Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Ciência da Computação

SERGIO SOARES DA SILVA

Governança de TIC na Administração Pública aplicada aos serviços operacionalizados por prestadores terceirizados

Brasília-DF
2019

Universidade Federal de Minas Gerais

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Especialização em Informática - Área de Concentração: Gestão de Tecnologia da Informação

Governança de TIC na Administração Pública aplicada aos serviços operacionalizados por prestadores terceirizados

por

Sergio Soares da Silva

Monografia de final de curso

Prof. Dr. José Nagib Cotrim Árabe
Orientador

Brasília-DF

2019

SERGIO SOARES DA SILVA

Governança de TIC na Administração Pública aplicada aos serviços operacionalizados por prestadores terceirizados

Monografia apresentada ao Curso de Especialização em Informática do Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como requisito para a obtenção do grau de Especialista em Informática.

Área de Concentração: Gestão de Tecnologia da Informação

Orientador: Prof. Dr. José Nagib Cotrim Árabe

Brasília-DF

2019

Silva, Sergio Soares da

S586g Governança de TIC na Administração Pública aplicada aos serviços operacionalizados por prestadores terceirizados/ Sergio Soares da Silva. – 2019.
93 f.

Monografia (especialização em informática) – Universidade Federal de Minas Gerais. Departamento de Ciência da Computação.

Orientador: Prof. Dr. José Nagib Cotrim Árabe.

1. Informática . 2.Governança de TIC –3. Governança de TIC na Administração Pública aplicada aos serviços operacionalizados por prestadores terceirizados. 4.Terceirização I. Orientador. II. Título.

CDU 519.6*

UNIVERSIDADE FEDERAL DE MINAS GERAIS

INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
ESPECIALIZAÇÃO EM INFORMÁTICA: ÁREA DE CONCENTRAÇÃO
GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

Governança de TIC na Administração Pública aplicada aos serviços operacionalizados por prestadores terceirizados

SÉRGIO SOARES DA SILVA

Monografia apresentada aos Senhores:

Prof. José Nagib Cotrim Árabe
Orientador
DCC - ICEx - UFMG

Prof. José Marcos Silva Nogueira
DCC - ICEx - UFMG

Belo Horizonte, 15 de março de 2019

Dedico este trabalho àqueles que formam minha base como pessoa, com os quais sempre pude contar e que nunca me faltaram nos momentos de tormenta, minha amada família.

AGRADECIMENTOS

Acima de todos a Deus, pela saúde, pela força de espírito para enfrentar os diversos desafios e pedras que surgiram no meu caminho.

À minha família, meus pais, meu irmão e especialmente à minha esposa, Cinthya da Silva, aos meus filhos, Mateus, Guilherme e Rafael, pela paciência, pelo companheirismo e pelo amor incondicional a mim desprendido.

RESUMO

Esta monografia tem como objetivo analisar leis, decretos, instruções normativas e boas práticas de gestão e governança de tecnologia da informação para verificar quais os principais pontos de atenção devem ser observados nos serviços operacionalizados por profissionais terceirizados. Para tanto, elencou-se os principais normativos governamentais que tratam do tema gestão e governança de TIC e tendo como referência as práticas de gestão e governança mais difundidas no mercado são verificadas quais orientações ou modelos mínimos de gestão e governança devem ser implementados pelos gestores de TIC dos órgãos da Administração Pública para garantir a confiabilidade, integridade e disponibilidade dos dados, informações e serviços de TIC que são mantidos por profissionais terceirizados. Verificou-se possíveis sanções nas esferas administrativa e criminal que podem ser aplicadas aos gestores da área de TIC e aos profissionais terceirizados em caso de falhas que coloquem em risco os dados e informações públicas. Também, ao fim, é proposto um modelo para auxiliar no processo de levantamento e normatização dos recursos e serviços de TIC.

Palavras-chave: Governança de TI; Gestão de TI; Terceirização; IN 04; Transformação Digital; Serviços Públicos; Licitação Pública; Administração Pública Federal.

