraudes e ajude na responsabilização de agentes corruptos.

Por fim, como trabalhos futuros, sugerem-se:

- A realização de auditorias-piloto para testar a metodologia proposta, melhorando-a e adaptando-a no que for necessário;

- A criação de um banco de dados de procedimentos, organizados por áreas de Auditoria de TI (item 2.3), genéricos o suficiente para serem aplicados em diversos projetos e específicos o suficiente para conduzirem adequadamente o processo de fiscalização;

- O levantamento de requisitos e o desenvolvimento de um sistema de apoio de acompanhamento de Auditoria de TI dentro da APF que incorpore as melhores práticas e legislação aplicável, que permita o armazenamento de procedimentos criados e que facilite o cadastro de constatações durante o trabalho de campo e posterior geração de relatório.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ABNT. NBR ISO/IEC 12207:1995: Tecnologia da Informação – Processos de ciclo de vida de software, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[2] ABNT. NBR ISO/IEC 12207:1995: Tecnologia da Informação – Processos de ciclo de vida de software. Associação Brasileira de Normas Técnicas.

[3] ABNT. NBR ISO/IEC 14598-1: Tecnologia da Informação – Avaliação de produto de software – Parte 1: Visão Geral, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[4] ABNT. NBR ISO/IEC 14598-2: Engenharia de Software – Avaliação de produto – Parte 2: Planejamento e Gestão, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[5] ABNT. NBR ISO/IEC 14598-3: Engenharia de Software – Avaliação de produto – Parte 3: Processo para desenvolvedores, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[6] ABNT. NBR ISO/IEC 14598-4: Engenharia de Software – Avaliação de produto – Parte 4: Processo para adquirentes, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[7] ABNT. NBR ISO/IEC 14598-5: Tecnologia de Informação – Avaliação de produto de software – Parte 5: Processo para avaliadores, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[8] ABNT. NBR ISO/IEC 14598-6: Engenharia de Software – Avaliação de produto – Parte 6: Documentação de módulos de avaliação, Rio de Janeiro, Associação Brasileira de Normas Técnicas.

[9] 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.

[10] ABNT. NBR ISO/IEC 27001:2006: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. Associação Brasileira de Normas Técnicas.

[11] ABNT. NBR ISO/IEC 9126-1: Engenharia de Software – Qualidade de produto – Parte 1: Modelo de Qualidade, Associação Brasileira de Normas Técnicas.

[12] AIPC, AU Section 312 - Audit Risk and Materiality in Conducting an Audit, 2006.

[13] ALBUQUERQUE, F.F.T. A Auditoria Operacional e seus desafios: Um estudo a partir da experiência do Tribunal de Contas da União, Salvador, 2006

[14] ALEXANDRINO, M.; PAULO, V. Direito Administrativo, Rio de Janeiro, Editora Impetus, 13ª Edição, 2007.

[15] AU 312 - AICPA. Audit Risk and Materiality in Conducting an Audit, SAS n-47, Nova Iorque, 1983.

[16] CMU. CMU/SEI-2001-TR028 – Capability Maturity Model Integration (CMMI), Version 1.1 – Software Engineering (Continuous Representation)

[17] CMU. CMU/SEI-2001-TR028 – Capability Maturity Model Integration (CMMI), Version 1.1 – Software Engineering (Staged Representation)

[18] CMU. CMU/SEI-2001-TR-034 – Appraisal Requirements for CMMI, Version 1.1 (ARC) – December/2001.

[19] COMITÊ DA BASILÉIA SOBRE SUPERVISÃO BANCÁRIA, Metodologia dos Princípios Básicos, 1999

[20] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, COSO: Gerenciamento de Riscos Corporativos - Estrutura Integrada, AUDIBRA, 2007

[21] CONSELHO FEDERAL DE CONTABILIDADE. BBC T 12 - Da Auditoria Interna, 1995.

