ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Cel QEM RODRIGO **MARTINS** DE SOUZA

A Gestão do Gabinete de Intervenção Federal na Tecnologia da Informação e Comunicação nos Órgãos de Segurança Pública do Estado do Rio de Janeiro

Rio de Janeiro

2019

Cel QEM RODRIGO **MARTINS** DE SOUZA

A Gestão do Gabinete de Intervenção Federal na Tecnologia da Informação e Comunicação nos Órgãos de Segurança Pública do Estado do Rio de Janeiro

Trabalho de conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Administração Militar.

Orientador: Cel Com José Fernando Chagas Madeira

Rio de Janeiro
2019

S729g Souza, Rodrigo Martins de

A Gestão do Gabinete de Intervenção Federal na Tecnologia da Informação e Comunicação nos Órgãos de Segurança Pública do Estado do Rio de Janeiro. / Rodrigo Martins de Souza. —2019.
100 f. : il. ; 30 cm.

Orientação: José Fernando Chagas Madeira.
Trabalho de Conclusão de Curso (Especialização em Curso de Política, Estratégia e Alta Administração do Exército)—Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019.
Bibliografia: f. 62-64.

1. INTERVENÇÃO FEDERAL. 2. BOAS PRÁTICAS. 3. GESTÃO. 4. GOVERNANÇA. 5. TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO. I. Título.

CDD 341.5

Cel QEM RODRIGO **MARTINS** DE SOUZA

A Gestão do Gabinete de Intervenção Federal na Tecnologia da Informação e Comunicação nos Órgãos de Segurança Pública do Estado do Rio de Janeiro

Trabalho de conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Administração Militar.

Aprovado em 03 de outubro de 2019.

COMISSÃO AVALIADORA

JOSÉ **FERNANDO** CHAGAS MADEIRA – Cel Com - Presidente
Escola de Comando e Estado-Maior do Exército

JOSÉ **RAMALHO** VAZ DE BRITTO NETO – Cel Eng - Membro
Escola de Comando e Estado-Maior do Exército

JOSÉ HELENO **ZANGALI** VARGAS – Cel Com R1 - Membro
Escola de Comando e Estado-Maior do Exército

A Deus Todo Poderoso, à minha querida esposa, filhos e neto, fontes de inspiração e encorajamento, e em memória de meus pais.

AGRADECIMENTOS

À Deus, pelo dom da vida, felicidade, tranquilidade e saúde.

À minha família, em especial minha esposa, Marcia, pelo apoio, incentivo, carinho e compreensão em todos os momentos, sendo fundamentais no sucesso da conclusão deste trabalho.

Aos meus pais, pela minha educação e formação, que me, ilustram a importância da dedicação, do trabalho árduo e da disciplina, como fontes prementes do sucesso pessoal.

Ao Exército Brasileiro, pela oportunidade em realizar um trabalho monográfico, de modo a ampliar o conhecimento profissional.

Ao meu orientador, não apenas pela orientação, como também pelo incentivo e confiança demonstrados em várias oportunidades.

A todos os amigos e familiares, em especial aos colegas do curso do CPEAEx, que de uma forma ou de outra me estimularam ou me ajudaram.

Aos meus amigos do Sistema de Telemática do Exército, em particular, aos 2º Centro de Telemática de Área, Capitão Marcelo e Subtenente Douglas, pela amizade e revisão ortográfica do trabalho.

Por mais brilhante que a estratégia seja, você deve sempre olhar para os resultados.

Winston Churchill, Ex-Primeiro Ministro do Reino Unido

RESUMO

As sociedades modernas tornaram-se dependentes da tecnologia, voltados para o domínio informacional em constantes mudanças, situações complexas e rápidas. Fatos que não se sabe serem verdadeiros, ou não, proliferam em mídias sociais. Cada vez mais, equipamentos conectados por Inteligência Artificial (IA) e Internet das Coisas (IoT), tornam o indivíduo um forte elo dos sistemas vulneráveis onde imperam bandidos, denominados de *hackers* do mal, e crimes virtuais. Para combater estes cenários, as Secretarias de Segurança Pública (SSP) precisam automatizar, informatizar, conectar e, principalmente, centralizar suas ações, só para mitigar as vulnerabilidades e em especial, para integrar o processo de tomada de decisões de Comando e Controle Conjunto dos órgãos de Segurança, com base em informações situacionais oriundas dos diversos sistemas de informação computacional dos órgãos constituintes.

Com o sucateamento das estruturas governamentais do Estado do Rio de Janeiro e a necessidade de uma Intervenção Federal nos Órgãos de Segurança Pública, no ano de 2018, uma das vertentes fundamentas de atuação, que permeia todas as demais áreas, foi a da Tecnologia da Informação e Comunicação (TIC). O Gabinete de Intervenção Federal (GIFRJ) valeu-se da expertise e da governança do Exército Brasileiro, na área de TIC, para induzir e implementar o apoio às ações e operações em todos os níveis: tático, operacional e estratégico. Nos níveis tático e operacional buscou-se a integração de todas as redes e sistemas, de cada um dos órgãos, para permitir, principalmente, o monitoramento, a vigilância e a comunicação das áreas de interesse, com base na integração dos mais diversos sistemas de conhecimentos situacionais. Foram utilizados sistemas de imagens remotas aéreas, produzidas por aeronaves tripuladas, ou não; e terrestres provenientes de sistemas de imagens, circuitos de TV públicos ou privados, que permitiram celeridade, presteza e confiabilidade na atuação dos agentes decisores. Na área estratégica, buscou-se implementar e orientar os órgãos da SSP em como alinhar o planejamento estratégico com um eficiente plano de Tecnologia da Informação e Comunicação, culminando com o emprego em ações de inteligência para prevenir e permitir uma maior governança. Em síntese, esse trabalho apresenta o processo de boas práticas de governança de TIC, implementado pelo GIFRJ, bem como seus impactos, ações e legados.

Palavras-chave: Intervenção Federal; Boas práticas; Gestão; Governança; Tecnologia da Informação e Comunicação.

ABSTRACT

Modern societies have become dependent on technology, focused on the ever-changing informational domain, complex and rapid situations. Facts that we don't known if they are true or not, proliferate on social media. Increasingly, equipment connected by Artificial Intelligence (AI) and the Internet of Things (IoT), make the individual a strong link of vulnerable systems where bad guys, called evil hackers, and cybercrimes reign. To counter these scenarios, the Public Security Agencies (PSA) need to automate, computerize, connect and, most importantly, centralize their actions, just to mitigate vulnerabilities and in particular to integrate the Command and Control Centers of the Public Security Agencies decision process based on the situational information originated from the various systems of the constituent agencies.

With the scrapping of the governmental structures of the State of Rio de Janeiro and the need for a Federal Intervention in the Public Security Agencies, in 2018, one of the fundamental areas of action, which permeates all other areas, was Information Technology. and Communication (ICT). The Federal Intervention Agency (GIFRJ) drew on the Brazilian Army's expertise and governance in the area of ICT to induce and implement support for actions and operations at all levels: tactical, operational and strategic. At the tactical and operational levels, the integration of all networks and systems of each of the agencies was sought to allow, mainly, the monitoring, surveillance and communication of the areas of interest, based on the integration of the most diverse systems of situational knowledge. Remote aerial imaging systems, produced by manned aircraft or not; and terrestrial from image systems, public or private TV circuits, which allowed for speed, readiness and reliability in the performance of decision makers. In the strategic area, the aim was to implement and guide the PSA's on how to align strategic planning with an efficient Information and Communication Technology plan, culminating in the use of intelligence actions to prevent and enable greater governance. In summary, this paper presents the process of good ICT governance practices implemented by the GIFRJ, as well as its impacts, actions and legacies.

Keywords: Federal Intervention; Good habits; Management; Governance; Information and Communication Technology.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CBERJ	Corpo de Bombeiros do Estado do Rio de Janeiro
CCTI	Centro de Coordenação Tático Integrado
CETI	Concepção Estratégica de Tecnologia da Informação
CFTv	Circuito Fechado de Televisão
CICC	Centro Integrado de Comando e Controle
Cmdo	Comando
CMM	Cabability Maturity Model
CMMI	Capability Maturity Model Integration
CML	Comando Militar do Leste
COBIT	Control Objectives for Information Related Technology
CTA	Centro de Telemática de Área
DCT	Departamento de Ciência e Tecnologia
GIFRJ	Gabinete de Intervenção Federal do Rio de Janeiro
Gu	Guarnição
IN	Instrução Normativa
IRP	Intenção de Registro de Preços
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Tecnology Infrastructure Library
MPOG	Ministério do Planejamento, Orçamento e Gestão
OD	Ordenador de Despesas
ODS	Órgão de Direção Setorial
OE	Objetivos Estratégicos
OEE	Objetivos Estratégicos do Exército
OM	Organização Militar
PCERJ	Polícia Civil do Estado do Rio de Janeiro
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PE	Pregão Eletrônico

PETI	Planejamento Estratégico de Tecnologia da Informação
PMBoK	Project Management Body of Knowledge
PMERJ	Polícia Militar do Estado do Rio de Janeiro
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
SEAP	Secretaria de Estado de Administração Penitenciária
SEDEC	Secretaria de Estado de Defesa Civil
SESEG	Secretaria de Estado de Segurança Pública
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SLTI	Secretaria de Logística e Tecnologia da Informação
SSP	Secretaria de Segurança Pública

SUMÁRIO

1 INTRODUÇÃO

Com o advento da era do conhecimento, cada vez mais, torna-se importante o envolvimento com a ciência e tecnologia, principalmente com os temas relacionados à área de tecnologia da informação. Essa necessidade é vital para o desenrolar das ações de globalização da informação e uso eficiente do conhecimento. Não basta apenas deter o conhecimento, é preciso ter capacidade de utilizá-lo de forma precisa e ágil. Para concretizar essas ações, ferramentas de gestão são cruciais. Daí decorre o ramo da Tecnologia da Informação e Comunicação (TIC).

Na Constituição Federal de 1988 já era contemplada uma reforma administrativa pública que impunha a mudança para um modelo moderno de gestão, agilizando os serviços públicos e evitando a burocracia. Para atingir esse objetivo, modelos de gestão são primordiais, inserindo a Tecnologia da Informação (TI) para tornar mais eficaz os processos administrativos.

Em relação ao meio civil corporativo, atualmente, para otimizar os processos e reduzir os custos, as empresas que desejam competitividade utilizam meios tecnológicos e necessitam empregar boas práticas de gestão, aliados às oportunidades de melhoria, para atingir a sua estratégia de negócio.

Esse novo cenário exige que, cada vez mais, empresas e órgãos governamentais se adequem, para não ficarem fora do mercado globalizado, no caso das empresas; e para não percam poder, no caso dos órgãos governamentais.

Nesse contexto, uma boa política de TI, aliada com planejamento, plano e projetos, nesta área, que se utilizam de técnicas de gerenciamento de projetos, processos e ferramentas como padrão ou modelo de gestão de TI, não pode ser dispensada. Dentre os modelos atuais, destacam-se: o Corpo de Conhecimento de Gerenciamento de Projetos – Project Management Body of Knowledge (PMBoK); o Modelo Integrado de Maturidade de Processos – Capability Maturity Model Integration (CMMI); os Objetivos de Controle para Informação e Tecnologias Relacionadas – Control Objectives for Information Related Technology (COBIT); a Biblioteca de Infraestrutura de Tecnologia da Informação – Information Technology Infrastructure Library (ITIL), sem contar os padrões de segurança, como a Organização Internacional de Padronização – International Organization for Standardization (ISO).

Por outro lado, a Intervenção Federal na Área de Segurança Pública do Estado do Rio de Janeiro foi um marco e não há referência de modelo e/ou série histórica que pretende ser seguida como parâmetro. Neste contexto, os diagnósticos foram dimensionados de acordo com as realizações implementadas em processo contínuo. Assim, na área de TIC, uma gestão com boas práticas tornou-se imprescindível para otimizar os processos, aquisições e transparências nas ações, bem como a tomada de decisão, com o apoio de Sistemas de Comando e Controle, permitindo avaliar as decisões e o emprego da tropa. Oportuno destacar que o assessoramento em TIC utilizou, como referência, as boas práticas adotadas pelo Exército Brasileiro, como marco inicial de um modelo exitoso.

1.1 PROBLEMA DE PESQUISA

Da importância do assunto exposto anteriormente, nota-se o largo emprego de TIC em sistemas de Comando e Controle e decisão do Alto Escalão, desde equipamentos de emprego operacional, como carros de combate que transmitem em tempo real uma manobra para um sistema de Comando e Controle, até sistemas mais complexos, salvando vidas. É nesse contexto, que são necessários controles que garantam uma decisão precisa, com rapidez e segurança. Entretanto, apenas controles não são suficientes para uma boa prática de governança. Há necessidade de conscientização dos recursos humanos através de emprego de uma gestão adequada.

Sob esse prisma, o estudo em tela apresenta relevância, uma vez que o Gabinete de Intervenção Federal necessitava implantar técnicas de governança de TIC, alinhadas com as melhores práticas apresentadas no cenário internacional, em pequena escala de tempo, apresentando resultados concretos. Assim, este estudo apresenta o modelo adotado pelo Gabinete de Intervenção Federal, destacando em que medida a governança de TIC, adotada pelo GIF na Área de Segurança Pública do Estado do Rio de Janeiro, impactou no êxito da Intervenção Federal levada a efeito.

Ressalte-se que este o presente trabalho não teve a pretensão de esgotar o assunto, mas, sim, de servir de instrumento inicial para sua discussão e possível referência em atuações futuras de Intervenção Federal.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O presente trabalho teve como objetivo geral apresentar a metodologia e a relevância do emprego de governança de Tecnologia da Informação adotado, no nível estratégico, do Gabinete de Intervenção Federal.

1.2.2 Objetivos Específicos

Para alcançar o objetivo geral delineado, o estudo abordou os seguintes objetivos específicos:

- apresentar a metodologia e o impacto do emprego de governança de Tecnologia da Informação no Gabinete de Intervenção Federal na Área de Segurança Pública do Estado do Rio de Janeiro;

- analisar as principais técnicas de gestão de Tecnologia da Informação utilizadas no Governo Federal ; e

- analisar as principais técnicas de gestão de Tecnologia da Informação utilizadas no Exército Brasileiro.

1.3 HIPÓTESE

A hipótese de estudo estabelecida foi baseada na seguinte afirmativa:

- “O êxito da intervenção Federal na Área de Segurança Pública do Estado do Rio de Janeiro recebeu acentuado impacto das medidas de governança de TIC adotadas pelo GIF”.

1.4 VARIÁVEIS

Considerando o tema, o problema e a hipótese estabelecida, as circunstâncias passíveis de medição e que influenciaram o estudo foram as seguintes, segundo a relação expressa entre elas:

- **Variável dependente** – o êxito da Intervenção Federal na Área de Segurança Pública do Estado do Rio de Janeiro

- **Variável independente** – medidas de governança de Tecnologia da Informação e Comunicação adotadas

1.5 DELIMITAÇÃO DA PESQUISA

Este estudo propiciou, inicialmente, apresentar os modelos de metodologias e principais conceitos empregados em governança de TI em universo governamental, para, em seguida, abordar a inserção das boas práticas de TI adotadas pelo Gabinete de Intervenção Federal na Área de Segurança Pública do Estado do Rio de Janeiro, ao longo do ano de 2018.

1.6 CONTRIBUIÇÃO DA PESQUISA

A grande importância do presente estudo está na apresentação e na consolidação das informações de técnicas de governança de TIC, as quais permitirão otimizar processos e extrair benefícios, em prol da racionalização de recursos e tomada de decisão, em situações futuras semelhantes. O estudo se justifica, na medida em que, cada vez mais sistemas informatizados surgem e precisam ser integrados, objetivando um melhor comando e controle, exigindo um modelo robusto que permita gerenciar a infraestrutura e os serviços de TIC de vários aplicativos, além de uma plataforma independe dos protocolos que eles utilizam.

Tendo como estudo de caso o período da Intervenção Federal no Estado do Rio de Janeiro, foi observado um momento único, onde os planejamentos tiveram que ser preparados ao longo do evento, o que levou a dilemas, na área de TIC, de como executar técnicas e ferramentas para a melhor Gestão e Governança dos processos, tendo como limitador, não só já ter iniciado o período da intervenção bem como a data fixada para término daquele período. Assim, os principais desafios foram: identificar parâmetros de modelagem anteriores, compatibilizar os ambientes completamente diferente aos encontrados no âmbito da Força Terrestre, com legislações internas também distintas e total ausência de normatização e alinhamento com o planejamento estratégico do Exército Brasileiro.

Desse modo, enfatiza-se que o estudo do problema levantado trouxe significativos benefícios para o EB, uma vez que apresentou reflexões e novas ideias com vistas ao incremento de técnicas de governança de TIC, especialmente, em um contexto atual e alinhado com as diretrizes e orientações do Governo Federal em casos de Intervenção Federal.