ABSTRACT

This monograph aims to analyze laws, decrees, normative instructions and good practices of information technology management and governance to verify what the main points of attention should be observed in the services operated by outsourced professionals. The main governmental regulations that deal with the topic of ICT management and governance are mentioned. Based on the most widespread management and governance practices in the market, it is verified which minimum guidelines and models of management and governance should be implemented by managers. ICT of Public Administration bodies to ensure the reliability, integrity and availability of ICT data, information and services that are maintained by outsourced professionals. Possible penalties have been found in the administrative and criminal spheres that may be applied to ICT managers and outsourced professionals in case of failures that put public data and information at risk. Also, at the end, a model is proposed to assist in the process of surveying and standardizing ICT resources and services.

Keywords: IT Governance; IT management; Outsourcing; IN 04; Digital Transformation; Public services; Public Bidding; Federal Public Administration.

Lista de Figuras

Lista de Tabelas

LISTA DE SIGLAS

PNAD	Pesquisa Nacional por Amostra de Domicílios Contínua
EGD	Estratégia de Governança Digital
TIC	Tecnologia de Informação e Comunicações
ATI	Analista em Tecnologia da Informação
BPMN	Business Process Model and Notation
COBIT	Control Objectives for Information and related Technology
ITIL	IT Infrastructure Library
PMBOK	Project Management Body of Knowledge
TCU	Tribunal de Contas da União
ISO	International Organization for Standardization
ABNT	Associação Brasileira de Normas Técnicas
AMN	Associação Mercosul de Normalização
IEC	International Electrotechnical Commission
iGovTI	Índice de governança de TI

Sumário

1. INTRODUÇÃO

As transformações na sociedade promovidas pela crescente massificação dos recursos e serviços de Tecnologia da Informação e Comunicação não poderiam passar despercebidas pelo governo e suas instituições. Expandir o acesso à informação de governo e melhorar os serviços públicos virou palavra de ordem em uma sociedade mais informada e exigente onde um cidadão, em média, possui mais de um meio de conexão ou acesso à internet.

A Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD), divulgada pelo IBGE em 2018, mostra que no ano de 2016 64,7% das pessoas de10 anos ou mais de idade utilizaram a Internet. Esse dado evidencia o potencial alcance dos serviços públicos oferecidos em plataformas digitais sem falar em alguns benefícios evidentes como transparência, padronização, desburocratização e economia na prestação dos serviços.

Buscando alcançar os benefícios proporcionados pelas plataformas tecnológicas atuais, o Governo Federal lançou o programa Estratégia de Governança Digital (EGD), que define desafios, oportunidades, objetivos, iniciativas, indicadores e metas para implementar a Política de Governança Digital, instituído pelo Decreto Nº 8.638, de 15 de janeiro de 2016.

Diante de tantos desafios para alcançar a transformação digital de governo, algumas questões são naturalmente colocadas: os gestores e órgãos que devem implementar essa transformação digital estão preparados? Os gestores e órgãos possuem mínimos instrumentos de gestão e controle para garantir a

confidencialidade, a integridade e a disponibilidade dos serviços, dados e informações mantidas em ambiente digital?

Com esses questionamentos em foco, outra sensível variável deve ser considerada: a massiva terceirização dos serviços de TIC. O Decreto Nº 2.271 de 7 de julho de 1997, em seu Art. 1º dispôs que atividades acessórias, instrumentais ou complementares poderiam ser objeto de execução indireta. Ou seja, poderiam ser terceirizadas. No mesmo decreto foi listado um rol de atividades que poderiam ser terceirizadas, conforme segue:

> *"§ 1º As atividades de conservação, limpeza, segurança, vigilância, transportes, informática, copeiragem, recepção, reprografia, telecomunicações e manutenção de prédios, equipamentos e instalações serão, de preferência, objeto de execução indireta."*

Como pode ser observado, o referido parágrafo incluiu nas atividades passíveis de terceirização o termo *informática.* Assim, a Administração Pública Federal direta e indireta poderia terceirizar as atividades de informática. O problema do Decreto nº 2.271 é que ele não explicitava que nas referidas atividades acessórias há atividades de gestão e controle que não podem ser terceirizadas.