[22] CONSELHO FEDERAL DE CONTABILIDADE. NBC P 1 – Normas Profissionais de Auditor Independente, 1997

[23] CONSELHO FEDERAL DE CONTABILIDADE. NBC P 3 - Normas Profissionais do Auditor Interno, 1995.

[24] CONSELHO FEDERAL DE CONTABILIDADE. NBC T 11 - Normas de Auditoria Independente das Demonstrações Contábeis, 1997.

[25] COSO BOARD, ADVISORY COUNCIL, AND PRICEWATERHOUSECOOPERS LLP, Enterprise Risk Management – Integrated Framework, 2004

[26] DIAS, C. Segurança e auditoria da tecnologia da informação. Rio de Janeiro, Axcel Books, 2000.

[27] ELIESON, B.D. Construction of an IT Risk Framework, Zions Bancorporation, Washington, 2006.

[28] ELIESON, B.D., Construction of an IT Risk Framework, Washington, Abril de 2006.

[29] FERNANDES, A.A.; ABREU, V.F. Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços, Rio de Janeiro, Brasport, 2006.

[30] Generally Accepted Government Auditing Standards (GAGAS/Yellow Book) – US version only

[31] GRIFFITHS, D. Risk based internal auditing – An Introduction, Arquivo digital, 2006.

[32] IBRACON – Instituto Brasileiro de Contadores. Normas Internacionais de Auditoria. São Paulo, 1997.

[33] IMONIANA, J.O. Auditoria de Sistemas de Informação, São Paulo, Editora Atlas, 2005.

[34] INSTITUTE OF INTERNAL AUDITORS (IIA) Professional Practices Framework (Includes the Code of Ethics, International Standards for the Professional Practice of Internal Auditing, Practice Advisories, and Development and Practice Aids)

[35] International Auditing Practice Statement 1009 - Computer-Assisted Audit Techniques

[36] INTERNATIONAL AUDITING PRACTICE STATEMENT, IAPS 1009 - Computer-Assisted Audit Techniques.

[37] INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI) Code of Ethics and Auditing Standards.

[38] ISO/IEC 15408-1:2005: Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. International Organisation for Standardisation.

[39] ISO/IEC 15408-2:2005: Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. International Organisation for Standardisation.

[40] ISO/IEC 15408-3:2005: Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requiremetns. International Organisation for Standardisation.

[41] IT GOVERNANCE INSTITUTE, Aligning COBIT, ITIL and ISO 17799 for Business Benefit, 2005.

[42] IT GOVERNANCE INSTITUTE, Board Briefing on IT Governance 2nd Edition, Rolling Meadows

[43] IT GOVERNANCE INSTITUTE, COBIT 3rd Edition Audit Guidelines, 2000.

[44] IT GOVERNANCE INSTITUTE, COBIT 4.0, Rolling Meadows, 2005.

[45] IT GOVERNANCE INSTITUTE, COBIT 4.1, Rolling Meadows, 2007.

[46] IT GOVERNANCE INSTITUTE, COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition, 2007.

[47] IT GOVERNANCE INSTITUTE, COBIT Mapping Overview of International IT Guidance 2nd Edition, 2006.

[48] IT GOVERNANCE INSTITUTE, COBIT Mapping to ISO/IEC 17799 :2000 With COBIT, 2nd Edition, 2006.

[49] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping of CMMI for Development V1.2 With COBIT 4.0, 2007.

[50] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0, 2006.

[51] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping of ITIL With COBIT 4.0, 2007.

[52] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0, 2007.

[53] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping of TOGAF 8.1 With COBIT 4.0, 2007

[54] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping PMBOK to COBIT 4.0, 2006.

[55] IT GOVERNANCE INSTITUTE, COBIT Mapping: Mapping SEI's CMM for Software to COBIT 4.0, 2006.

[56] IT GOVERNANCE INSTITUTE, COBIT Quickstart, 2nd Edition, 2007.

[57] IT GOVERNANCE INSTITUTE, COBIT Security Baseline, 2nd Edition, 2007.

[58] IT GOVERNANCE INSTITUTE, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006.