1.7 METODOLOGIA

Segundo (ALVES-MAZZOTTI; GEWANDSZNAJDER, 2001) em sua conceituação sobre metodologia, o presente trabalho teve como base a leitura e análise de textos, ou seja, uma pesquisa bibliográfica, tendo como técnica de pesquisa a documentação indireta, pois foram empregadas técnicas diretas de entrevistas e questionário. Ao apresentar as ferramentas de controle, em alguns aspectos, foi utilizado o método de procedimento comparativo. Quanto aos objetivos, um estudo exploratório foi realizado com a finalidade de apresentar o impacto do emprego da Tecnologia da Informação no Gabinete de Intervenção Federal na Área de Segurança Pública do Estado do Rio de Janeiro no que diz respeito a Governança. Como o trabalho não mediu variáveis, o presente estudo adotou uma abordagem qualitativa. Os passos, conforme o Manual Escolar Trabalhos Acadêmicos na ECEME (BRASIL, 2004, p.23-24), foram:

- levantamento da bibliografia e de documentos pertinentes;
- seleção da bibliografia e dos documentos;
- leitura da bibliografia e dos documentos selecionados, dando ênfase aos métodos e ferramentas de controle de gestão da governança de TI;
- pesquisa de levantamento de dados por meio de documentação militar, destacando as do Departamento de Ciência e Tecnologia (DCT), e não-militar;
- montagem de arquivos: ocasião em que foram elaboradas as fichas bibliográficas de citações, resumos e análises (Op. cit., 2004, p. 24); e
- análise crítica, tabulação das informações obtidas e consolidação das questões de estudo. (Op. cit., p.24).

A coleta de material foi realizada por meio de consultas aos noticiários e artigos de jornais e revistas; manuais, política e planos do Governo Federal, do Governo Estadual e do Exército Brasileiro, e, ainda, a rede mundial de computadores.

O presente trabalho apresenta sugestões para a implantação de ferramentas de controle de governança de Tecnologia da Informação e Comunicação em cenários onde haja necessidade de Intervenção Federal em Órgãos de Segurança Pública Estaduais, destacando as técnicas dos modelos COBIT e ITIL, sendo empregadas para a melhoria da otimização de recursos de Tecnologia da Informação e Comunicação em prol dos Sistemas de Comando e Controle para apoio da decisão.

Esse trabalho não teve por objetivo abordar/desenvolver uma nova teoria, sendo classificada como uma pesquisa aplicada.

2 REFERENCIAL TEÓRICO DE GOVERNANÇA DE TIC

2.1 CONCEITOS DE GOVERNANÇA E GESTÃO

Inicialmente, para tratar e uniformizar entendimentos, é preciso definir e diferenciar TI e TIC, no contexto deste trabalho. TI são as técnicas de comando e controle da informação baseados em meios eletrônicos, ou seja, são os *hardwares* (servidores, computadores, armazenadores de banco de dados etc) ou os softwares (sistemas operacionais, programas, aplicativos, banco de dados). Com a evolução da Era do Conhecimento e Informação, foram agregadas a esse termo as Comunicações, sendo definido TIC. Esse novo termo, portanto, agregou ~~à~~ definição inicial de TI de como a informação dos processos de comando e controle seriam transmitidas. Dessa forma, para fins deste trabalho, na área de Gestão e Governança, os conceitos de TI são aplicados aos de TIC.

2.1.1 Planejamento e Alinhamento Estratégico

Para abordar o assunto governança é preciso, antes, compreender alguns conceitos. Primeiramente, a definição de planejamento estratégico, que, de uma forma simples, são ações coordenadas no contexto de um processo que tem por objetivo orientar a tomada de decisões futuras. Até o final do século XVIII, o conceito de estratégia estava diretamente ligado às questões militares e era chamado de “arte da guerra”, ou seja, estratégia era a arte de, através de um conjunto de forças coordenadas, conduzir os objetivos da nação nos diversos setores: político, econômico, social, terrestre, marítimo, aéreo, etc., para derrotar o inimigo. Modernamente, o conceito foi estendido para todos os campos da sociedade.
Portanto, uma definição clássica de planejamento estratégico pode ser compreendida como:

> O processo contínuo de tomar decisões atuais que envolvam riscos, organizar sistematicamente as atividades necessárias à execução dessas decisões e através de um feedback organizado e sistemático, medir os resultados dessas decisões em confronto com as expectativas alimentadas (DRUCKER,1997).

Assim, o planejamento estratégico permite que uma Instituição conheça melhor seus: pontos fortes e fracos, vulnerabilidades, oportunidades e ameaças. Com base nesse mapeamento, qualquer Instituição poderá elaborar um plano de trabalho que elaborará as premissas, objetivos, metas e caminhos para melhorar e usufruir os aspectos positivos e tentar eliminar, evitar ou adequar os aspectos negativos (OLIVEIRA, 2001). Neste sentido, o planejamento estratégico permite propor os objetivos e onde se deve concentrar os esforços para que a Instituição atinja o sucesso na sua área de atuação. São definidos, também, outros dois níveis de planejamento: o tático (decomposição do planejamento estratégico em setores intermediários, detalhando o planejamento estratégico identificado pelo alto escalão) e o operacional (nos níveis mais baixos da Instituição, isto é , o planejamento de como serão executadas as estratégias da Instituição com ações de curto prazo).

Para atingir os objetivos estratégicos, a Instituição precisa desenvolver capacidades as quais costumam ser dividas em áreas de negócios. As principais áreas são: capacidade de informação, processos, estrutura organizacional, pessoas e relacionamento externo. As capacidades de informação nos níveis estratégico, tático e operacional são delineadas no Planejamento Estratégico de Tecnologia da Informação (PETI), cujos processos são pautados na gestão de pessoas e na infraestrutura necessárias para a tomada de decisão. Consequentemente, o PETI deve estar alinhado e em conformidade com o Planejamento Estratégico da Instituição, não sendo uma auditoria e, sim, um apoio às decisões estratégicas adotadas no nível gerencial, bem como realimentar o processo de melhoria da estratégia de negócio da Instituição (SODRÉ; SOUZA, 2007).

As etapas do PETI, segundo BOAR (apud SODRÉ; SOUZA, 2007), são: avaliação (auditoria e inventário dos equipamentos e soluções), estratégia (identificação dos objetivos estratégicos) e execução (execução da estratégia). O PETI só é concluído após a definição das prioridades dos processos de recursos de investimento e custeio. Esta definição é concretizada no portfólio, que será o balizador para execução e as ações em TI em dado período. Cabe destacar que, o PETI é dinâmico e interativo, permitindo, então, ser atualizado a qualquer momento, desde que alinhado com os objetivos estratégicos.

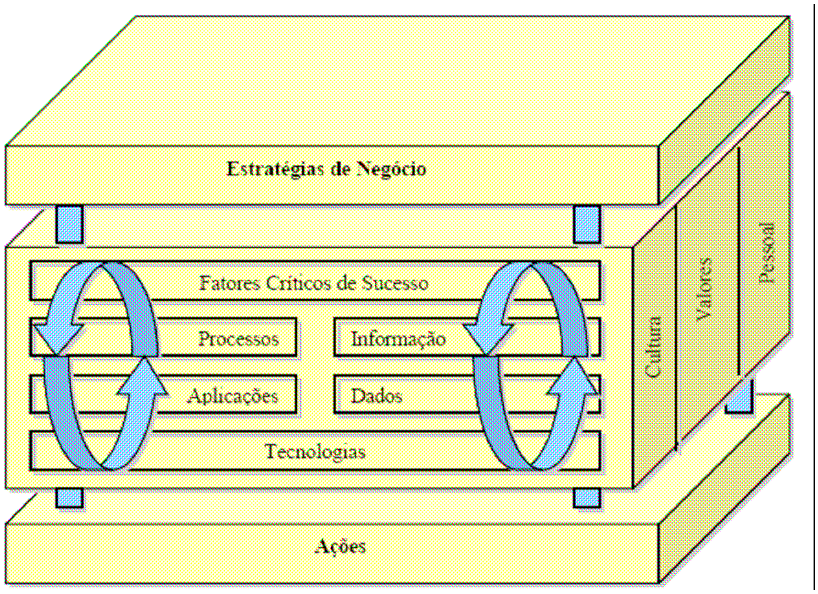

Fig 01 – Estrutura para alinhamento de estratégias, processos e TIC
(Fonte: SOPHR; SAUVÉ, 2003)

Nas ações de transformação do negócio da Instituição para atingir os objetivos delineados, o alinhamento estratégico de TI cada vez se torna mais crucial como fator crítico de sucesso. De acordo com SPOHR & SAUVÉ (2003), o alinhamento estratégico de TI permeia todas as ações nas áreas: cultural, de valores e pessoal da Instituição, apoiando os processos, aplicações, informações e dados na obtenção dos fatores críticos de sucesso para a estratégia do negócio, conforme a figura 01. A literatura especializada apresenta diversos modelos de alinhamento estratégico de TI que não serão abordados por não fazerem parte do escopo deste trabalho.

2.1.2 Governança de TIC

A governança de TIC decorre do conceito de governança coorporativa, ganhando importância após a crise financeira do início do século XXI.

> Governança corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade (Instituto Brasileiro de Governança Corporativa – IBCG).

Sendo assim, a governança de TIC é de inteira responsabilidade da alta administração, que deverá definir e incentivar o cumprimento das metas, estratégias e boas práticas para atingir os objetivos institucionais. De acordo com o IT Governance Institute (2005 apud FERNANDES, ABREU; 2006, p. 11), “a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização”.

Segundo Weill; Ross (2006) (apud SODRÉ;SOUZA,2007), Governança de TI é “a especificação de direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização de TI”.

No cenário atual, pode-se constatar um elevado aumento nos sistemas de TIC para o sucesso de uma Instituição, sem contar com a exigência, cada vez maior, dos colaboradores e clientes por celeridade nas informações. Dessa forma, ameaças de ataques cibernéticos, como hackers e vírus, e necessidades de novas tecnologias fazem com que cresça a importância na gestão de TIC, procurando reduzir custos nos processos internos e externos e alinhando aos interesses da empresa.

2.2 PRINCIPAIS FERRAMENTAS DE GESTÃO DE TIC

Neste contexto, para otimizar a gestão de governança de TI, surgiram vários modelos e técnicas para sua implantação. Dentre esses modelos pode-se destacar de acordo com Holm; Kühn; Viborg (2006, p. 1-5):

> - **ITIL** (Information Technology Infrastructure Library) - É o padrão mundial em Gerência de Serviço (Behr et al., 2004 apud Holm; Kühn; Viborg, 2006, p. 2). ITIL estabelece melhores práticas compreensivas e consistentes, baseadas na experiência coletiva de milhares de profissionais de TI. (Niessink; van Vliet, 2001 apud Holm; Kühn; Viborg, 2006, p. 2). ITIL está focado em processos críticos de negócio e disciplinas necessárias para que se tenha serviços de alta qualidade. Fora do framework ITIL, surgiu o British Standard BS15000, o primeiro padrão do mundo para gerenciamento de serviços de TI. Toda atividade é classificada em dois grupos: Gerência de Serviço e Prestação de Serviço. Isso define qualidade de TI como o nível de alinhamento entre serviços de TI e as efetivas necessidades de negócio (Niessink; van Vliet, 2000 apud Holm; Kühn; Viborg, 2006, p. 2). Como resultado, as organizações podem amadurecer suas melhores práticas sem ter que levar em consideração tecnologias específicas.
> - **COBIT** (Control Objectives for Information and Related Technology) - Foi desenvolvido como um padrão genericamente aplicável para boas práticas de segurança e controle de TI (Lainhart, 2000 apud Holm; Kühn; Viborg, 2006, p.2). As ferramentas incluem: elementos de medição de desempenho; uma lista de Fatores Críticos de Sucesso (FCS); modelos de Maturidade para auxiliar nos testes de desempenho e na tomada de decisões.
> - **ASL** (Application Services Library) - É uma coleção de melhores práticas para gerenciar o desenvolvimento e a manutenção de aplicações. É o padrão de domínio público para o

gerenciamento de aplicações, diferente do ITIL, mas ligado a ele em termos de aderência para padrões de gerenciamento de processos e provimento de um coerente, rigoroso e de domínio público conjunto de orientações. (Bastiens, 2004; van der Pols, 2004 apud Holm; Kühn; Viborg, 2006, p.3). ASL é uma parte do IT Service Management (ITSM) Library. ASL reconhece três tipos de controle: funcional, aplicação e técnico. Enquanto o ITIL é um padrão geralmente aceito para organizar o gerenciamento técnico, o ASL oferece um framework para a organização do gerenciamento de aplicação (Meijer, 2003 apud Holm;Kühn; Viborg, 2006, p. 3).

- **Seis Sigma** - Essa metodologia provê as técnicas e ferramentas para melhorar a capacidade e reduzir os defeitos em qualquer processo. Ela aperfeiçoa qualquer processo de negócio através de constante revisão (Hammer, 2002 apud Holm; Kühn; Viborg, 2006, p. 3). Para isso, a Seis Sigma usa uma metodologia conhecida por DMAIC (Definir oportunidades, Medir desempenho, Analisar oportunidades, Melhorar desempenho, Controlar desempenho) (Puzdek, 2003 apud Holm; Kühn; Viborg, 2006, p. 3). Estes são os principais elementos do Processo de Aperfeiçoamento Seis Sigma: requerimentos do consumidor, qualidade do projeto, métricas e medidas, envolvimento do empregado e aperfeiçoamento contínuo.
- **CMM/CMMI** (Capability Maturity Model/ Capability Maturity Model Integrated) - Metodologia utilizada para desenvolver e refinar um processo de desenvolvimento de software da organização. O modelo descreve um caminho evolutivo de cinco níveis de crescimento organizado e sistematicamente processos mais maduros. CMM foi desenvolvido pelo Software Engineering Institute (SEI), um centro de pesquisa e desenvolvimento patrocinado pelo U.S. Department of Defense (DoD). Os cinco níveis sugeridos pelo CMM são: o inicial, o repetitivo, o definido, o gerenciado e o otimizado (Mathieassen e Sørensen, 1996 apud Holm; Kühn; Viborg, 2006, p. 3). O CMM é baseado no modelo clássico de cascata. Já o CMMI baseia-se no desenvolvimento iterativo e é mais orientado aos resultados.
- **IT Service CMM** - É um modelo de crescimento de maturidade focado nos provedores de serviços de TI (Niessink, 2003 apud Holm; Kühn; Viborg, 2006, p. 3). É uma evolução do CMM para desenvolvimento de software e incorpora estágios de maturidade similares. Origina-se dos esforços para desenvolver um framework de aperfeiçoamento de qualidade para empresas de serviços (Niessink; van Vliet, 1998 apud Holm; Kühn; Viborg, 2006, p. 3). O modelo não mede a maturidade serviços, projetos ou unidades da orgaização individualmente. Ele mede a maturidade de toda a organização, cobrindo o processo de prestação do serviço (Niessink et al., 2005 apud Holm; Kühn; Viborg,2006, p. 3). Esse modelo é delimitado pelo cobrimento do desenvolvimento de novos serviços.
- **SAS70** (Statements on Auditing Standards, nº. 70 for Service Organizations) - É um padrão de auditoria projetado para permitir que um auditor independente avalie e opine nos controles de uma organização de serviços. Desenvolvido pelo American Institute of Certified Public Accountants (AICPA), é internacionalmente reconhecido. Uma auditoria SAS70 é altamente reconhecida, porque representa que a empresa foi exposta a uma auditoria profunda, por uma firma independente de contabilidade e auditoria, das atividades de controle, as quais geralmente incluem controles sobre TI e seus processos. As organizações devem demonstrar que possuem controles adequados quando armazenam ou processam dados dos seus consumidores. Objetivos e atividades de controle deveriam também ser organizados de maneira a permitir ao usuário auditor e à organização identificar quais controles suportam as informações dos relatórios financeiros.
- **ISO 17799** - Padrão para segurança da informação que inclui um conjunto compreensível de controles e melhores práticas. O padrão pretende servir como um ponto de referência para identificar o conjunto de controles necessários para a maioria das situações onde os sistemas de informações são usados na indústria e no comércio. A aderência ao padrão garante que a organização tem estabelecido um determinado nível de concordância para cada uma das dez categorias cobertas (Ma; Pearson, 2005 apud Holm; Kühn; Viborg, 2006, p. 3): política de segurança, organização da segurança, classificação e controle de valor, segurança de pessoal, segurança física e ambiental, gerenciamento de comunicações e operações, controle de acesso, desenvolvimento e manutenção de sistemas, gerenciamento de continuidade de negócio, e concordância (ISO 2000, BS 2002).
- **SOX** (Sarbanes-Oxley Act of 2002) - Decreto para proteger os investidores e o público em geral de erros na contabilidade e práticas fraudulentas na organização (SOX, 2002

apud Holm; Kühn; Viborg, 2006, p. 3). Essa lei não afeta só o lado financeiro da corporação, mas também o departamento de TI, cuja função é armazenar os registros eletrônicos da corporação. O SOX define que todos os registros do negócio, incluindo registros e mensagens eletrônicas, devem ser salvos por pelo menos cinco anos (Alles et al., 2004 apud Holm; Kühn; Viborg, 2006, p. 3-4). As conseqüências do não cumprimento são multas, prisão ou ambos. A concordância ao SOX traz implicações significantes para a função de TI (Moore; Swartz, 2003 apud Holm; Kühn; Viborg, 2006, p. 4). Os requerimentos do SOX estão cada vez mais integrados às iniciativas de gerenciamento de riscos (Beasley et al., 2004; Sammer, 2004 apud Holm; Kühn; Viborg, 2006, p. 4).