O Decreto nº 2.271 foi revogado pelo Decreto Nº 9.507, de 21 de setembro de 2018 e esse novo decreto corrige o equívoco ao especificar não só as atividades que podem ser terceirizadas, mas também especifica as que não podem ser terceirizadas.

Art. 3º Não serão objeto de execução indireta na administração pública federal direta, autárquica e fundacional, os serviços:

I - que envolvam a tomada de decisão ou posicionamento institucional nas áreas de planejamento, coordenação, supervisão e controle;

II - que sejam considerados estratégicos para o órgão ou a entidade, cuja terceirização possa colocar em risco o controle de processos e de conhecimentos e tecnologias;

III - que estejam relacionados ao poder de polícia, de regulação, de outorga de serviços públicos e de aplicação de sanção; e

IV - que sejam inerentes às categorias funcionais abrangidas pelo plano de cargos do órgão ou da entidade, exceto disposição legal em contrário ou quando se tratar de cargo extinto, total ou parcialmente, no âmbito do quadro geral de pessoal.

§ 1º Os serviços auxiliares, instrumentais ou acessórios de que tratam os incisos do caput poderão ser executados de forma indireta, vedada a transferência de

> *responsabilidade para a realização de atos administrativos ou a tomada de decisão para o contratado.*
>
> *§ 2º Os serviços auxiliares, instrumentais ou acessórios de fiscalização e consentimento relacionados ao exercício do poder de polícia não serão objeto de execução indireta.*

O Decreto Nº 9.507 foi explícito ao vedar a terceirização de atividades de gestão e governança. Ações ou atividades de gestão devem ser definidas e executadas por profissionais com vínculo direto com a Administração Pública.

O Governo Federal, segundo Cruz, Andrade e Figueiredo (2012, p.1), em 2010 gastou com TI aproximadamente R$ 12,5 bilhões e para o mesmo ano era previsto um orçamento total da União de R$ 1,8 trilhão, sendo provável que a execução da maior parte dependa, direta ou indiretamente de TIC. Esse cenário evidencia que a TI tem sido uma preocupação e necessidade para os programas de governo. Ao mesmo tempo, esse volume de recursos fez com que a TI se tornasse alvo constante de apurações e auditorias de diversos órgãos de controle do governo, dentre os quais se destaca o Tribunal de Contas da União (TCU).

Partindo da premissa de que a operacionalização dos recursos e serviços de TIC é executada por profissionais contratados por empresas terceirizadas, as seguintes questões são levantadas: como os gestores de TIC de governo mantêm a gestão e governança dos serviços de TIC de forma a garantir a confidencialidade, a integridade e a disponibilidade dos serviços, dados e informações mantidas em ambiente digital? Os prestadores terceirizados têm ciência da criticidade e dos riscos

inerente na operacionalização dos serviços? Os prestadores terceirizados têm ciência de que poderão ser responsabilizados por danos causados na operacionalização dos serviços? Eles podem ser responsabilizados?

Este trabalho lança um olhar mais profundo sobre as questões levantadas. Buscando não só reponde-las, mas também fazendo um diagnóstico aproximado da realidade de TIC, além de tentar indicar ações ou medidas para mitigar os riscos identificados.

Na seção 2 será explanado o que é governança e gestão de TIC. A seção 3 trata do volume de contratações de TIC com causas e consequência para a Administração Pública. Na seção 4 é retomado o tema gestão e governança sob o viés do que deve ser gestão e controle de TIC. A seção 5 verifica os principais marcos regulatórios sobre o tema de gestão e governança de TIC, enquanto que a seção 6 analisa os principais modelos de gestão e governança de mercado com COBIT e ITIL sob o aspecto de gestão sob os terceirizados. À luz do Código Penal Brasileiro a seção 7 explana sobre as possíveis penas ou sanções que podem ser aplicadas aos gestores ou terceirizados. A seção 8 descreve pontos e características que podem atrapalha na implementação um modelo de gestão e governança de TIC. Finalmente, a seção 9 propõe um modelo em macroprocesso para facilitar ou orientar os passos iniciais na implementação de modelo de gestão sobre os recursos e serviços de TIC.