[59] IT GOVERNANCE INSTITUTE, IT Assurance Framework (ITAF), Draft, 2007.

[60] IT GOVERNANCE INSTITUTE, IT Assurance Guide using COBIT, Rolling Meadows, 2007.

[61] IT GOVERNANCE INSTITUTE, IT Control Objectives do Sarbanes-Oxley, Rolling Meadows, 2004.

[62] IT GOVERNANCE INSTITUTE, IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition , 2007.

[63] LIMA, L.H., Controle Externo, Rio de Janeiro, Editora Campus, 2007.

[64] MORAES, J.C.F. Análise da eficácia da disseminação de conhecimentos sobre controles internos após sua implementação no Banco do Brasil. Florianópolis, 2003.

[65] Normas Internacionais para o exercício da Auditoria Interna, The Institute of Internal Auditors, dezembro de 2003, USA.

[66] OCG, Introduction to PRINCE2, Office of Government Commerce, 2006.

[67] OGC. ITIL Application Management book – Versão 1.0 (2002).

[68] OGC. ITIL Managing IT Services – Security Management, 2005.

[69] OGC. ITIL Service Delivery book – Versão 2.0 (2003).

[70] OGC. ITIL Service Support book – Versão 2.1 (2000).

[71] OGC. Managing successful projects with PRINCE2. London, The Stationary Office, 2005.

[72] OGC. Security Management. London, TSO, 2005

[73] Página de fontes sobre a metodologia Seis Sigma (http://www.isixsigma.com)

[74] Página de lançamento da versão 3 do ITIL (http://www.itilv3launch.com/br/). Acessado em 20.07.2007.

[75] Página de padrões e normas da ISACA (http://www.isaca.org/standards)

[76] Página do American Institute of Certified Public Accountants (AICP) (http://www.aicpa.org/)

[77] Página do Auditing Practices Board (http://www.frc.org.uk/apb/).

[78] Página do Banco do Brasil (http://www.bb.com.br). Acessado em 03.08.2007.

[79] Página do Canadian Institute of Chargered Accountants (CICA) (http://www.cica.ca).

[80] Página do COSO (http://www.coso.org/).

[81] Página do Portal da Transparência (http://www.portaltransparencia.gov.br/). Acessado em 15.07.2007.

[82] Página do software ACL [http://www.acl.com].

[83] Página do software Galileo [http://www.galileoontheweb.com].

[84] Página do software IDEA [http://www.audimation.com].

[85] Página do software Pentana [http://www.pentana.com].

[86] Página do software SAS [http://www.sas.com].

[87] Página oficial do Balanced Scorecard (http://www.balancedscorecard.org/).

[88] Página Oficial do CMMI no sítio do Software Engineering Institute/Carnegie Mellon University (http://www.sei.cmu.edu/cmmi).

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

[90] Página oficial do SOX (http://www.sarbanes-oxley.com/).

[91] Página sobre Auditoria Governamental (http://www.governmentauditors.org).

[92] Página sobre eSCM (http://itsqc.cs.cmu.edu)

[93] Página sobre fórum do SOX (http://www.sarbanes-oxley-forum.com/).

[94] PINHEIRO, P.P. Direito Digital, Editora Saraiva, São Paulo, 2ª Edição, 2007.

[95] PMI. A guide to the Project Management Body of Knowledge, Newton Square, third edition, 2004.

[96] Portal de Auditoria (http://www.auditnet.org/).

[97] Portal do Institute of Internal Auditors (IIA) (http://www.theiia.org/)

[98] REMYRECH,R. Controle interno na administração pública, 2005

[99] SAISSE, N.C.; JÚLIO L.N.C. Auditabilidade Plena como Fator de Segurança de TI.

[100] SIGA Brasil. Acessado em: http://www.senado.gov.br/sf/orcamento/siga/siga.asp, em 18.04.2007.

[101] SOFTEX. MPS.BR – Melhoria de Processo do Software Brasileiro – Guia Geral, Versão 1.2, 2007.