- **SysTrust** - Serviço de garantia desenvolvido pelo American Institute of Certified Public Accountants (AICPA) em conjunto com o Canadian Institute of Chartered Accountants (CICA). É projetado para aumentar o conforto da gerência, dos clientes e dos parceiros de negócio com sistemas que suportam um negócio ou atividade particular (Pacini et al., 2000 apud Holm; Kühn; Viborg, 2006, p. 4). Numa implantação SysTrust, o participante avalia e testa se um sistema específico é confiável quando medido sob três princípios essenciais: disponibilidade, segurança e integridade (McPhie, 2000 apud Holm; Kühn; Viborg, 2006, p. 4).
- **PRINCE2** (Projects IN Controlled Environments) - PRINCE é um método de gerenciamento de projetos que cobre a organização, o gerenciamento e o controle dos projetos. A princípio, ele foi desenvolvido como um padrão do governo britânico. Desde então, o PRINCE tem sido largamente utilizado nos setores público e privado e, agora, é um padrão de facto no Reino Unido. PRINCE foi desenvolvido inicialmente para projetos de TI, mas é usado também em muitos projetos que não são de TI. O PRINCE2, a última versão dessa metodologia, foi desenvolvido para incorporar requerimentos de usuários existentes e melhorar o método em direção a uma abordagem genérica de melhores práticas para a gerência de todos os tipos de projetos (OGC, 2005 apud Holm; Kühn; Viborg, 2006, p. 4).
- **IT Audit -** Uma revisão de TI deveria focar em três principais áreas: tecnologia, organização de TI e processos de TI (Sisco, 2002 apud Holm; Kühn; Viborg, 2006, p. 4). Como a organização tecnológica possui muitas partes funcionais, uma quantificação da estrutura organizacional de TI incluirá: infraestrutura (redes) e aplicações de negócio (pesquisa & desenvolvimento e suporte) (Sisco, 2002 apud Holm; Kühn; Viborg, 2006, p. 4).
- **IT Due Diligence - Sisco** (2002b apud Holm; Kühn; Viborg, 2006, p. 4) estabelece que o objetivo do plano de continuidade precisa estar claramente definido. Para isso, sugere que ele seja quebrado em sete partes: operação corrente de TI, planos de riscos e contingência, plano financeiro, requerimentos de investimento de capital, planos de oportunidades de inovação e recomendações, plano de transição e relatório de continuidade.
- **IT Governance Review** - Contém as seguintes atividades: mapear a governança atual das organizações com ferramentas de um Governance Design Framework (GDF) e de uma Governance Arrangements Matrix (GAM), comparar o GDF e a GAM, realizar auditoria em mecanismos de governança de TI, projetar a estrutura da futura governança de TI, transformar a versão futura do GDF e da GAM da organização, e focar em comunicar, ensinar, convencer, refinar e medir o sucesso da governança de TI (Weill; Ross, 2006).
- **IT Governance Assessment** - é um enquadramento para avaliar o desempenho da governança de TI. A performance da governança deve ser avaliada para analisar quão bem as suas estruturas encorajam comportamentos desejáveis (Weill; Ross, 2006). Por essa razão, o framework propõe que a governança de TI deve abordar cinco fatores importantes, que são: a configuração da empresa, as estruturas da governança, o desempenho da governança, e o desempenho financeiro.
- **IT Governance Checklist** - Damianides (2005 apud Holm; Kühn; Viborg, 2006, p. 4) sugere um checklist para governança de TI, contendo um conjunto de questões de diagnóstico. Para cada uma das questões existe uma extensão para: valor da prestação de TI, alinhamento estratégico de TI, gerenciamento de risco e/ou desempenho. O questionário contém três subgrupos: assuntos de TI, relação da gerência com assuntos de TI e auto-avaliação da prática de governança de TI com relação à diretoria e gerência.
- **IT Governance Assessment Process (ITGAP) Model** – Peterson (2004 apud Holm; Kühn; Viborg, 2006, p. 4-5) sugere um processo de quatro estágios para avaliar

> governança de TI. Os estágios são: descrição e avaliação dos valores impulsionadores da governança de TI, descrição e avaliação da diferenciação da autoridade de tomada de decisão de TI para o portfólio de atividades de TI, descrição e avaliação das capacidades de governança de TI e descrição e avaliação da realização de valor de TI (SODRÉ; SOUZA,2007).

Alguns modelos de outras áreas, tais como segurança da informação e gerenciamento de projetos, podem trabalhar em consonância com os modelos anteriormente abordados. Na área de segurança da informação há o British Standard 7799 (BS7799) e suas versões, o International Standard Organization / International Eletrotechnical Commission 27001 (ISO/IEC 27001) e suas versões, que estabelece normas e diretrizes para iniciar, manter, monitorar, operar e melhorar Sistemas de Gestão de Segurança da Informação (SGSI), alinhando-se às recomendações previstas pelo ITIL. Na área de gerenciamento de projetos há, como referência de modelo e reconhecimento, o Project Management Body of Knowledge (PMBOK). O Balanced Scoredcard (BSC) atua na área de gestão estratégica (SODRÉ; SOUZA,2007).

Não só por serem os modelos mais aplicados, mas, principalmente, por formarem a base dos modelos a serem adotados pelo sistema de telemática do Exército Brasileiro (EB), serão abordados com mais detalhes os modelos ITIL e COBIT. O EB, na área estratégica e de normatização de TIC adota o COBIT e, na área operacional dos sistemas e infraestrutura de TIC, o ITIL. Essas duas ferramentas serão abordadas a seguir.

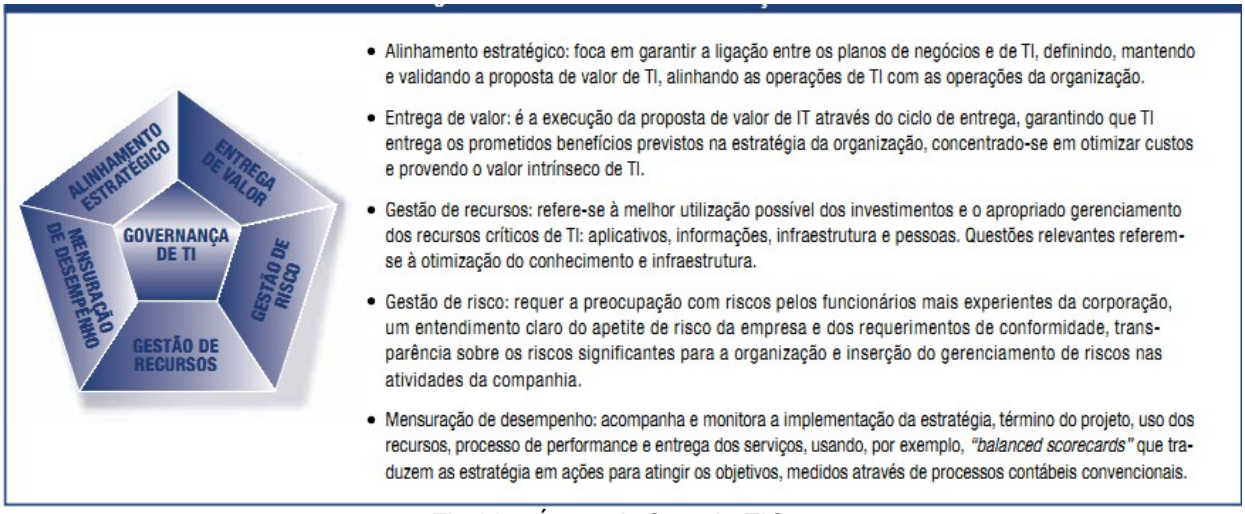

Fig 02 – Áreas de foco da TIC
(Fonte: COBIT, versão 4.1; 2007)

Conforme a figura 02, a necessidade de alinhamento com o negócio, conduz os objetivos de TIC a focarem em cinco áreas: alinhamento estratégico; entrega de valor; gestão de recursos; gestão de riscos; e mensuração de desempenho.

2.2.1 Control Objectives for Information and Related Technology (COBIT)

O COBIT foi publicado e projetado pelo Instituto de Governança de Tecnologia da Informação (ITGI – Information Technology Governance Institute), sendo um modelo, diferentemente de outros, em nível estratégico visando abranger a área financeira, principalmente para promover a ética e medidas antifraudes. Sua missão inicial foi desenvolver e elaborar um modelo de controle de objetos de TI que desse suporte ao Comitê das Organizações Patrocinadores da Comissão Treadway (COSO – Committee of Sponsoring Organisations of the Treadway Commission). O ITGI foi criado pela Associação de Auditoria e Controle de Sistemas de Informação (ISACA – Information Systems and Audit Control Association), ou seja, uma Associação que fomenta e patrocina o desenvolvimento de metodologias e certificações para o desempenho das atividades de auditoria e controle em sistemas de informação.

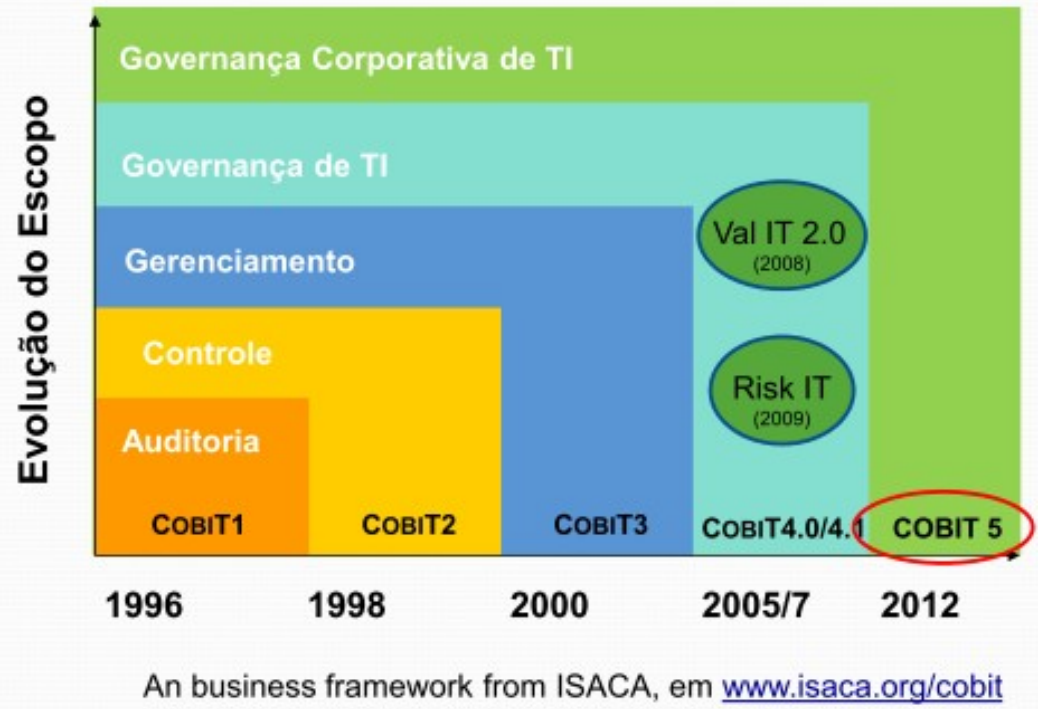

Fig 03 – Evolução do COBIT
(Fonte: ISACA)

Elaborado em sua primeira versão, em 1996, o modelo COBIT evoluiu até a quinta versão, em 2012, conforme apresentado na figura 03. Esse ano foi lançada a mais recente versão denominada de COBIT 2019, descartando as anteriores. A cada evolução do COBIT tem-se um amadurecimento dos processos e novas áreas vão sendo acrescidas. A versão 4.1 do COBIT tinha 34 (trinta e quatro) processos, enquanto na versão 5, conforme figura 04, já eram 37 (trinta e sete) processos.

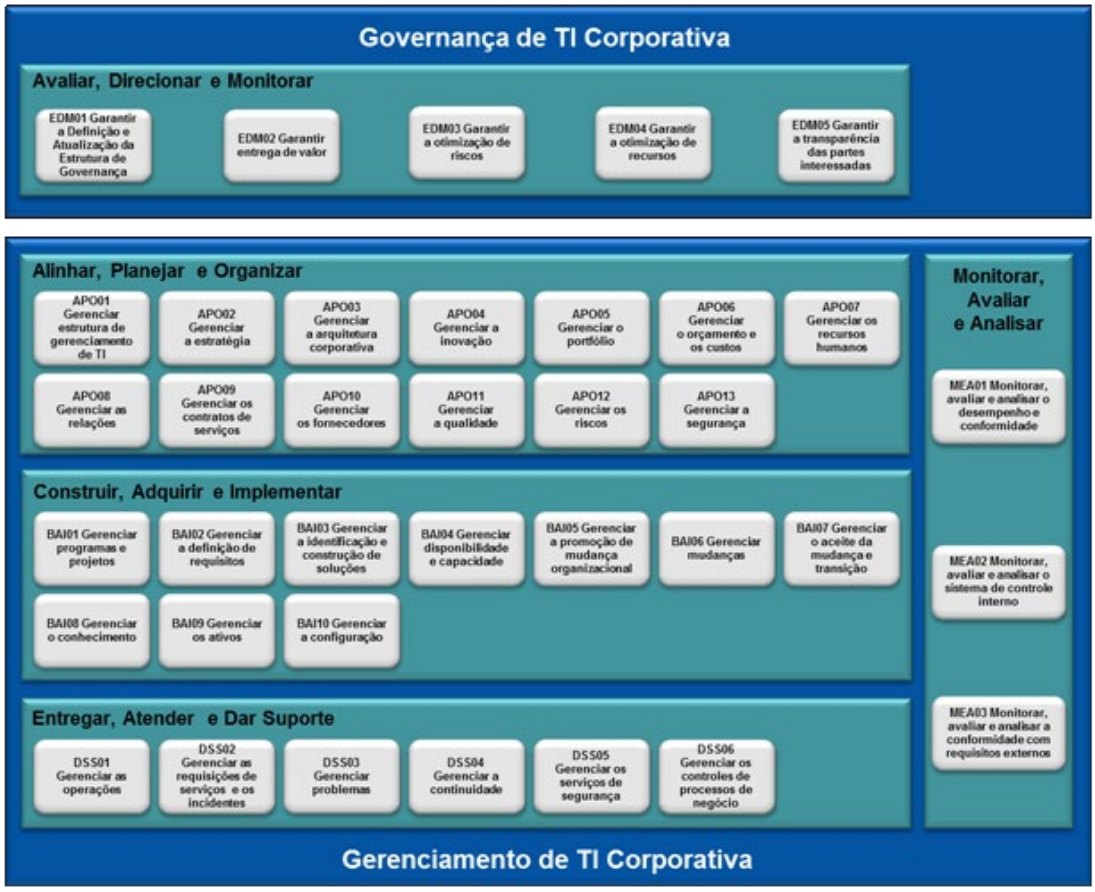

Fig 04 – Modelo COBIT 5 e os processos
(Fonte: COBIT 5; 2012)

A versão atual aumenta o número de processos para 40 (quarenta), com as seguintes modificações em relação aos processos COBIT 5, apresentados na figura 04:

- no domínio Avaliar, Direcionar e Monitorar não houve alteração;
- no domínio Alinhar, Planejar e Organizar foi inserido o processo APO14 – Dados Gerenciados;

- no domínio Construir, Adquirir e Implementar houve um desmembramento do processo BAI01 – Gerenciar Programas e Projetos em BAI01 – Gerenciar Programas e BAI11 – Gerenciar Projetos;
- no domínio Entregar, Atender e Dar Suporte não houve alteração; e
- no domínio Monitorar, Avaliar e Analisar teve o incremento de MEA04 – Avaliação com Garantia Gerenciada.