2. GOVERNANÇA E GESTÃO DE TIC

Antes de discorrer sobre o tema da monografia é muito importante definir e estabelecer o que é governança e gestão de TIC. Qual é o objetivo e quais são os principais conceitos sobre gestão e governança de TIC.

A governança de TIC orienta o melhor uso da estrutura, serviços e orçamento de TIC de forma controlada para suportar os processos de negócios e auxiliar o alcance dos objetivos estratégicos de uma organização.

A governança de TIC é implementada através de processos, ferramenta e métodos que visam manter as ações de TIC alinhadas aos objetivos estratégicos da organização.

O *Control Objectives for Information and related Technology* (COBIT) na versão 5 (2012, p.16), define governança:

> *"A governança garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos."*

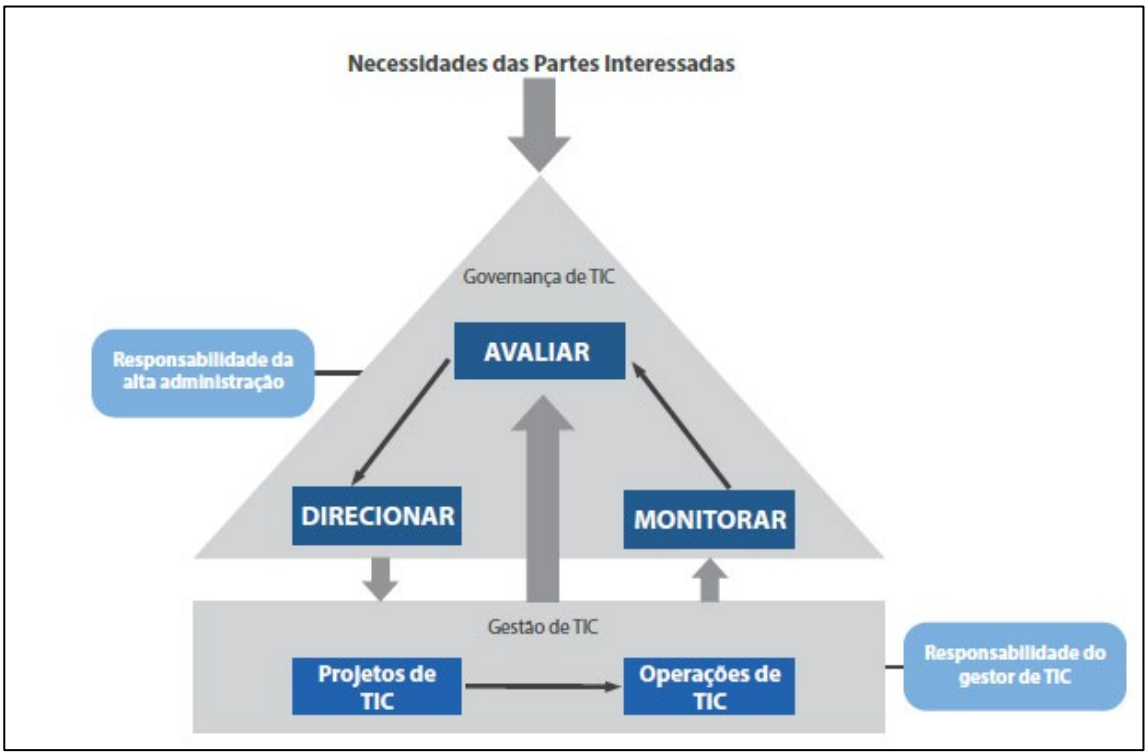
O Acórdão Plenário 1.603/2008 do TCU-Plenário, define:

> *"O objetivo da governança de TI é assegurar que as ações de TI estejam alinhadas com o negócio da organização, agregando-lhe valor. O desempenho da área de TI deve ser medido, os recursos propriamente alocados e os riscos inerentes, mitigados. Assim, é possível gerenciar e controlar as iniciativas de TI nas organizações para garantir o retorno de investimentos e a adoção de melhorias nos processos organizacionais."*

Já a gestão de TIC é responsável pela execução das ações de TIC conforme direcionamento definido pela governança. Segundo a Portaria Nº 19, de 29 de maio de 2017 do Ministério do Planejamento, Desenvolvimento e Gestão, a gestão de TIC é a atividade responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TIC em consonância com a direção definida pela função de governança a fim de atingir os objetivos institucionais.

Em suma, enquanto a governança de TIC tem por atribuição alinhar as atividades e operações de TIC aos objetivos estratégicos, a gestão de TIC tem a atribuição de executar e operar a TIC conforme as definições da governança (figura 1).

Figura 1: Relação entre Governança e Gestão



Fonte: http://www.sisp.gov.br/govtic/wiki/download/file/Guia_de_Governan%E7a_de_TIC_do_SISP_v_2.0

2.1. Governança e Gestão de TIC na Administração Pública

A governança de TIC aplicada à Administração Pública está sendo alvo de exigência dos vários órgãos de controle.

Palmeira (2008) em seu voto no Acórdão Plenário 1.603/2008 recomenda ao Ministério do Planejamento que promova ações no sentido de orientar todos os órgãos integrantes da estrutura do Executivo Federal de forma que sejam adotadas as melhores práticas de governança e de gestão de segurança da informação.

Em 2014, a Nota Técnica 7/2014 - Sefti/TCU informa que no segundo levantamento, realizado em 2010 (Acórdão 2.308/2010-TCU-Plenário), verificou-se que mais da metade das instituições pesquisadas se encontravam em estágio inicial de governança de TI, pouco mais de 1/3 (um terço) apresentavam nível intermediário, e apenas 5% (cinco por cento) dessas instituições estavam em nível

aprimorado. Como consequência da baixa maturidade de governança a nota técnica destaca as seguintes consequências:

- priorização de investimentos em TI que não alinhados às necessidades do negócio;
- riscos de TI que não são adequadamente identificados e tratados;
- aquisições em desconformidade com a legislação aplicável, indisponibilidade de serviços públicos providos com uso de TI; e
- falhas de segurança da informação, entre outros.

O Ministério do Planejamento publicou em maio de 2017 a Portaria Nº 19 que dispõe sobre implantação de Governança de TIC nos órgãos pertencentes ao Sistema de Administração de Recursos de Tecnologia da Informação do Poder Executivo, conforme explicita seu Art. 1º.

"Art. 1º Os órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal deverão adotar medidas para implantar, desenvolver e aperfeiçoar a governança de Tecnologia da Informação e Comunicação - TIC conforme disciplinado nesta Portaria".

No levantamento do iGovTI de 2016 já é possível verificar melhora considerável no índice de governança, quando comparado com o levantamento de 2014. Dos 339 órgãos pesquisados apenas 14% (quatorze por cento) foi classificado com índice inicial, 37% (trinta e sete por cento) estão com índice básico, 37% (trinta e sete por cento) estão com índice intermediário e 11% (onze por cento) com índice aprimorado.

3. CONTRATAÇÕES DE TIC

O Estado ou a Administração Pública é obrigado a seguir uma série de princípios para a concepção dos serviços à sociedade, conforme explicita Constituição da República Federativa do Brasil de 1988, além de obediência aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência, Administração Pública direta e indireta de qualquer dos poderes da União, dos Estados, do Distrito Federal e dos Municípios, deverá também, obedecer ao ato licitatório nos processos de contratação de terceiros para execução de obras, serviços, compras e alienações. Do Art. 37 da Constituição da República temos:

> *"XXI - ressalvados os casos especificados na legislação, as obras, serviços, compras e alienações serão contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes, com cláusulas que estabeleçam obrigações de pagamento, mantidas as condições efetivas da proposta, nos termos da lei, o qual somente permitirá as exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações."*

O objetivo da licitação é atender o interesse público, buscar a proposta mais vantajosa em igualdade de condições para todos os interessados na

contratação com a Administração Pública, bem como os demais princípios resguardados pela Constituição.