[102] STONEBUMER, G.; GOGUEN, A.; FERINGA, A., Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, July 2002.

[103] SWANSON, MARIANNE, Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26, November 2001.

[104] THE AUDITING PRACTICES BOARD, ISA 315 - Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement

[105] The Orange Book - Management of Risk - Principles and Concepts, HM Treasury contacts, October 2004.

[106] TRIBUNAL DE CONTAS DA UNIÃO, Manual de Auditoria de Sistemas, 1998.

[107] TRIBUNAL DE CONTAS DA UNIÃO, Técnicas de Auditoria - Análise RECI, 2001.

ANEXO I: LEGISLAÇÃO DE CONTROLE

A tabela abaixo se refere à legislação ligada a Controle dentro do Brasil:

Legislação	Conteúdo
Constituição Federal de 1988	A Seção IX trata da Fiscalização Contábil, Financeira e Orçamentária
Decreto n.º 3.591 6 de setembro de 2000	Dispõe sobre o Sistema de Controle Interno do Poder Executivo Federal e dá outras providências.
Lei n.º 10.180 6 de fevereiro de 2001	Organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, e dá outras providências.
Decreto n.º 5.683 24 de janeiro de 2006	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas da Controladoria-Geral da União, e dá outras providências.
Lei n.º 8.443 16 de julho de 1992	Dispõe sobre a Lei Orgânica do Tribunal de Contas da União e dá outras providências.

ANEXO II: LEGISLAÇÃO APLICÁVEL À TI

A tabela abaixo possui a legislação brasileira aplicável à área de Tecnologia da Informação:

Legislação	Conteúdo
Lei 7.232 29 de outubro de 1984	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
Lei n.º 8.159 8 de janeiro de 1991	Dispõe sobre a política nacional de arquivos públicos e privados.
Lei 8.248 23 de outubro de 1991	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
Lei n.º 8.666 21 de junho de 1993	Institui normas para licitações e contratos da Administração Pública.
Decreto nº 1.048 de 21 de janeiro de 1994	Dispõe sobre o Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências.
Decreto n.º 1.070 2 de março de 1994	Dispõe sobre contratações de bens e serviços de informática e automação pela Administração Federal.
Decreto n.º 2.271 7 de julho de 1997	Dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.
Lei n.º 9.609 19 de fevereiro de 1998	Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
Lei n.º 9.610 19 de fevereiro de 1998	Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.
Decreto n.º 3.505 13 de junho de 2000	Estabelece diretrizes gerais para definição da Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, bem como institui o Comitê Gestor de Segurança da Informação – CGSI.
Lei n.º 9.983 14 de julho de 2000	Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal. Prevê penas específicas para crimes de inserção, alteração, exclusão e divulgação indevidas de dados nos sistemas informatizados ou bancos de dados da Administração Pública.
Medida Provisória n.º 2.200-2 24 de agosto de 2001	Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil e transforma o Instituto Nacional de Tecnologia da Informação em autarquia.
Decreto nº 3.555 8 de agosto de 2000	Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.
Decreto n.º 3.587 5 de setembro de 2000	Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov.
Decreto nº 3.697 21 de dezembro de 2000	Regulamenta o parágrafo único do art. 2º da Medida Provisória nº 2.026-7, de 23 de novembro de 2000, que trata do pregão por meio da utilização de recursos de tecnologia da informação.
Decreto n.º 3.872 18 de julho de 2001	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva.

Decreto nº 3.931 19 de setembro de 2001	Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e dá outras providências.
Decreto n.º 3.996 31 de outubro de 2001 Alterado pelo Decreto n.º 4.414 7 de outubro de 2002	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Lei no 10.520 17 de julho de 2002	Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto n.º 4.553 27 de dezembro de 2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.
Decreto n.º 5.408 1º de abril de 2005	Acrescenta às atribuições da Subchefia Executiva do Gabinete de Segurança Institucional - GSI da Presidência da República as tarefas de planejar e coordenar, em articulação com os órgãos e entidades da Administração Pública Federal direta e indireta, a execução das atividades de segurança e informação, bem como implementar, com a assessoria do CGSI e em articulação com os demais órgãos e entidades, a Política de Segurança da Informação da Administração Pública Federal.