Observa-se, no COBIT 2019, um foco maior em segurança, gerenciamento de risco e governança de informação. Além disso, ocorre a interação com os usuários de forma colaborativa, através de feedback com a comunidade profissional, que pode fazer comentários, propondo melhorias, conceitos e ideias novas.

Na figura 05, nota-se que o COBIT tem como princípios a utilização de um conjunto de processos para fornecer informações organizacionais que irão aos objetivos dos negócios, tendo, como foco, a orientação por negócios não apenas para provedores de serviços e auditores, bem como gerentes, executivos de negócios. Dessa forma, provê as necessidades de investimentos, gerenciamento e controle de recursos de TIC para atender os requisitos do negócio (FAGUNDES,2012).

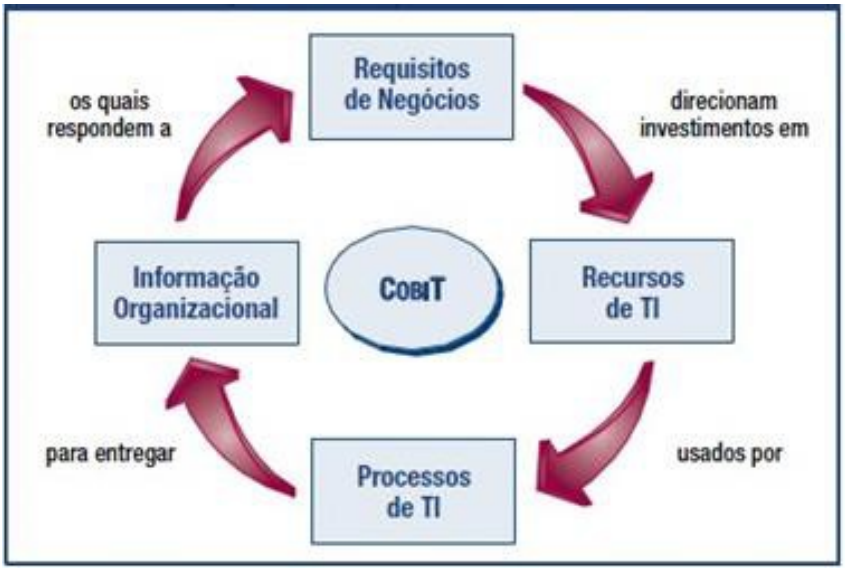

Fig 05 – Princípios básicos do COBIT
(Fonte: COBIT, versão 4.1; 2007)

E quais seriam esses requisitos ? Na uma visão integrada 3 D do modelo, denominado como cubo do COBIT, são apresentados os seguintes requisitos básicos, ilustrados na figura 06:

- ser relevante e pertinente (eficácia);

- fornecer as melhores informações possíveis utilizando-se dos recursos (eficiência);
- ter níveis de confidencialidade, evitando que pessoas não autorizadas acessem informações (confidencialidade);
- garantir que o dado não seja manipulado indevidamente (integridade);
- estar disponível dentro da perspectiva de negócio (disponibilidade);
- estar em conformidade com os padrões da empresa, órgãos reguladores (conformidade); e
- ter a certeza que a informação é correta quando for acessada (confiabilidade).

Do ponto de vista de recursos de TI, os sistemas de aplicação devem atender aos requisitos mínimos do negócio, ter uma informação com qualidade, infraestrutura compatível com o negócio e pessoas qualificadas.

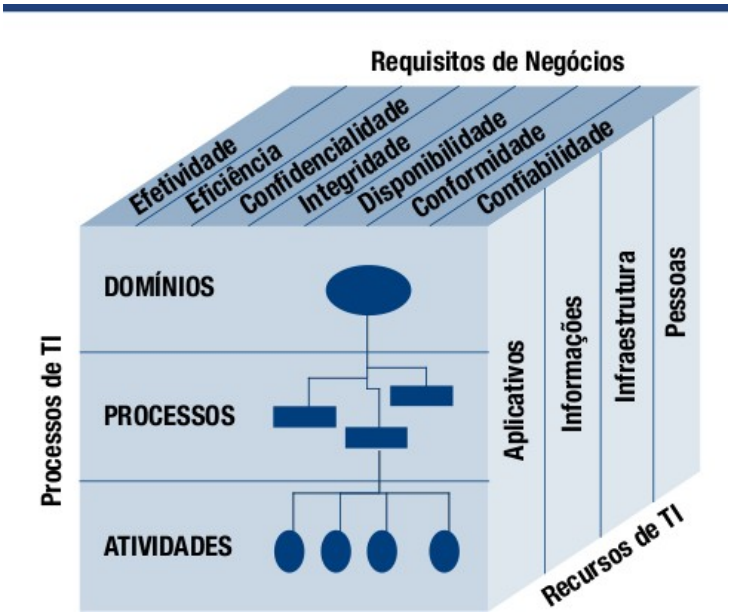

FIG 06 – O cubo COBIT
(Fonte: COBIT, versão 4.1; 2007)

Da análise detalhada da figura 07, verifica-se que cada processo do COBIT é definido seguindo uma sequência, onde os controles dos processos de TI que satisfazem os requisitos do negócio são permitidos por declarações de controle considerando práticas de controle. Ou seja, os objetivos de controle do COBIT são definidos a partir dos requisitos de negócio (ZORELLO,2005).

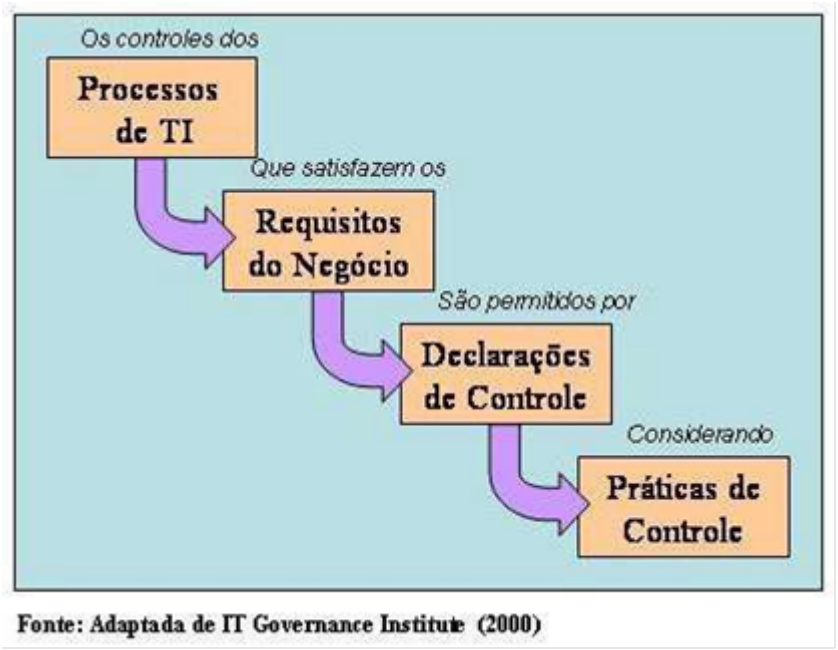

Fig 07 – Sequência para definição dos processos do COBIT
(Fonte: ZORELLO,2005)

Em termos gerais, o principal foco do COBIT é possibilitar um efetivo controle e gerenciamento de TI em um nível estratégico elevado, organizando seu suporte em três níveis: executivos da alta administração; gerente de TI e negócios; e profissionais de avaliação, controle e segurança. Seus produtos são, conforme ilustrado na figura 08 (COBIT 4.1; 2007):

- Board Briefing on IT Governance, 2th Edition – publicação para os executivos entenderem qual o principal papel e questões de gerenciamento de TI;
- Diretrizes de gerenciamento / modelos de maturidade – auxiliam na designação de responsabilidades, avaliação de desempenho e “benchmark” (referência), e trata da solução de deficiência de capacidades;
- Métodos - organiza os objetivos de governança de TI por domínios e processos de TI e os relaciona com os requisitos de negócio;
- Objetivos de controle - proporcionam um completo conjunto de requisitos de alto nível a serem considerados pelos executivos para o controle efetivo de cada processo;
- IT Governance Implementation Guide: Using COBIT and Val IT TM, 2th Edition – provê um mapa geral para implementar a governança de TI usando os recursos do COBIT e Val IT;

- COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2th Edition - explica porque e como os controles devem ser implementados; e
- IT Assurance Guide: Using COBIT – traz orientações de como o COBIT pode ser usado para suportar as variadas atividades de avaliação junto com sugestões de passos de testes para todos os processos e objetivos de controle de TI.

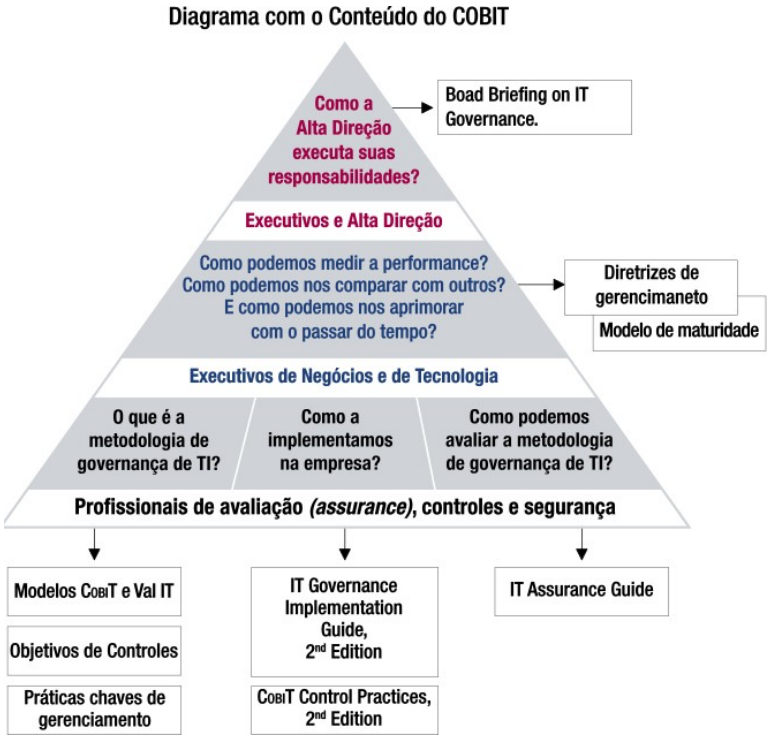

FIG 08 – Diagrama representativo dos conteúdos do COBIT
(Fonte: COBIT, versão 4.1; 2007)

Para medir a eficácia e identificar as responsabilidades aos processos de negócio e de TI, o modelo de maturidade para gerenciamento e controle dos processos de TIC é baseado em um método para avaliar a organização, permitindo que ela seja pontuada de um nível de maturidade não existente (0) até otimizado (5), graficamente apresentado na figura 09.

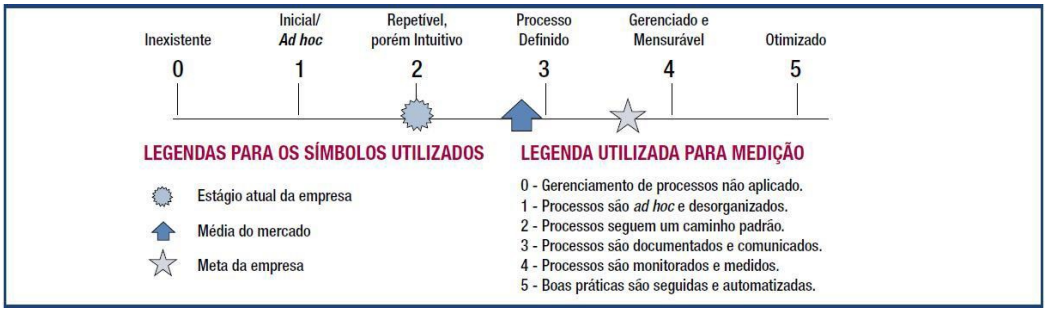

FIG 09 – Representação gráfica do modelo de maturidade
(Fonte: COBIT, versão 4.1; 2007)

2.2.2 Information Technology Infrastructure Libary (ITIL)

Cada vez mais há uma dependência de TIC para que uma Instituição possa atingir os objetivos do negócio. Com isso, a TIC deve estar perfeitamente alinhada com a estratégia da Instituição. No que se refere ao alinhamento estratégico, a seção anterior abordou uma das ferramentas mais comuns de governança de TI: o COBIT. Entretanto, para um maior detalhamento das técnicas de governança na área operacional, o COBIT, por exemplo, não se aplica, pois é uma ferramenta mais adequada para o nível estratégico, estruturada em um conjunto de boas práticas (*framework*) de “o que” se deve fazer, mas não especifica, detalhadamente, o “como“ fazer (operacional). Desta forma, será abordado o modelo ITIL, que pode ser empregado em conjunto com o COBIT.

A primeira versão do modelo ITIL foi desenvolvida, na década de 1980, pela Agência Central de Telecomunicações e Computação (CCTA – Central Computer and Telecommunication Agency), do governo britânico. Depois, em 2001, foi fundida ao Escritório Governamental de Comércio (OGC - Officce Government Commerce), sendo amplamente difundida e aceita na Europa como conjunto de boas práticas de TI. O modelo ITIL foi concebido como um padrão aberto, com objetivo de desenvolver metodologias e criar padrões dentro dos órgãos governamentais, buscando melhorar e aprimorar os processos internos. Esse modelo apresenta as boas práticas em forma de livros que descrevem as melhores práticas em gestão de TI, detalham como os processos devem ser organizados e o gerenciamento da infraestrutura de TI. Atualmente, o ITIL está na versão 3 (publicada em 2007) e atualizada em 2011, sendo que há previsão do lançamento da nova versão, ainda em 2019.

O modelo foi baseado em gerenciamentos e processos que estão inseridos em uma série de sete publicações (livros) versão 2, conforme ilustrado na figura 10 e cinco volumes, denominados ciclo de vida de serviço, na versão 3. Cada publicação é direcionada a uma área do framework (conjunto de boas práticas). Na futura versão, estão previstas a inclusão de orientações práticas sobre como modelar e adaptar uma estratégia de TI em um ambiente mais moderno e cada vez mais complexo, entretanto, sem perder os elementos centrais da versão anterior. Tal atualização consolidará as boas práticas dessa metodologia ágil, amplamente empregada na Indústria 4.0, conhecida como Quarta Revolução Industrial.

Fig 10 – Livros do ITIL
(Fonte: SODRÉ; SOUZA, 2007)

Segundo (SODRÉ; SOUZA, 2007) e (TJDFT), o alinhamento do ITIL, na versão 2, é dividido nas seguintes áreas de gerenciamento:

- gerenciamento de serviços de TI – detalha o suporte diário e atividades de manutenção relacionados aos serviços de TI;
- gerenciamento de segurança – descreve os processos de planejamento e gerenciamento detalhando no nível de Segurança da Informação e Serviços de TI, incluindo todos os aspectos associados com a reação dos incidentes, a avaliação e gerenciamento dos riscos e vulnerabilidade, e implementação de custos justificáveis para a implementação de contra-recursos (estratégia de segurança);
- perspectivas do negócio – fornece um conselho e guia para ajudar o pessoal de TI a entender como eles podem contribuir para os objetivos do negócio e como suas funções e serviços podem estar mais bem alinhados e aproveitados para maximizar sua contribuição para a organização;
- gerenciamento de infraestrutura – atua em todos os aspectos do Gerenciamento da Infraestrutura como a identificação dos requisitos do negócio, testes, instalação, entrega, e otimização das operações normais dos componentes que fazem parte dos Serviços de TI;
- gerenciamento das aplicações – descreve como gerenciar as aplicações a partir das necessidades iniciais dos negócios, passando por todos os estágios do

ciclo de vida de uma aplicação, incluindo até a sua saída do ambiente de produção (quando o sistema é aposentado). Este processo dá ênfase em assegurar que os projetos de TI e as estratégias estejam corretamente alinhados com o ciclo de vida da aplicação, assegurando que o negócio consiga obter o retorno do valor investido;

- gerenciamento e organização – cobre os processos necessários para o planejamento, organização e entrega de Serviços de TI com qualidade e se preocupa, ao longo do tempo, com o aperfeiçoamento desta qualidade; e
- planejamento e implementação – examina questões e tarefas envolvidas no planejamento, implementação e aperfeiçoamento dos processos do Gerenciamento de Serviços dentro de uma organização. Também foca em questões relacionadas à Cultura e Mudança Organizacional.