Promulgada em 21 de junho de 1993, a lei de licitações e contratos, Lei 8666/93, estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações. Nessa seara estão incluídas também as aquisições de serviços e recursos de TIC. Ou seja, para Administração Pública contratar desde pen-drives até datacenters é necessário executar o processo instruído na Lei 8666/93.

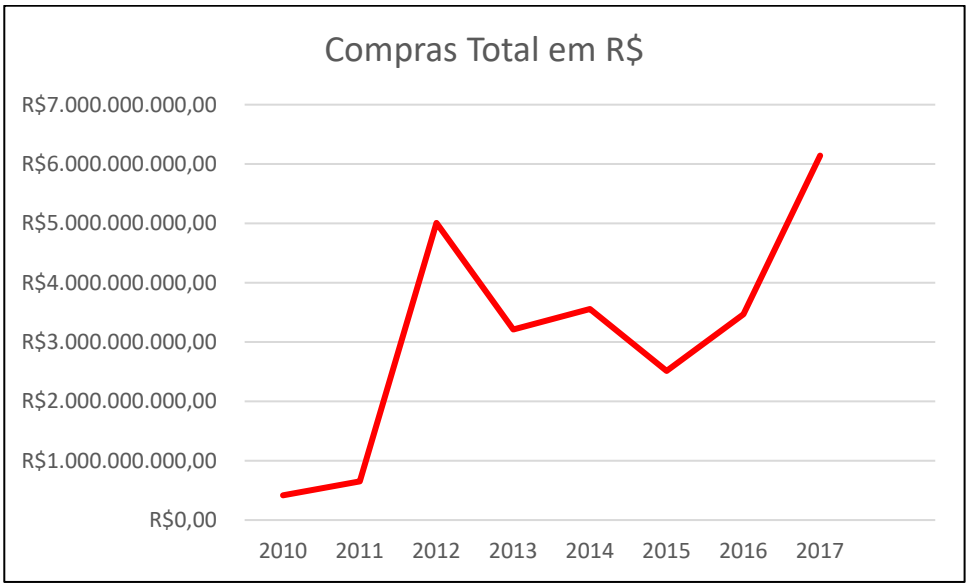
Entretanto, a Lei 8666/93 é genérica e não alcança as peculiaridades comuns nas contratações de serviços e recursos de TIC. A complementação ou especialização do processo de contratação por meio de leis ou instruções normativas específicas é necessária para a melhoria contínua do processo em destaque para alguns tipos de contratações onde a Lei 8666/93 não atende.

Atualmente, na esfera do Poder Executivo Federal, no que se refere a contratações de recursos e serviços de TIC o normativo de maior referência é a Instrução Normativa n° 4, de 11 de setembro de 2014 do Ministério do Planejamento, Desenvolvimento e Gestão. Popularmente conhecida como IN04, esta dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicações. Assim, além de cumprir as determinações e orientações da Lei 8666/93 e outras, para os Órgãos do Poder Executivo Federal devem executar o processo e determinações descritas na IN04, de 11 de setembro de 2014.

O volume de compras de TIC do Governo Federal é expressivo. Segundo o Painel de Gastos de TI da Controladoria-Geral da União, de 2010 a 2017 o volume total de compras foi de **R$ 24.966.346.700,39 (vinte e quatro bilhões, novecentos**

e sessenta e seis milhões, trezentos e quarenta e seis mil, setecentos reais e trinta e nove centavos). No gráfico da figura 2 é possível verificar a evolução das compras de recursos de TIC nos últimos oito anos.