ANEXO III: ACÓRDÃOS DO TCU

A tabela abaixo apresenta os principais acórdãos do TCU envolvendo Tecnologia da Informação.

Número Acórdão	Colegiado	Assunto
393/1994	P	Divisão do Objeto- Adjudicação por itens
819/2000	P	Contratação de serviços de TI - M. Justiça
1521/2003	P	Microsoft – Contrato *Select* - inadequação. Exigência de licitação
461/2004	P	Avaliação da confiabilidade e segurança dos sistemas de processamento de dados do Datasus.
782/2004	PC	Verificação da consistência, confiabilidade, segurança e regularidade do sistema automático de pagamento de pessoal do Exército.
1094/2004	P	Irregularidade licitação MDIC/Anulação de concorrência 01/2004
2094/2004	P	Bens e serviços TI – Consolidação de FOC, entendimentos.
1558/2004	P	Bens e serviços
2561/2004	SC	Bens TI – ISO 9001, Divisão Objeto
667/2005	P	Bens TI/MDIC Monitoramento Acórdão 1094/2004
140/2005	P	Mão-de-obra em TI
449/2005	P	Cautelar suspendendo licitação 01/2005 MDIC
2023/2005	P	Auditoria de Gestão de TI no MTE
2103/2005	P	Licitação para contratar a prestação de serviços de organização e métodos e de tratamento de documentação e informação para o MDIC.
2171/2005	P	Licitação para cotratação de prestação de serviço de operação, suporte e manutenção de BD para MDIC.
2172/2005	P	Monitoramento de licitação promovida com o objetivo de contratar a prestação de serviços de operação, suporte e manutenção de rede corporativa de computadores para o MDIC.
2095/2005	P	Contratação de serviços técnicos especializados em TI.
786/2006	P	Licitação para contratação de serviços de informática nas áreas de desenvolvimento de sistemas e acompanhamento de projetos. Traçar linhas gerais de um novo modelo de licitação e contratação de serviços de informática.
914/2006	P	Contratação de Serviços de TI.
71/2007	P	Avaliação da Segurança e Consistência das Informações do Infoseg.
362/2007	P	Contratação de Serviços de TI.
1480/2007	P	Recomendação para elaboração de modelo de licitação e contratação de serviços de TI para a APF.

ANEXO IV: NORMAS, DIRETRIZES E PROCEDIMENTOS DA ISACA

No sítio da ISACA [www.isaca.org/standards], são encontradas as publicações de padrões, diretrizes e procedimentos de Auditoria de Sistemas da Informação emitidos pelo Comitê de Padrões da Associação de Controle e Auditoria de Sistemas de Informação. Tradução livre.

Padrões para Auditoria de Sistemas de Informação (SI)	
S1	Código Carta
S2	Independência
S3	Ética e Padrões Profissionais
S4	Competência Profissional
S5	Planejamento
S6	Desempenho do Trabalho de Auditoria
S7	Relatórios
S8	Atividades de Acompanhamento
S9	Irregularidades e actos ilegais
S10	Governança de TI
S11	Uso da avaliação de riscos no planeamento de auditoria
S12	Materialidade da Auditoria
S13	Uso do Trabalho de Outros Especialistas
S14	Evidência de Auditoria

Diretrizes de Auditoria de Sistemas de Informação		Data
G1	Usando o trabalho de outros auditores e especialistas	1-jun-98
G2	Requisitos de evidências de auditoria	1-dez-98
G3	Uso de Técnicas de Auditoria Assistidas por Computados (TAACs)	1-dez-98
G4	Terceirização de Atividades de SI para outras organizações	1-set-99
G5	Filial de Auditoria	1-set-99
G6	Conceitos de Materialidade para Sistemas de Informação de Auditoria	1-set-99
G7	Devidos cuidados profissionais	1-set-99
G8	Documentação de Auditoria	1-set-99
G9	Considerações de auditoria para irregularidades	1-mar-00