Quadro 1 – Processos ITIL

Fase do Ciclo de Vida do Serviço	**Processo**	**Publicação**	**Extensão**
Estratégias de Serviço	Geração de Estratégia	SS	
	Gerenciamento Financeiro	SS	
	Gerenciamento de Portfólio de Serviço	SS	SD
	Gerenciamento da Demanda	SS	SD
Desenho de Serviço	Gerenciamento da Capacidade	SD	SO, CSI
	Gerenciamento da Continuidade de Serviço de TI	SD	CSI
	Gerenciamento da Disponibilidade	SD	CSI
	Gerenciamento de Fornecedor	SD	
	Gerenciamento de Segurança de Informação	SD	SO
	Gerenciamento do Catálogo de Serviço	SD	SS
	Gerenciamento do Nível de Serviço	SD	CSI
Transição de Serviço	Avaliação de Serviço	ST	
	Gerenciamento da Configuração e de Ativo de Serviço	ST	SO
	Gerenciamento de Liberação e Implantação	ST	SO
	Gerenciamento de Mudança	ST	

Continua

Continuação

Fase do Ciclo de Vida do Serviço	Processo	Publicação	Extensão
Transição de Serviço	Gerenciamento do Conhecimento	ST	CSI
	Planejamento e Suporte da Transição	ST	
	Validação de Serviço e Teste	ST	
Operação de Serviço	Cumprimento de Requisição	SO	
	Gerenciamento de Acesso	SO	
	Gerenciamento de Evento	SO	
	Gerenciamento de Incidente	SO	CSI
	Gerenciamento de Problema	SO	CSI
Melhoria Contínua de Serviço	Medição de Serviço	SD	CSI
	Melhoria em 7 Etapas	CSI	
	Relatório de Serviço	CSI	

(Fonte: ITIL, 2011)

Apesar do ITIL abordar as áreas de planejamento estratégico, operacional e tático, seu foco é muito mais voltado para operacional e tático do que estratégico. Assim a grande maioria das empresas implementava apenas a área de Gerenciamento de Serviços de TI (Prestação de Serviços e Suporte de Serviços).

Em 2007, houve uma nova versão, atualizada em 2011 (v3), com a biblioteca de cinco volumes (fases do ciclo de vida do serviço) e vinte e seis processos, dos quais apenas um volume: Estratégias de Serviços (SS – Service Strategy) é relacionado ao planejamento estratégico. Os demais quatro volumes são direcionados para as áreas operacionais e táticas: Desenho de Serviço (SD – Service Design), Transição de Serviço (ST – Service Transition), Operação de Serviço (SO – Service Operation) e Melhoria Contínua de Serviço (CSI - Continual Service Improvement), de acordo com o quadro 1.

A estruturação do ITIL nessas cinco fases do ciclo de vida tem como núcleo principal o livro “Estratégias de Serviço”, onde são identificados os requisitos e o pacote de níveis de serviço (SLP – Service Level Package) para os tipos de serviço de TI do negócio da Instituição. Complementado e envolvendo essa fase central, há as bibliotecas de “Desenho de Serviço”, “Transição de Serviço” e “Operação de

Serviço". Envolvendo todas essas fases encontra-se a biblioteca "Melhoria de Serviço Continuada". A figura 11 procura exemplificar esse conceito de forma ilustrativa.

Fig 11 – Conceitos ITIL
(Fonte: http://jkolb.com.br/fundamentos-itil/)

O ciclo de vida da estruturação do ITIL divide-se em três níveis de conceituação:

- análise de requisitos: Estratégia de Serviço e Desenho de Serviço;
- implantação no ambiente: Transição de Serviço; e
- operação e melhoria em produção: Operação de Serviço e Melhoria de Serviço Continuada.

Várias Instituições implementam apenas o primeiro nível, mas é extremamente importante todas as fases do ciclo para que haja uma realimentação do sistema, como é abordado no terceiro nível.

Conforme apresentado, a ferramenta COBIL tem uma abordagem mais aplicada a processos em um nível mais macro, com uma especificação no campo da estratégia, monitorando continuamente os processos de qualidade dos serviços prestados. Enquanto isso, a ferramenta ITIL detalha procedimentos de forma operacional, relacionados à gerência de serviços, de infraestrutura de Tecnologia da Informação e Comunicação (TIC) e aplicativos da atividade fim da organização. A figura 12 apresenta uma relação entre as ferramentas, destacando a atuação do COBIT, na área estratégica de qualidade dos serviços e, o ITIL, na área de operação de controle e execução de processos.

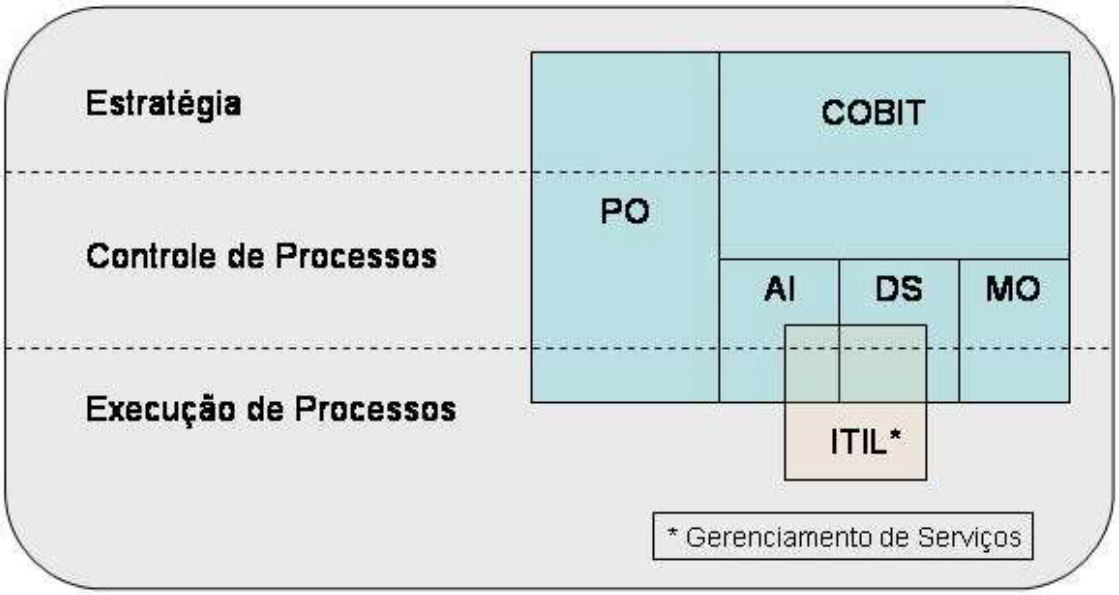

Fig 12 – Relacionamento entre COBIT e ITIL
(Fonte: ZORELLO, 2005)

2.3 GOVERNANÇA DE TIC NO GOVERNO FEDERAL

Em consonância com o exposto e alinhado com os avanços tecnológicos, o Governo Federal, através do Decreto nº 7579/11, dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), antigo Sistema de Informática do Serviço Público. O SISP gera informações: da organização, da operação, do controle, da supervisão e da coordenação de toda a Administração Pública Federal direta, autárquica e fundacional. Essa gerência está a cargo do Ministério do Planejamento, atuando por intermédio da Secretaria de Logística e Tecnologia da Informação (SLTI), no que tange à normatização e coordenação das ações do sistema.

Como forma de nortear e servir de referência para o Governo Federal, a SLTI elaborou uma série de obras de governança de TI, em que se destacaram: a “Metodologia de Gerenciamento de Projetos do SISP” e a “Metodologia de Gerenciamento de Portfólio de Projetos do SISP”, que são baseadas nas boas práticas para o gerenciamento de projetos abordadas no Project Management Body of Knowledge (PMBoK).

Portanto, independente do grau de importância e/ou relevância da Governança Pública e da Governança de TI, para melhores práticas de gestão, os agentes da administração federal são regidos pelas normas e orientações desses

órgãos reguladores, principalmente, no setor de aquisição, a irrestrita observância da Instrução Normativa (IN) nº 04/2010, do MPOG/SLTI, atualizada recentemente pela IN nº 01/2019, da Secretaria de Governo Digital (SGD). Em particular, as IN04/2010 e IN01/2019 são específicas para as soluções de TIC. Entretanto, para lograr êxito, não bastam apenas orientações, planejamentos e planos bem definidos. Outra grande necessidade é a sensibilização e a participação da Alta Administração, a fim de impulsionar e definir as estratégias a serem seguidas.

Em relação ao Exército Brasileiro, a Força mantém em sua estrutura organizacional um Órgão de Direção Setorial (ODS), o Departamento de Ciência e Tecnologia (DCT), que centraliza as regras e as normas de TIC, sendo responsável, portanto, pela gestão de TIC no EB. Apesar de haver um Departamento centralizando as orientações e os planejamentos na área de TIC, foi criado, por meio de Portaria do Comandante do Exército, com a participação de todos os membros do Alto Comando, o Conselho Superior de Tecnologia da Informação do Exército (CONTIEx). Ou seja, com a participação total da Alta Administração EB. Esse Conselho, para dar credibilidade às ações técnicas, criou o Comitê Técnico de TI (COMTEC-TI), com a participação de membros de Organização Militares Diretamente Subordinadas do DCT, que apoiam, tecnicamente, em informações técnicas os pareceres para subsidiar as decisões do CONTIEx.

A figura 13 apresenta o modelo de orientação do MPOG acerca da relação entre os instrumentos de planejamento e seus produtos. No caso do EB, o Planejamento Estratégico Institucional (PEI) chama-se Plano Estratégico do Exército (PEEx) e a Estratégia Geral de Tecnologia da Informação (EGTI) é a Concepção Estratégica e Tecnologia da Informação (CETI). O Plano Estratégico de Tecnologia da Informação (PETI) e o Plano Diretor de Tecnologia da Informação (PDTI), produtos do Planejamento de TI, também recebem essa nomenclatura na Força. No EB, encontra-se esse alinhamento no Objetivo Estratégico (OE), no número sete do Plano Estratégico de Exército (PEEx; 2016-2019), OEE 7 – Aprimorar a Governança de TI. Cabe ao CONTIEx propor e elaborar para aprovação pelo Comando do Exército a Concepção Estratégica de Tecnologia da Informação (CETI). Essa concepção estratégica tem como objetivos definir responsabilidades na área de TI, relacionar os Objetivos Estratégicos de TI (OETI) com os OEE, orientar a elaboração do PETI, aperfeiçoar o controle interno de TI e estabelecer o mapa estratégico de TI. O OETI número 4, OETI 4 – Aperfeiçoar a Governança de TI, está alinhado não só com o OEE

7 mencionado anteriormente, mas também indiretamente com o OEE 6 – Implantar um novo e efetivo sistema de doutrina no EB; e o OEE 9 – Implantar um novo e efetivo sistema de Ciência, Tecnologia e Inovação. O OETI 4 permeia esses dois últimos OEE.

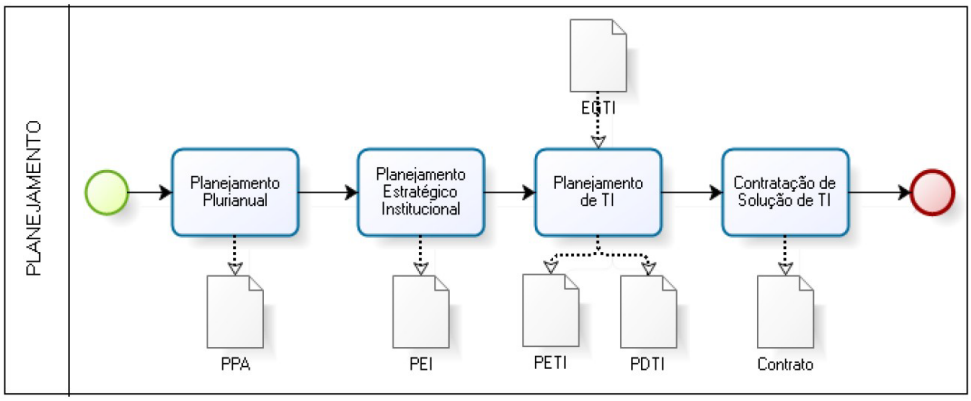

Fig 13 – Relação entre os instrumentos de planejamento
(Fonte: Guia de Elaboração do PDTI, SISP, 2012)

3 PLANEJAMENTO ESTRATÉGICO DE TIC DO GABINETE DE INTERVENÇÃO FEDERAL

3.1 PLANEJAMENTO ESTRATÉGICO DO GABINETE DE INTERVENÇÃO FEDERAL DO RIO DE JANEIRO (GIFRJ)

Inicialmente, cumpre destacar que este trabalho aborda apenas o quesito TIC da Intervenção Federal, não sendo foco outras importantes e eficazes ações realizadas pelo Gabinete de Intervenção Federal (GIF) no Rio de Janeiro. Neste contexto, para uniformizar informações, este capítulo apresentará a estrutura organizacional da área de TIC da Secretaria de Segurança Púbica (SSP), anterior ao momento da Intervenção, e as ações e os planejamentos levados a efeito pelo GIF, a fim de melhorar a gestão e governança de TIC na SSP.

Com o Decreto Federal nº 9.288, de 16 de fevereiro de 2019, que determinou a Intervenção Federal no Estado do Rio de Janeiro, com objetivo de pôr termo ao grave comprometimento da ordem pública, com prazo fixado até 31 de dezembro de 2018, algumas das primeiras ações foi identificar o limite e o alcance de atuação, na área de Segurança Pública do Estado, ou seja, nas: Secretaria de Estado de Segurança (SESEG), Secretaria de Estado de Administração Penitenciária (SEAP) e Secretaria de Estado de Defesa Civil (SEDEC), e criar a arquitetura e a estrutura organizacional, nos níveis político, estratégico, operacional e tático por meio da criação de estruturas "*ad hoc*", conforme a figura 14 (Plano Estratégico da Intervenção Federal na área da Segurança Pública no Estado RJ,2018).

As estruturas do Centro de Coordenação Tático Integrado (CCTI) e Gabinete de Intervenção Federal (GIFRJ) foram as estruturas "ad hoc" criadas com o intuito de permitir o planejamento, a coordenação, o controle e o assessoramento às ações de intervenção e nas operações. Dessa forma, observa-se que, como estruturas temporárias, ao término da Intervenção, as estruturas, tanto do Exército Brasileiro no Rio de Janeiro, Organizações Militares do Comando Militar do Leste (CML), das Secretarias de Estado e de outros agentes envolvidos retornam, no que se refere ao nível político, ao "status quo", portanto, não havendo uma ingerência política no Estado ao término da Intervenção, bem como mantendo preservadas as estruturas federais. Houve, nesse sentido, apenas o uso dual dos Recursos Humanos

e dos meios materiais necessários à condução das atividades relacionadas à Intervenção Federal.

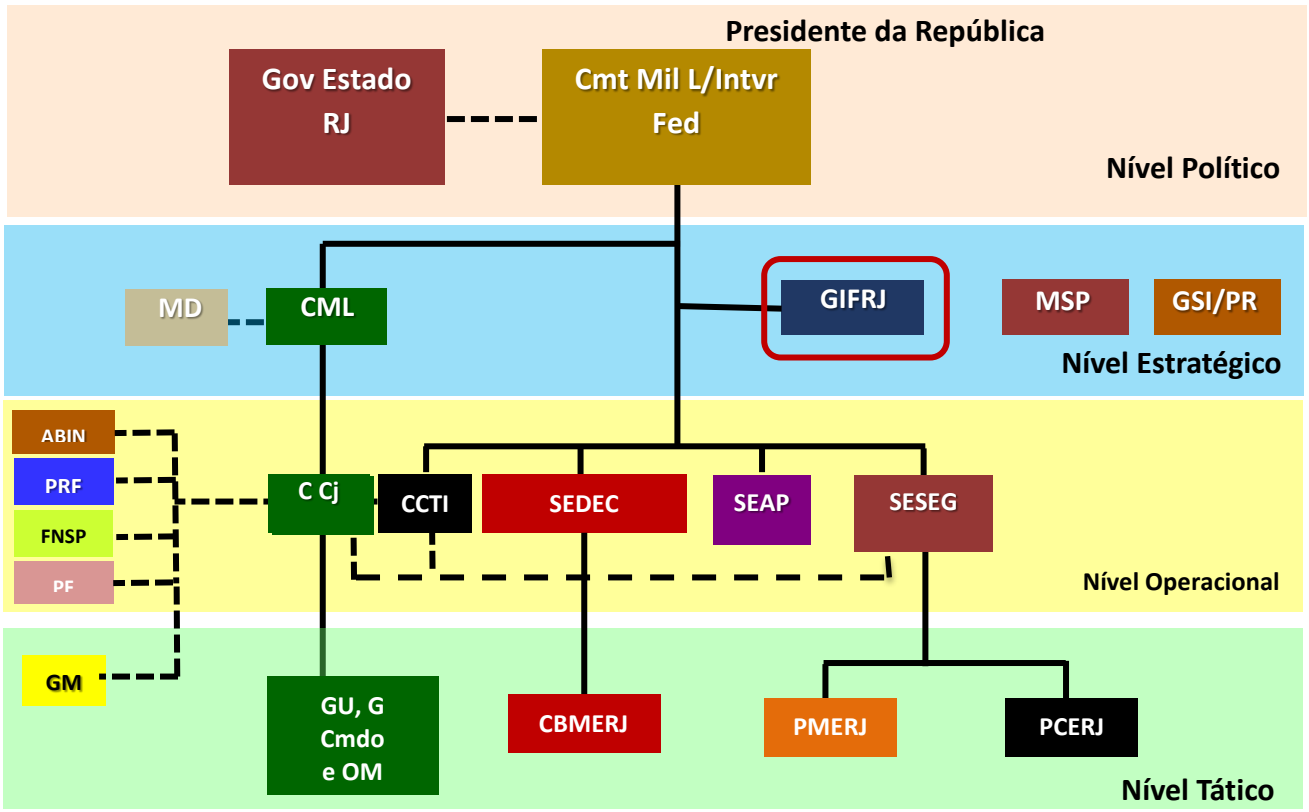

Fig 14 – Arquitetura de Comando e Controle e Relações Institucionais da Intervenção Federal na área de Segurança Pública do RJ
(Fonte: Adaptado de Plano Estratégico da Intervenção Federal na área da Segurança Pública no Estado do RJ, 2018)

O GIFRJ, órgão de planejamento, coordenação e controle, foi organizado em duas secretarias, cuja organização é apresentada na figura 15. A Secretaria de Intervenção Federal (SIF) foi a responsável por conduzir o planejamento e a coordenação das ações e a Secretaria de Administração (SA) promoveu a gestão orçamentária, financeira e patrimonial, incluindo o gerenciamento do legado e da desmobilização.