G10	Amostra de Auditoria	1-mar-00
G11	Efeitos de controles de SI genéricos	1-mar-00
G12	Relacionamento organizacional e independência	1-set-00
G13	Uso da análise de risco no planejamento da auditoria	1-set-00
G14	Exame de sistemas de aplicação	1-nov-01
G15	Planejamento	1-mar-02
G16	Efeito de terceiros no controle de uma organização de TI	1-mar-02
G17	Efeitos de papéis alheios à auditoria sobre o auditor independente de SI	1-jul-02
G18	Governança de TI	1-jul-02
G19	Irregularidades e atos ilegais	1-jul-02
G20	Relato	1-jan-03
G21	Exame de sistemas de *Enterprise Resource Planning* (ERP)	1-ago-03
G22	Exame de comércio eletrônico *business-to-consumer* (B2C)	1-ago-03
G23	Exames de revisão de ciclo de vida de desenvolvimento de software	1-ago-03
G24	*Internet Banking*	1-ago-03
G25	Exame de Redes Virtuais Privadas	1-jul-04
G26	Exame de projeto de reengenharia de processo de negócio	1-jul-04
G27	Computação móvel	1-set-04
G28	Computação forense	1-set-04
G29	Exame pós-implementação	1-jan-05
G30	Competências	1-jun-05
G31	Privacidade	1-jun-05
G32	Exame do Plano de Continuidade de Negócio de uma perspectiva de TI	1-set-05
G33	Considerações Gerais sobre o uso da *Internet*	1-mar-06
G34	Responsabilidade, autoridade e *accountability*	1-mar-06
G35	Atividades de *follow-up*	1-mar-06
G36	Controles biométricos	1-fev-07

Procedimento para Auditoria de Sistemas de Informação		Data
P1	Medidas de avaliação de risco de SI	1-jul-02
P2	Assinaturas digitais	1-jul-02
P3	Detecção de intrusão	1-ago-03
P4	Vírus e outros códigos maliciosos	1-ago-03
P5	Auto-avaliação de risco de controle	1-ago-03
P6	*Firewalls*	1-ago-03
P7	Irregularidades e atos ilegais	1-nov-03
P8	Avaliação de Segurança - Teste de penetração e análise de vulnerabilidade	1-set-04
P9	Avaliação de gerenciamento de controles sobre tecnologias de criptografia	1-jan-05
P10	Controle de mudança de aplicação de negócio	1-out-06
P11	Transferência eletrônica de fundos	1-mai-07

ANEXO V: TABELA COBIT

A tabela abaixo possui todos os 34 Processos do COBIT divididos em seus 4 Domínios com o mapeamentos dos Critérios da Informação e Recursos de TI relevantes em cada processo. Tradução livre.

Legenda:
Critério da Informação
Em branco = Sem impacto
P = Impacto primário
S = Impacto Secundário
Recursos de TI
Em branco = Não usado
x = Usado