A área de TIC ficou alocada, mais especificamente, na Coordenação de Comando e Controle da Diretoria de Planejamento e Operações. Entretanto, por sua natureza, foi transversal e indutora, permeando todos os processos, o planejamento, a operação, a aquisição, o legado e a desmobilização.

Uma vez definida a estrutura organizacional, o GIFRJ, na área de TIC, solicitou o apoio do 2º Centro de Telemática de Área (2º CTA), Organização Militar

(OM) responsável pela TIC das OM, no âmbito do CML, para auxiliar a elaboração do planejamento das ações na área de TIC do GIFRJ.

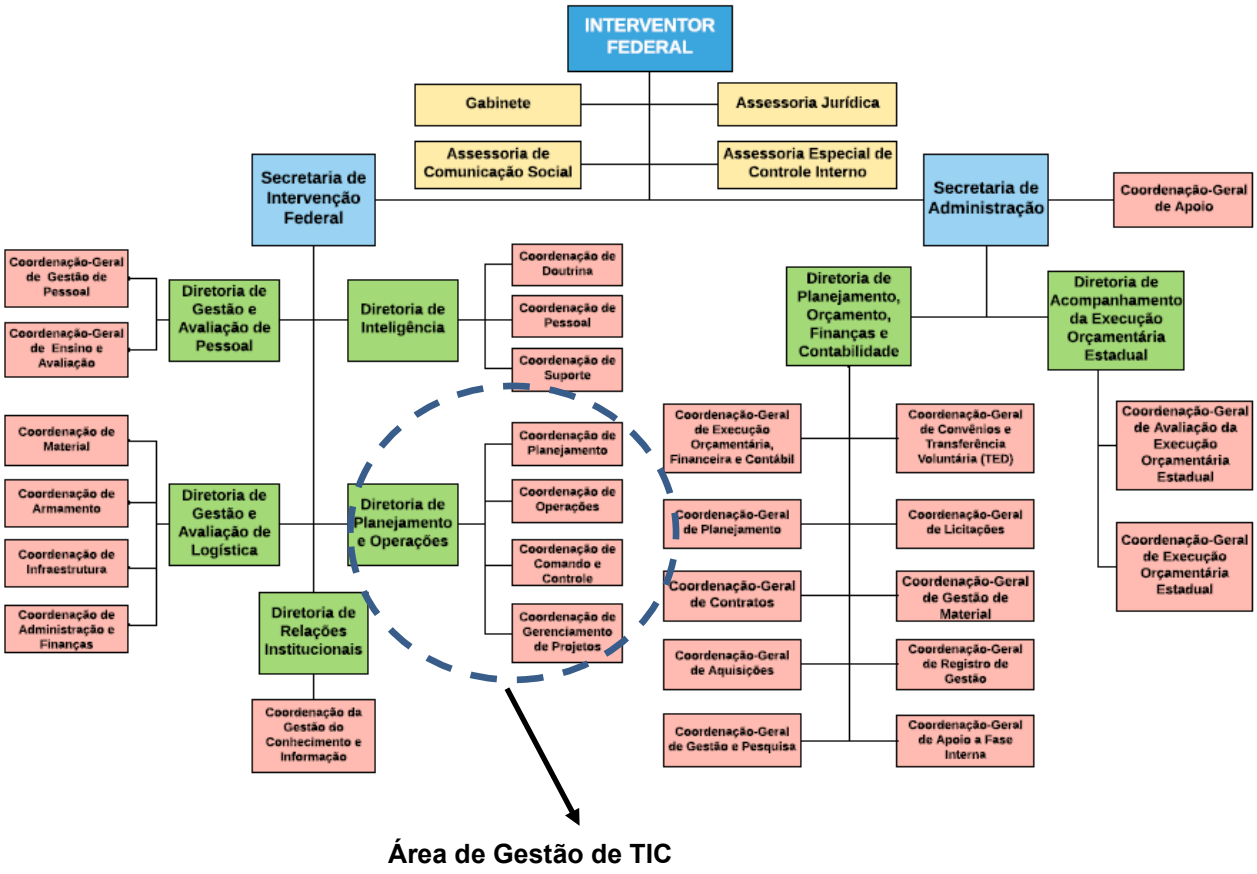

Fig 15 – Organograma do Gabinete de Intervenção Federal
(Fonte: Adaptado de Plano Estratégico da Intervenção Federal na área da Segurança Pública no Estado RJ, 2018)

Coube, portanto, ao 2º CTA coordenar as ações de planejamento e assessoramento no tocante às necessidades de TIC para apoiar os eventos e as operações nas ações de Comando e Controle, bem como orientar e melhorar a gestão de governança nas três Secretarias do Estado, conforme a figura 16. Para que os decisores alcançassem a máxima consciência situacional e agilidade na tomada de decisão, coube ao 2º CTA planejar, projetar e executar toda a infraestrutura que permitiu acesso aos sistemas computacionais corporativos, ou não, que cada órgão envolvido necessitasse visualizar e operar. Nesse contexto, destacam-se circuitos internos de TV, imagens urbanas fixas ou móveis geradas por veículos tripulados ou não, sistemas de comando e controle, videoconferências, sistemas administrativos dos órgãos, acesso as intranet e/ou internet e sistemas de radiocomunicações. Para tanto, foi composta, em termos de recursos humanos, pelo 2º CTA, de forma

permanente e diária, uma escala de oficial superior, que serviu como oficial de ligação junto ao Comando Conjunto do GIFRJ e, com delegação do Chefe do 2º CTA, para tomar decisões que permitissem celeridade, uma vez que, normalmente, o ambiente das operações era volátil, incerto, complexo e ambíguo (VUCA[1]).

Em função dos chamados Grandes Eventos ocorridos anteriormente, principalmente na cidade do Rio de Janeiro, no período de 2011 a 2016, o 2º CTA soube, particularmente, aproveitar aquele período para expandir sua infraestrutura de cabeamento ótico e de rádio enlaces da Rede Metropolitana privativa do EB, integrando-a com diversas agências governamentais. Dessa forma, a malha de rede de conexões e interações permitiu à Rede do 2º CTA alcançar uma elevada capilaridade, alta disponibilidade e resiliência, sendo aproveitada, em grande parte, para apoiar as Operações de Segurança Pública ocorridas durante a Intervenção.

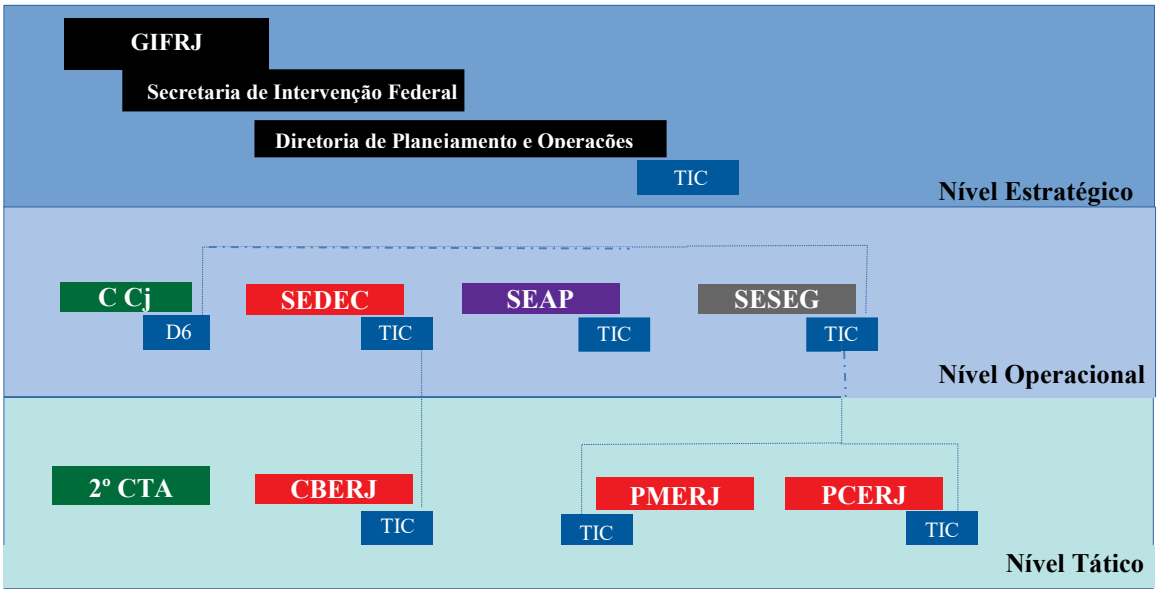

Fig 16 – Organização da TIC na Intervenção Federal
(Fonte: Adaptado de Plano Estratégico da Intervenção Federal na área da Segurança Pública no Estado RJ, 2018)

Paralelamente, o 2º CTA também disponibilizou uma equipe fixa para compor a Coordenação de Comando e Controle da Diretoria de Planejamento e Operações, apoiando na gestão de TIC do GIFRJ e buscando gerar, para as Secretarias de Segurança Pública, um modelo de governança de TIC.

---

[1] VUCA é um acrônimo das palavras em inglês volatility (volátil), uncertainty (incerteza), complexity (complexidade) e ambiguity (ambiguidade), que em português seria VICA.

3.1.1 Estrutura de TIC da Secretaria de Segurança Pública do Rio de Janeiro

Uma vez constituída a equipe de TIC da Coordenação de Comando e Controle, diversas reuniões foram realizadas para compreender a estrutura e a governança de TIC da Secretaria de Segurança Pública, até então existentes. Assim, alguns levantamentos importantes foram diagnosticados:

- existência de uma infraestrutura moderna de TIC, fruto do legado dos Grandes Eventos (Copa do Mundo-2014 e Jogos Olímpicos-2016), em franca degradação devido à ausência de manutenção e atualizações dos sistemas;
- ausência de boas práticas, gestão e governança de TIC;
- falta de planejamento e disponibilidade regular de recursos financeiros;
- recursos adquiridos, em sua maioria, com práticas de dispensa de processos licitatórios, impostas por emergência ou por inexigibilidade;
- centralização de ações de infraestrutura, não consideradas de TIC, na edificação do Centro Integrado de Comando e Controle (CICC), como por exemplo responsabilidade sobre periféricos computacionais (impressoras, papeis) e configurações de contas que poderiam ser separadas da área de planejamento de TIC; e
- existência de uma melhor infraestrutura de TIC na SESEG do que nas SEDEC e SEAP, em função da maioria dos sistemas integrados estarem localizados no CICC, que é subordinado à SESEG.

A TIC na SESEG, ilustrada no organograma da figura 17, encontra-se alocada à Superintendência de Administração e Controle, sendo responsável pela infraestrutura de TIC que permeia toda a SESEG. Na SEAP e na SEDEC existe um pequeno setor de TIC que é responsável pelas redes locais e sistemas internos dessas secretarias como, por exemplo, o sistema de Circuito Fechado de Televisão (CFTv) do sistema prisional da SEAP ou especifico de Defesa Civil e Corpo de Bombeiros, no caso da SEDEC.

Tendo em vista a equipe de TIC da SESEG ser reduzida, uma primeira sugestão apresentada para otimizar as ações foi retirar de sua estrutura os atendimentos aos usuários do CICC no que tange a assuntos mais elementares: elaborar palestras, questões de impressões de documentos, tirar dúvidas de acesso à provedores externos à intranet. Esses apoios deveriam ser de algum elemento

interno das outras superintendências, responsáveis pelo atendimento de primeiro nível ao usuário. Diferentemente, nas secretarias SEAP e SEDEC não poderia ser feita essa alteração, por se tratar de Secretarias com menores estruturas de TIC e reduzida capacidade de RH, podendo o ônus desses encargos indiretos de TIC ficar centralizados na própria estrutura de TIC dessas Secretarias. A SEAP e SEDEC contavam apenas com um setor de TI, com cerca de 15 (quinze) profissionais, e não uma Superintendência.

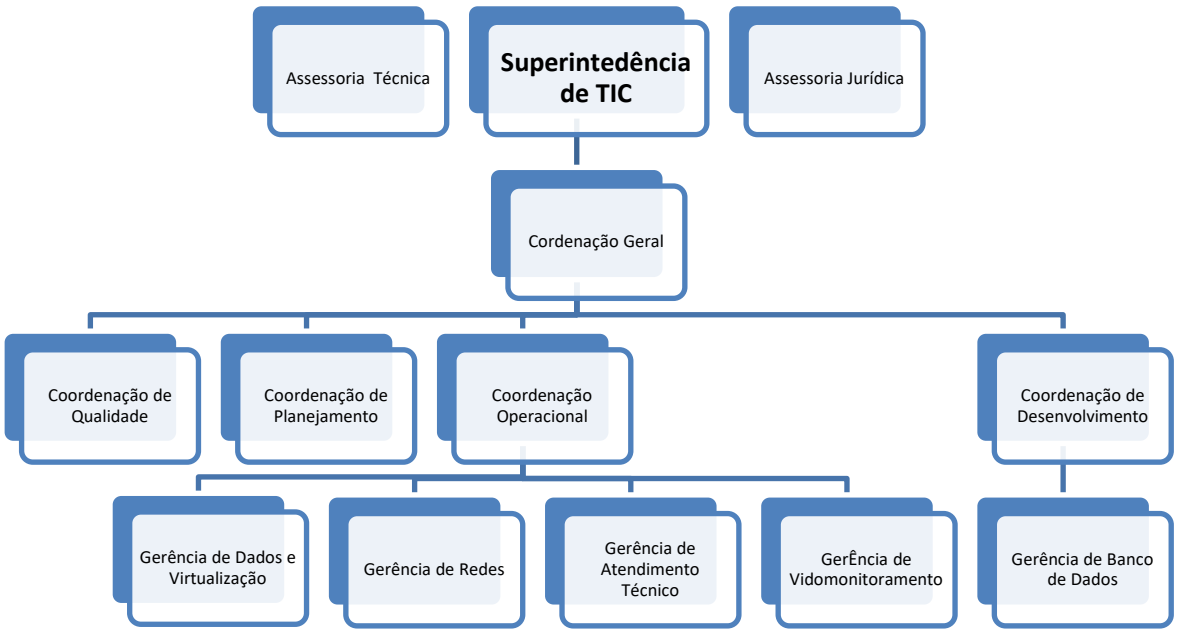

FIG 17 – Organograma de TIC da Secretaria de Segurança (SESEG)
(Fonte: o autor)

Outra importante contribuição implementada foi o repasse de conceitos de governança de TIC, apresentando algumas técnicas das ferramentas usadas pelo EB: ITIL e COBIT, alinhamento com orientações da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MPOG), como as Instruções Normativas nº 04 e nº 05 (IN04 e IN05), e, por fim, um Plano Diretor de TIC (PDTIC) estruturado e relacionado com o Planejamento Estratégico do GIFRJ, como apresentado a seguir.

3.2 PLANO DIRETOR DE TIC DO GIFRJ

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) é um documento de gestão na área de TIC. Tem como motivação a necessidade de se buscar um alto nível de eficiência na gestão de recursos e serviços de TIC em apoio às Secretarias sob a Intervenção Federal, críticos para os diversos processos da área finalística. Visa a melhoria contínua dos serviços de TIC no âmbito dos Órgãos de Segurança Pública no Estado do Rio de Janeiro, à execução de suas missões, bem como à manutenção da qualidade do atendimento aos serviços internos do GIFRJ (PDTIC GIFRJ,2018).

Com base no Planejamento Estratégico do GIFRJ para a Intervenção Federal, aprovado pela Portaria Normativa nº 05 do GIFRJ, de 29 de maio de 2018, o PDTIC GIFRJ possibilitou alinhar o Plano de TIC aos Objetivos Estratégicos (OE) do Planejamento Estratégico do GIFRJ e suas respectivas estratégias, conforme ilustra quadro 2.

Quadro 2 – Objetivos Estratégicos e Estratégias do Planejamento do GIFRJ

OE	DESCRIÇÃO	ESTRATÉGIA
OE/01	Diminuição dos índices de criminalidade.	1.1 - Empregar com efetividade os OSP no cumprimento de suas missões constitucionais 1.2 - Buscar a eficácia das Forças de Segurança
OE/02	Recuperar a capacidade operativa dos Órgãos de Segurança Pública (OSP) do Estado do Rio de Janeiro	2.1 - Fortalecer as estruturas de formação e capacitação de recursos humanos das instituições. 2.2 - Reorganizar a gestão de recursos humanos dos OSP. 2.3 - Aquisição, manutenção e recuperação do material de emprego individual e coletivo para os OSP do Estado. 2.4 - Organizar as funções logísticas. 2.5 – Elaborar um Plano Diretor de Obras e Serviços (PDOS). 2.6 - Aquisição do material de subsistência (expediente, limpeza e consumo em geral) para os OSP e SEAP do Estado
OE/03	Articulação das instituições dos entes federativos	3.1 - Desenvolver protocolos interagências para as ações de segurança pública e inteligência. 3.2 – Potencializar o CICC como órgão de Comando e Controle para as ações de Segurança Pública.

Continua

Continuação

OE/04	Fortalecimento do caráter institucional da Segurança Pública e do Sistema Prisional.	4.1 - Reorganizar a estrutura da Segurança Pública do Estado do Rio de Janeiro. 4.2- Sistematizar visitas e inspeções corporativas 4.3 - Resgatar e desenvolver princípios, crenças, valores, e tradições nos OSP. 4.4 – Aperfeiçoar a Gestão Financeira dos OSP, SEAP e SESEG. 4.5 - Melhorar o relacionamento e a imagem dos OSP junto à população.
OE/05	Melhoria da qualidade e da gestão do sistema prisional	5.1 - Reorganizar a estrutura organizacional e de gestão da SEAP 5.2 – Modernizar a infraestrutura do sistema prisional do estado
OE/06	Implantar estruturas necessárias ao planejamento, coordenação e gerenciamento das ações estratégicas da Intervenção Federal	6.1 – Prover as estruturas da Intervenção Federal com meios (pessoal e material) necessários ao planejamento, coordenação e gerenciamento das ações estratégicas

(Fonte: Adaptado de Plano Estratégico da Intervenção Federal na área da Segurança Pública no Estado RJ, 2018)

Assim, com base nos Objetivos Estratégicos (OE), para a composição do PDTIC foram identificadas as necessidades, categorizando-as segundo a classificação a seguir:

- **Capacitação** (Tipo “C”): necessidades de capacitação, treinamento e desenvolvimento de competências relacionadas com tecnologia da informação, tanto para a equipe técnica, quanto para o usuário final;
- **Projetos** (Tipo “P”): necessidades relacionadas à configuração ou implementação de infraestrutura sobre a base tecnológica existente ou aquisição/expansão da base;
- **Gestão** (Tipo “G”): necessidades relacionadas com mapeamento, análise, revisão e melhoria de processos de negócios; e
- **Sustentação** (Tipo “S”): necessidades relacionadas a suporte de infraestrutura e sistemas, compreendendo suporte funcional, manutenções corretivas e preventivas (na forma de contratos) e atendimento de questionamentos sobre os sistemas (inclusive investigação de possíveis erros reportados pelos usuários).

O quadro 3 apresenta as necessidades levantadas, relacionando-as com as categorias e origem dos OE do Planejamento Estratégico do GIFRJ. O OE 06 foi colocado em uma segunda versão do Planejamento Estratégico do GIFRJ, por isso

não está relacionado na versão do PDTIC. Mas o OE 06 poderia ser indutor e permear todas as necessidades identificadas, de N1 a N8.

Quadro 3 - Necessidades levantadas no PDTIC do GIFRJ

Id	Cat	Descrição da Necessidade	Origem
N1	P/S	Implantar a Infraestrutura de TIC em apoio às operações das Forças de Segurança	OE 01 - Estratégia 1.2
N2	P/S	Aperfeiçoar a infraestrutura de TIC para o incremento da capacidade operativa dos OSP	OE 02 - Estratégia 2.4
N3	P/S	Implantar melhorias necessárias para a hospedagem do Portal de Segurança no CICC	OE 03 - Estratégia 3.2
N4	P/G	Implantar melhorias necessárias na Infraestrutura de TIC do CICC para maior integração dos sistemas e serviços em proveito das ações de Segurança Pública	OE 03 - Estratégia 3.2
N5	P/S	Desenvolver um sistema unificado de chamadas de emergência	OE 03 - Estratégia 3.2
N6	P/S	Implantar melhorias da infraestrutura de TIC necessárias para a unificação dos sistemas de inteligência nos OSP	OE 04 - Estratégia 4.1
N7	P/S	Implantar um sistema de vigilância e monitoramento em apoio às atividades de administração penitenciária	OE 05 - Estratégia 5.2
N8	S/C	Capacitar pessoal interno para melhorar gerenciamento das soluções de TIC, incluindo contratadas, em apoio à Segurança Pública	OE 02 - Estratégia 2.4 Análise SWOT

(Fonte: Adaptado de Plano Estratégico da Intervenção Federal na área da Segurança Pública no Estado RJ, 2018)

Constitui anexo ao presente trabalho o PDTIC em sua versão completa, par fins de consultas complementares.

3.3 MODELO DE AQUISIÇÃO ADOTADO PELO GIFRJ

Nesta seção será apresentada a estratégia adotada para atender, principalmente, ao OE 06 do Planejamento Estratégico do GIFRJ. Ao longo do trabalho foram apresentadas diversas técnicas e ferramentas de boas práticas e melhoria dos processos de gestão e governança de TIC. Ressalta-se que boas práticas devem gerar resultados práticos positivos e não apenas processos teóricos. Para atender ao GIFRJ, buscou-se atender às orientações do Governo Federal para soluções de TIC, através da IN04, MPOG/SLTIC. Neste contexto, o modelo de aquisição de solução de TIC foi dividido em três fases:

1) Planejamento da Contratação;

2) Seleção do Fornecedor; e

3) Gestão do Contrato.

A figura 18 apresenta, de forma resumida, alguns processos necessários em cada fase da aquisição. Entre a fase do Planejamento da Contratação e a Seleção do Fornecedor ocorre a etapa licitatória, onde há a elaboração de uma juntada de documentações, dentre as quais destaca-se o Termo de Referência/Projeto Básico, que descreve, tecnicamente, o que se deseja contratar, e o Edital, com todas as regras do certame licitatório. Importante destacar a necessidade de o encaminhamento do processo para os órgãos de assessoramento jurídico afim de assegurar que órgãos externos possam ratificarem que estão sendo cumpridos todos os princípios da Administração Pública: Legalidade, Impessoalidade, Moralidade, Publicidade e Eficiência.

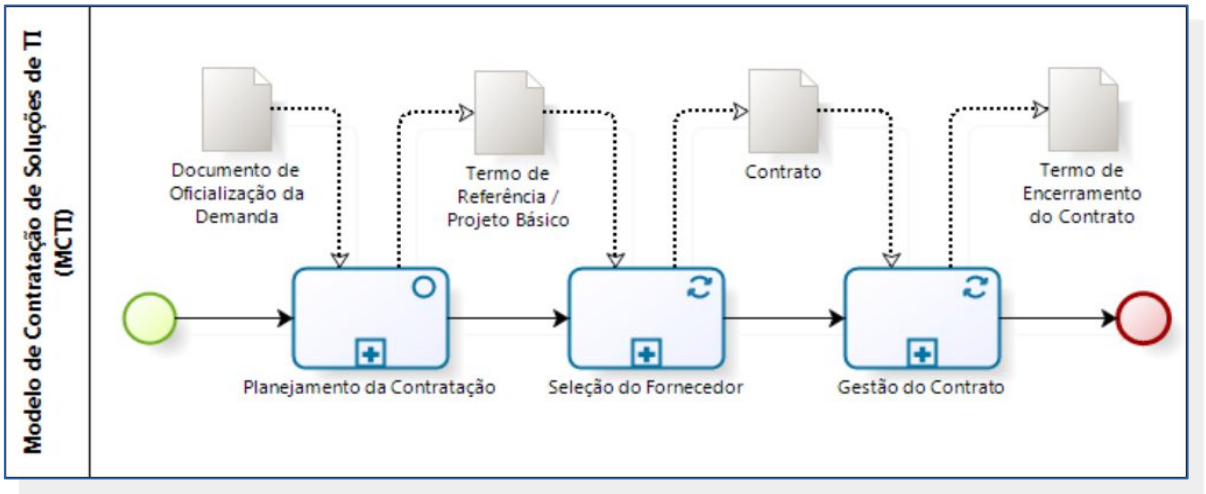

Fig 18 – Modelo de Contratação de TIC do Governo Federal usado no GIFRJ
(Fonte: Guia Prático para Contratação de Solução de Tecnologia da Informação v1.1 do MPOG, 2011)

Para uma melhor compreensão do processo, faz-se necessário analisar os principais interessados nas atividades, denominados atores ou agentes, podendo ser internos ou externos às fases do modelo de aquisição, conforme apresentado na figura 19.

Para se obter êxito nas contratações, algumas boas práticas devem ser consideradas nas três fases. Na fase de Planejamento da Contratação observa-se a atuação direta da chefia, isto é, do agente interessado na contratação de TIC, junto aos principais clientes e potenciais patrocinadores, com orientações técnicas, podendo se valer de diversas formas de contratação. No caso do GIFRJ, esse órgão de assessoramento, conforme relatado anteriormente, foi o 2º CTA.

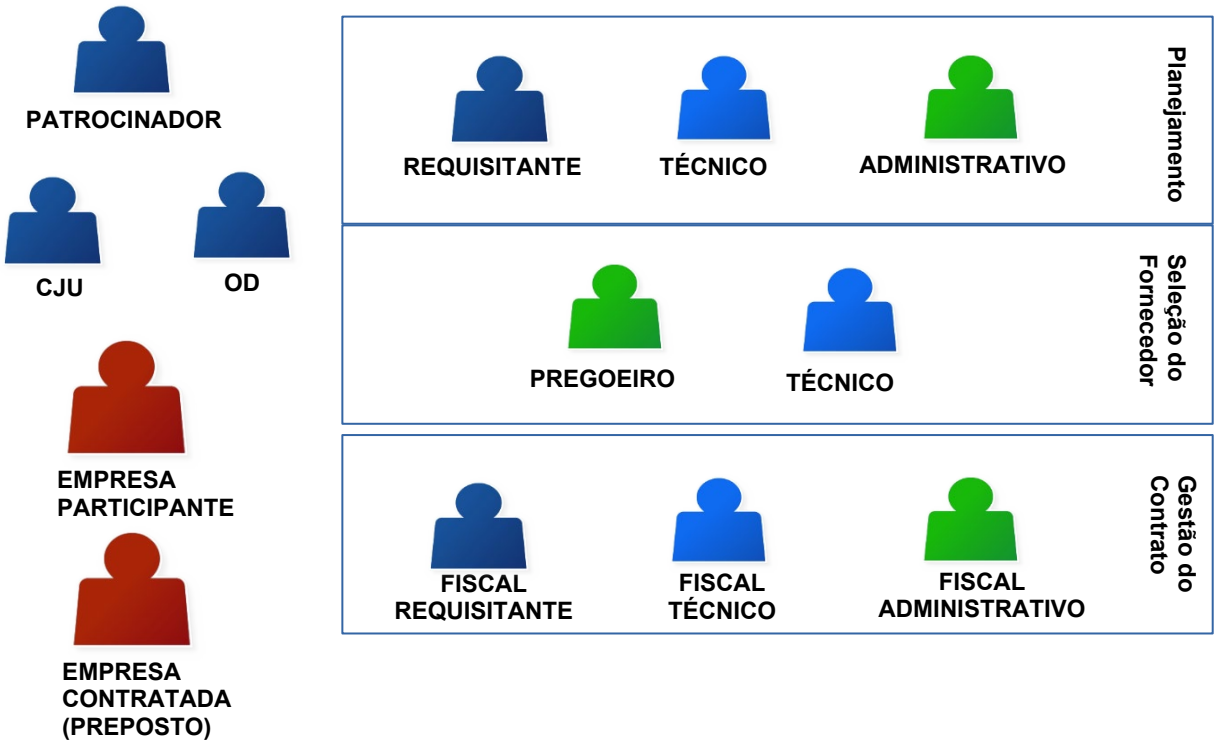

FIG 19 – Principais interessados no processo
(Fonte: palestra 2º CTA, 2018)

Uma forma de agilizar os processos aquisitórios, quando possível, é a participação em processos semelhantes de outros órgãos, as chamadas Intenções de Registro de Preços (IRP). A participação em IRP pode tornar o processo mais ágil e possibilita melhores práticas, com valores menores nos certames, devido ao fornecedor poder atender a uma maior quantidade de órgãos com o mesmo item a ser adquirido. Entretanto, devido à especificidade e unicidade dos processos para a Intervenção, essa prática não foi muito usual. Outra boa prática recomendável, seria iniciar o planejamento em “A-1”, ou seja, no ano anterior. Essa prática também não pôde ser aplicada uma vez que a Intervenção não foi planejada com antecedência e tinha prazo de término no mesmo ano fiscal. Entretanto, foi possível propiciar à área técnica um constante contato com tecnologias atuais por meio da participação em diversos fóruns, seminários, palestra e visitas, em órgãos que utilizavam tecnologias de sucesso em Segurança Pública, antes de decidir qual tecnologia seria empregada para atender à demanda levantada.

Outras técnicas de boas práticas na fase de Planejamento da Contratação adotadas pelo GIFRJ foram a criação de: Grupos de Trabalho permanentes para o gerenciamento do processo, com a participação dos atores de diversas áreas (demanda técnica e administrativa), coordenados pela chefia da Coordenação de

Comando e Controle do GIFRJ; o estabelecimento de um Escritório de Projetos integrador das áreas finalísticas, gerenciando as demandas, relacionamento com clientes e portifólio de serviços e projetos; e a utilização de modelos pré-definidos de documentos, alinhados com as IN04 e a Consultoria Jurídica da União (CJU) regional, para os diversos artefatos (documentos), revisados, periodicamente, por todas as áreas. Planejar os processos de seleção dos fornecedores (licitação), separados por tipo de serviço ou material, permite uma maior participação de empresas especializadas e um número de itens menores, o que aumenta, consideravelmente, as chances de êxito no certame.

Cumpre destacar que o modelo de contratação da IN04 sugere as seguintes documentações, denominadas artefatos:

Artefato 1: Documento de Oficialização de Demanda;

Artefato 2: Estudo Técnico Preliminar;

Artefato 3: Análise de Riscos;

Artefato 4: Termo de Referência ou Projeto Básico;

Artefato 5: Plano de Inserção;

Artefato 6: Plano de Fiscalização;

Artefato 7: Termo de Ciência;

Artefato 8: Termo de Compromisso;

Artefato 9: Ordem de Serviço ou Fornecimento de Bens;

Artefato 10: Termo de Recebimento Provisório;

Artefato 11: Termo de Recebimento Definitivo;

Artefato 12: Termo de Encerramento;

Artefato 13: Plano de Capacidade; e

Artefato 14: Histórico de Gestão de Contrato.

Oportuno, também, ressaltar que o Governo Federal, por intermédio do MPOG, elaborou, em 2011, um Guia Prático para Contratação de Solução de Tecnologia da Informação, o qual descreve todas as etapas para a contratação de soluções de TIC e apresenta "*templates*" que são modelos de documentos, com os artefatos apresentados anteriormente, disponíveis no sítio eletrônico: <https://www.governodigital.gov.br/documentos-e-arquivos/guia-pratico-para-contratacao-de-solucoes-de-ti-v1.1.pdf>.

Como o critério para a Administração Pública normalmente é o de menor custo, uma descrição técnica apurada e detalhada, congruente com as necessidades levantadas, permite satisfazer o critério de qualidade, eliminando as soluções de qualidade inferior, que provavelmente terão menor preço, mas que não atendam às necessidades e expectativas. Em contrapartida, maiores questionamentos e pedidos de impugnação devem surgir oriundos desses fornecedores menos qualificados que deverão cuidadosamente ser analisados, com base nos princípios básicos da Administração Pública. Especial atenção aos detalhes da especificação (Termo de Referência/ Projeto Básico) e a presença assertiva de um assistente técnico capacitado junto ao pregoeiro, minimiza insucessos no processo.