Processos		Critérios da Informação							Recursos de TI			
		Eficácia	Eficiência	Confidencialidade	Integridade	Disponibilidade	Conformidade	Confiabilidade	Aplicações	Informação	Infra-estrutura	Pessoas
Planejamento e Organização - PO												
PO1	Definir um plano estratégico para TI.	P	S						x	x	x	x
PO2	Definir a arquitetura da informação.	S	P	S	P				x	x		
PO3	Determinar a direção tecnológica.	P	P						x		x	
PO4	Definir a organização de TI, os seus processos e relacionamentos.	P	P									x
PO5	Gerenciar o investimento em TI.	P	P					S	x		x	x
PO6	Comunicar objetivos e direcionamentos gerenciais.	P					S			x		x
PO7	Gerenciar os recursos humanos.	P	P									x
PO8	Gerenciar a qualidade.	P	P		S			S	x	x	x	x
PO9	Avaliar e gerenciar riscos de TI.	S	S	P	P	P	S	S	x	x	x	x
PO10	Gerenciar projetos.	P	P						x		x	x
Aquisição e Implementação - AI												
AI1	Identificar soluções automatizadas.	P	S						x		x	
AI2	Adquirir e manter software aplicativo.	P	P		S			S	x			
AI3	Adquirir e manter infra-estrutura tecnológica.	S	P		S	S					x	
AI4	Viabilizar operação e utilização.	P	P		S	S	S	S	x		x	x
AI5	Adquirir recursos de TI.	S	P				S		x	x	x	x
AI6	Gerenciar mudanças.	P	P		P	P		S	x	x	x	x
AI7	Instalar e aprovar soluções e mudanças.	P	S		S	S			x	x	x	x
Entrega e Suporte - DS												
DS1	Definir e gerenciar níveis de serviço.	P	P	S	S	S	S	S	x	x	x	x
DS2	Gerenciar serviços terceirizados.	P	P	S	S	S	S	S	x	x	x	x
DS3	Gerenciar desempenho e capacidade.	P	P			S			x		x	
DS4	Garantir a continuidade dos serviços.	P	S			P			x	x	x	x
DS5	Garantir a segurança dos sistemas.			P	P	S	S	S	x	x	x	x
DS6	Identificar e alocar custos.		P					P	x	x	x	x
DS7	Educar e treinar usuários.	P	S									x
DS8	Gerenciar central de serviços e incidentes.	P	P						x			x
DS9	Gerenciar a configuração.	P	S			S		S	x	x	x	
DS10	Gerenciar problemas.	P	P			S			x	x	x	x
DS11	Gerenciar dados.				P			P		x		
DS12	Gerenciar o ambiente físico.				P	P					x	
DS13	Gerenciar operações.	P	P		S	S			x	x	x	x
Monitoramento e Avaliação - ME												
ME1	Monitorar e avaliar o desempenho da TI.	P	P	S	S	S	S	S	x	x	x	x
ME2	Monitorar e avaliar os controles internos.	P	P	S	S	S	S	S	x	x	x	x
ME3	Assegurar conformidade com requisitos externos.						P	S	x	x	x	x
ME4	Prover governança de TI.	P	P	S	S	S	S	S	x	x	x	x

ANEXO VI: RELAÇÃO ENTRE OBJETIVOS DE NEGÓCIO E DE TI

A tabela abaixo faz parte do Anexo I do COBIT 4.1 e demonstra a relação entre objetivos de negócio e objetivos de TI.

LINKING BUSINESS GOALS TO IT GOALS

		Business Goals	IT Goals								CobiT Information Criteria						
											Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24														
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22							
	3	Improve corporate governance and transparency.	2	18													
Customer Perspective	4	Improve customer orientation and service.	3	23													
	5	Offer competitive products and services.	5	24													
	6	Establish service continuity and availability.	10	16	22	23											
	7	Create agility in responding to changing business requirements.	1	5	25												
	8	Achieve cost optimisation of service delivery.	7	8	10	24											
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26										
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11												
	11	Lower process costs.	7	8	13	15	24										
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27								
	13	Provide compliance with internal policies.	2	13													
	14	Manage business change.	1	5	6	11	28										
	15	Improve and maintain operational and staff productivity.	7	8	11	13											
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28												
	17	Acquire and maintain skilled and motivated people.	9														

ANEXO VII: RELAÇÃO ENTRE OBJETIVOS DE TI E PROCESSOS

A tabela abaixo faz parte do Anexo I do COBIT 4.1 e demonstra a relação entre objetivos de TI e os 34 Processos do COBIT.

LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes											COBIT Information Criteria						
													Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4							P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Optimise the use of information.	PO2	DS11											S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3								P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6									P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5									P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5										S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5										P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2											P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7									P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8							P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9							S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9											S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5									P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12								P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13								P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6										S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10										P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5										P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4										S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4								P	P					P