Na fase de Seleção do Fornecedor, foi essencial a nomeação em Boletim Interno de assistente técnico com experiência, dedicado e com contato direto junto ao pregoeiro ou comissão de seleção. Sempre que possível, processos licitatórios centralizados, por especialidade, e em áreas de abrangência nacional também contribuem para melhoria do processo de seleção do fornecedor. Neste sentido, as principais vantagens são: itens do processo pertencentes a mesma área de TIC, facilitando o gerenciamento do certame e participação das empresas; melhor condução do certame, em relação ao apoio técnico especializado por órgão competente e maior expertise na área; padronização da solução, facilitando, também, o custeio; e participação de empresas com maior capacidade de entrega do produto ou serviço, além de maior *expertise*.

Na fase da Gestão do Contrato, foi primordial a nomeação do Fiscal do Contrato em Boletim Interno em conjunto com orientações da Seção de Licitações e Contratos sobre os procedimentos relacionados à fiscalização. O Fiscal de Contrato deve ser, de preferência, técnico, com experiência na área da solução contratada. O Fiscal pode solicitar a nomeação de um assistente da administração para auxiliá-lo na conformidade documental. Alguns artefatos (documentos), sugeridos, que foram juntados ao Termo de Encerramento:

- *Checklist*, baseado no Termo de Referência/Projeto Básico validando todos os itens a serem entregues;
- Cobertura fotográfica, para o relatório de entrega que deverá ser juntada ao Termo de Encerramento; e
- Relatório de testes, realizados após entrega da solução para comprovar a qualidade e/ou capacidade prevista em contrato.

Dessa forma, o GIFRJ realizou, conforme apresentado no quadro 4, a aquisição dos seguintes materiais de TIC, em apoio à Intervenção Federal, que permanecem como significativo legado para os OSP/RJ.

Quadro 4 – Aquisições do GIFRJ na área de TIC

Descrição detalhada do objeto	Destinatário	Quantidade adquirida	Valor Total (R$)	Modalidade
Equipamento computacional Oracle Exadata Modelo Quarter, com suporte por 60 meses, incluso instalação e configuração, contendo 96 cores de processamento instaladas para Banco de dados Oracle e Options, 1536 GB de RAM e 106,9 TB de disco utilizável.	PCERJ	1	7.526.250,01	PE
Equipamento computacional Oracle Exadata Modelo Oitavo, com suporte por 60 meses, incluso instalação e configuração, contendo 48 cores de processamento instaladas para Banco de dados Oracle e Options, 768 GB de RAM e 53 TB de disco utilizável.	PCERJ	1	5.175.000,01	PE
Equipamento computacional Oracle Private Cloud, com suporte por 60 meses, incluso instalação e configuração, 4x Compute Nodes (192 cores), Block Sotorages (90 TB) e Object Sotarege (125 TB) conectados via Infiniband.	PCERJ	1	5.342.400,01	PE
Equipamento computacional Oracle Private Cloud, com suporte por 60 meses, incluso instalação e configuração, 2x Compute Nodes (96 cores), Block Sotorages (90 TB) e Object Sotarege (125 TB) conectados via Infiniband.	PCERJ	1	4.426.305,53	PE

Continua

Continuação

Descrição detalhada do objeto	Destinatário	Quantidade adquirida	Valor Total (R$)	Modalidade
Serviço de migração de banco de dados existentes para nova plataforma Exadata.	PCREJ	1400	488.600,00	PE
Serviço de migração de aplicações existentes para nova plataforma Oracle Private Cloud.	PCERJ	800	311.200,00	PE
Serviço de apoio à criação de rotinas de contingência, contemplando replicação de banco de dados e aplicações de equipamentos Exadata e Oracle Private Cloud do Site Principal para equipamentos Exadata e Oracle Private Cloud do Site Secundário.	PCERJ	1200	474.000,00	PE
Workshop para capacitação quanto às funcionalidades e administração do Exadata e Oracle Private Cloud.	PCERJ	1	55.000,00	PE
Terminais Transceptores fixos no protocolo TETRA (Terrestrial Trunked Radio), na frequência de 380 – 430 MHz, Digital.	SEAP	10	89.880,00	PE
Sistema de Programação e Gerência Terminais do sistema de radiocomunicação TETRA.	SEAP	1	82.680,00	PE
Hardware de interligação entre Terminal e Sistema de programação e gerência do sistema de radiocomunicação TETRA.	SEAP	2	45.880,00	PE
Terminais Transceptores portáteis no protocolo TETRA (Terrestrial Trunked Radio), na frequência de 380-430 MHz, Digital.	SEAP	1000	3.201.000,00	PE

Continua

Continuação

Descrição detalhada do objeto	Destinatário	Quantidade adquirida	Valor Total (R$)	Modalidade
Sistema de Programação e Gerência de novos Terminais do sistema de radiocomunicação TETRA.	SEAP	1	64.000,00	PE
Hardware de interligação entre Terminal e Sistema de programação e gerência do novo sistema de radiocomunicação TETRA.	SEAP	3	45.000,00	PE
Treinamento em sistema de programação e Gerência de Terminais.	SEAP	4	46.560,00	PE
Treinamento em sistema de programação e Gerência de Terminais.	SEAP	4	40.000,00	PE
Simulador Virtual de tiro (180 graus).	PMERJ	1	1.550.000,00	PE
Microcomputador, memória RAM 5 a 8 GB, núcleos por processador até 4, armazenamento hdd 1 TB, armazenamento ssd, sem disco ssd, monitor 21 a 29 pol, componentes adicionais com teclado e mouse, sistema operacional proprietários, garantia on site 36 meses.	SESEG	9468	40.664.775,96	PE
Notebook, tela até 14 pol, interatividade da tela sem interatividade, memória RAM 5 a 8 gb, núcleos por processador até 4 armazenamento hdd 1 TB, armazenamento ssd sem disco ssd, bateria até 4 células, alimentação bivolt., sistema operacional proprietário, garantia on site 36 meses.	SESEG	1016	5.454.304,56	PE

Continua

Continuação

Descrição detalhada do objeto	Destinatário	Quantidade adquirida	Valor Total (R$)	Modalidade
Contratação de empresa especializada na execução de serviço de instalação de sistema e vídeo monitoramento (CFTV IP) nas instalações prediais de 54 unidades prisionais e hospitalares da SEAP.	SEAP	1	10.119.064,04	DISP
Equipamentos de informática para a instalação de sistema de vídeo monitoramento nas instalações prediais de 54 unidades prisionais e hospitalares da SEAP.	SEAP	1	17.530.055,00	DISP
Switch, quantidade portas 48 un, velocidade porta 10/100 mbps, características adicionais padrão iee, com 2 portas 10/100/1000 gerenciável.	SEAP	3	45.328,20	PE
Microcomputador, memória ram 5 a 8 GB, núcleos por processador até 4, armazenamento hdd 2 TB, armazenamento ssd sem disco ssd, monitor 21 a 29 pol,componentes adicionais com teclado e mouse, sistema operacional proprietário, garantia on site 36 meses.	SEAP	195	901.836,00	PE
Microcomputador, memória ram 5 a 8 GB, núcleos por processador até 4, armazenamento hdd 2 TB, armazenamento ssd sem disco ssd, monitor 21 a 29 pol, componentes adicionais com teclado e mouse, sistema operacional proprietário, garantia on site 36 meses.	SEAP	1105	4.579.120,00	PE
	TOTAL:	**108.258.239,32**		

Legenda:

- PE: Pregão Eletrônico
- DISP: Dispensa de Licitação

(Fonte: GIF/RJ, 2018)

Observa-se que grande parte dos processos utilizou-se do sistema de Pregão Eletrônico, buscando ao máximo eficiência, agilidade, economicidade e desburocratização dos procedimentos licitatórios, dando celeridade aos processos. Dessa forma, houve um favorecimento da concorrência de preços em favor da gestão pública, sem contar na maior transparência durante a realização dos certames. A Dispensa de Licitação realizada foi em função da importância da continuidade dos serviços no sistema penitenciário de monitoramento e controle de acesso. Em relação às aquisições, elas procuraram atender, com qualidade e eficiência, seguindo todos os princípios básicos da administração pública, a todos os órgãos da Secretaria de Segurança Pública. Assim, considerando os investimentos de um pouco mais de 1 bilhão de materiais e serviços adquiridos, cerca de 11,5 % do total foi na área de TIC, demostrando a importância desse peculiar segmento de apoio para a atividade fim de segurança pública e defesa do cidadão.

4 CONCLUSÃO

Este trabalho teve como objetivo principal apresentar a metodologia e a relevância do emprego de governança de Tecnologia da Informação adotado no nível estratégico do Gabinete de Intervenção Federal do Rio de Janeiro (GIFRJ). Foi dado maior enfoque para o apoio às operações realizadas e para orientação aos órgãos de TIC da SSP. Foram apresentadas as principais metodologias de Governança de TI, destacando as que estão sendo adotadas no Centro Integrado de Telemática do Exército (CITEx) e suas OMDS (os Centros de Telemática - CT/CTA), que compõem o Sistema de Telemática do Exército (SisTEx).

Neste contexto, destacam-se a disseminação dos dois modelos empregados no Departamento de Ciência e Tecnologia do Exército (DCT) na área da Secretaria de Segurança Pública (SSP) do Estado do Rio de Janeiro: COBIT, em um nível estratégico, no ambiente do GIFRJ, e ITIL, como modelo de governança para as áreas operacionais das Secretarias SESEG, SEAP e SEDEC, principalmente, para a PMERJ, PCERJ e CBERJ. Esses dois modelos são complementares e podem ser empregados em conjunto como boas práticas de Governança de TI. O COBIT, por sua origem focada em um comitê, que reúne algumas empresas americanas, descreve e foca em macroprocessos das diversas áreas de conhecimento em um nível mais estratégico; enquanto, o ITIL, desenvolvido por uma agência governamental britânica, com objetivos inicias de governança pública, é uma biblioteca de boas práticas que detalha mais como fazer, isto é, como implementar procedimentos operacionais.

A decisão intempestiva de Intervenção Federal no Estado do Rio de Janeiro e o tempo pré-definido e reduzido da Intervenção, para as soluções de TIC implicaram em ausência de tempo para um planejamento prévio. A clara falta de governança e gestão de TIC na Secretaria de Segurança Pública identificadas logo após a intervenção, foram evidenciadas e prontamente tratadas pelos gestores de TIC do GIFRJ. Neste sentido, foi fundamental identificar um método de gestão e governança a ser empregado. Desse modo, puderam ser mapeadas as reais necessidades e elaborados os processos licitatórios, conforme as recomendações do Governo Federal através das normas e orientações pertinentes, IN04 e IN05, do MPOG, para as contratações de soluções de TIC necessárias.

Para que pudesse implementar as práticas apresentadas anteriormente, várias mudanças tiveram que ser adotadas, desde o relacionamento dos Órgãos com os principais clientes, como a normatização de procedimentos para tratar com fornecedores. Entretanto, as mudanças mais relevantes residem na reestruturação interna: na nova forma de identificar o problema, no mapeamento dos processos e projetos, na elaboração do catálogo de serviços, abandonando a visão de produto para trabalhar com o fornecimento de serviços ao cliente.

Por fim, pode-se concluir que todas essas novas abordagens conduziram a uma significativa mudança de comportamento e restruturação organizacional da SSP/RJ, para uma melhor ação na área de planejamento, direção e controle. Como resultado, o GIFRJ não só conseguiu empregar em TIC cerca de 11,5% dos recursos recebidos, mas alcançou estabelecer novas práticas para a aquisição de bens e serviços, maximizando a utilização dos recursos com qualidade oferecendo um sólido legado para os órgãos de SSP, além de orientações de governança de TIC que, se seguidas, conduzirão a um período de transformação de gestão de seus ativos, pessoais e materiais.

REFERÊNCIAS

ALVES-MAZZOTTI, A. J.; GEWANDSZNAJDER, F. **O método nas ciências naturais e sociais: pesquisa quantitativa e qualitativa.** São Paulo: Pioneira Thomsom Learning, 2001.

BRASIL. Exército. Conselho Superior de Tecnologia da Informação. **Plano Estratégico de Tecnologia da Informação.** Brasília, DF, 2003.

_____._____. Escola de Comando e Estado-Maior do Exército. **Manual escolar trabalhos acadêmicos na ECEME.** Rio de janeiro, RJ, 2004.

_____._____. Estado-Maior. **IP 20-10: Liderança militar.** 1. ed. Brasília, DF, 1991.

_____. Gabinete de Intervenção Federal do Rio de Janeiro. **Plano Estratégico da Intervenção Federal na Área da Segurança Pública do Estado do Rio de Janeiro.** Rio de Janeiro, RJ, 2018.

_____._____. **Plano Diretor de Tecnologia da Informação da Intervenção Federal na Área da Segurança Pública do Estado do Rio de Janeiro.** Rio de Janeiro, RJ, 2018.

_____._____. **Portaria Normativa nº 22/Gabinete da Intervenção Federal (GIF),** de 11 de outubro de 2018.

_____. Governo Federal. **Decreto Federal nº 9.288**, de 16 de fevereiro de 2018.

_____. Ministério do Planejamento, Orçamento e Gestão. Sistema de Administração de Recursos de Tecnologia da Informação (SISP). **Guia de Elaboração de PDTI do SISP.** Brasília, DF, 2012. Disponível em: <http://www.sisp.gov.br>. Acessado em: 20 junho 2019.

_____._____._____. **Guia Prático para Contratação de Solução de Tecnologia da Informação v1.1.** Brasília, DF, 2011.

_____._____. Secretaria de Logística e Tecnologia da Informação. **Guia Prático para Contratação de Solução de Tecnologia da Informação v1.1.** Brasília, DF, 2011.

_____._____._____. **Metodologia de Gerenciamento de Projetos do SISP / Ministério do Planejamento, Orçamento e Gestão, Secretaria de Logística e Tecnologia da Informação.** Brasília, DF, 2011.

_____._____._____. **Metodologia de Gerenciamento de Portfólio de Projetos do SISP / Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação.** Brasília, DF, 2013.

DRUCKER, P. F. **Como Reagir às Mudanças.** Revista HSM Management L, abril/maio 1997.

FAGUNDES, E. M. **Artigo Um kit de ferramentas para a excelência de TI** (atualizado em 2012). Disponível em: < http://efagundes.com/artigos/cobit/>. Acesso em: 17 maio 2019.

_____. **Transparências COBIT – Um framework para a eficiência das organizações de Tecnologia da Informação e Telecomunicações** (atualizado em 2012). Disponível em:<http://efagundes.com/arquivos/Cobit_EduardoFagundes.pdf Acesso em: 17 maio 2019.

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

HOLM, M. L.; KÜHN, M. P.; VIBORG, K. A. **IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S. Proceedings of the 39th Hawaii International Conference on Systems Sciences - 2006.** IEEE. Koloa, Kauai. Janeiro, 2006, p. 11.

IBGC. **Governança Corporativa.** Disponível em: <http://www.ibgc.org.br>. Acesso em 30 maio 2019.

ISACA. Informations System Audit and Control Association. **COBIT, versão 4.1, 2007.** Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf>. Acesso em: 20 junho 2019.

_____._____. **COBIT, versão 5, 2012**. Disponível em: < http://www.isaca.org/cobit/pages/cobit-5-portuguese.aspx>. Acesso em 20 junho 2019.

_____._____. **ITIL, versão 3, 2011**. Disponível em: <http://www.isaca.org/gro Ups/professional-english/itil/groupdocuments/edition_key_facts_for_practitioners_fin al.pdf>. Acesso em: 20 junho 2019.

OLIVEIRA, D. de P. R de. **Estratégia empresarial e Vantagens Competitivas: como Estabelecer, Implementar e Avaliar.** 3 ed. São Paulo: Atlas, 2001.

SODRÉ, M. G.; SOUZA, S. M. de. **Uma Análise Comparativa de Metodologias para Governança de Tecnologia da Informação – ITIL e COBIT.** 2007, 157 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Departamento de Informática e Estatística da Universidade Federal de Florianópolis, 2007.

SPOHR DE MEDEIROS, E. M.; SAUVÉ, J. P. **Avaliação do Impacto de Tecnologias da Informação Emergentes nas Empresas.** Rio de Janeiro: Qualitymark. 2003.

WEIL, P.; ROSS, J. W. **Governança de TI: Tecnologia da Informação.** São Paulo: M Books, 2006.

ZORELLO, G. **Metodologias COBIT e ITIL e as perspectivas de Alinhamento Estratégico de TI.** XII Simpósio de Engenharia de Produção (SIMPEP). Bauru, 2005.

ANEXO A – PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PDTIC)