Figura 2: Evolução das compras de TIC



Fonte: http: //paineis.cgu.gov.br/gastosti/index.htm

3.1. A Atuação dos Terceirizados no Serviço Público

De fato, o Governo Federal tem gasto muitos recursos com aquisições de serviços e produtos de TIC. Pode-se efetivamente concluir que a participação das empresas privadas na execução e entrega dos serviços públicos são fundamentais para a continuidade na prestação dos serviços em TIC.

Em uma pesquisa no Painel de Compras do Governo, especificamente para empresas que prestam serviços de TIC, no ano de 2017, foram assinados 125 (cento e vinte e cinco) contratos, totalizando R$ 733.105.975,70 (setecentos e trinta e três milhões, cento e cinco mil, novecentos e setenta e cinco reais e setenta centavos). Diante desses números podemos inferir que, bem provavelmente, um

prestador de serviço terceirizado está atuando diretamente nos recursos de TIC que suportam os serviços prestados à sociedade.

Quando o cidadão entra em um portal ou sistema informatizado do governo solicitando um serviço público, seus dados ou informações, durante todo o fluxo de negócio, passam por ferramentas ou soluções de TIC que são operacionalizadas e acessadas por profissionais de TIC terceirizados na grande maioria dos órgãos públicos.

Em um levantamento no Portal de Dados Abertos foi verificado que o Poder Executivo Federal possui aproximadamente 67 (sessenta e sete) cargos da área de TIC e nesses estavam ativos, em dezembro de 2017, cerca de 8.537 (oito mil, quintetos e trinta e sete) servidores de carreira. Distribuídos nos 26 (vinte e seis) Estados da Federação e no Distrito Federal, esses servidores estão alocados em 175 (cento e setenta e cinco) órgãos do Poder Executivo Federal. Se a distribuição desses servidores de TIC fosse igual entre os órgãos do Poder Executivo Federal teríamos a média aproximada de 49 (quarenta e nove) servidores por órgão. Acontece que na prática a distribuição não é uniforme e muitos dos órgãos do Executivo Federal não possui quadro específico de profissionais ou técnicos de TIC.

Esse cenário forçou numa excessiva terceirização dos serviços, incluindo em muitos casos até mesma a gestão do setor de TIC. As decisões técnicas eram dadas por gerentes ou gestores das empresas terceirizadas e, normalmente, havia servidores sem capacidade técnica que apenas formalizavam as decisões. Em 2008, após uma série de auditorias nos órgãos do Executivo, o TCU publicou o Acórdão Plenário 2.471/2008, que recomendou ao Ministério do Planejamento tomar medidas para prover os setores de TIC da Administração Pública Federal com um quadro

permanente de pessoal, de modo a garantir independência das empresas prestadoras de forma que a autoridade e controle fiquem com a Administração.

4. GESTÃO E CONTROLE DOS SERVIÇOS DE TIC

O Acórdão Plenário 2.471/2008 é explicito no item 9.4.5, conforme segue:

> *"9.4.5. adote as medidas necessárias para prover os setores de informática dos órgãos e entidades da Administração Pública Federal da estrutura organizacional e de quadro permanente de pessoal que sejam suficientes para realizar, de forma independente das empresas prestadoras de serviços, o planejamento, a definição, a coordenação, a supervisão e o controle das atividades de informática, com a finalidade de garantir a autoridade e o controle da Administração sobre o funcionamento daqueles setores. Deve ser avaliada a conveniência e a oportunidade da criação de carreira específica, semelhante ao ocorrido com as carreiras de Especialista em Meio Ambiente e a de Analista de Infra-Estrutura;"*

Portanto, de acordo com o TCU, a definição, a coordenação, a supervisão e o controle das atividades das áreas de TIC dos órgãos devem ser executados por servidores com vínculos diretos com a Administração Pública.

A Instrução Normativa n° 4, de 11 de setembro de 2014 do Ministério do Planejamento, Desenvolvimento e Gestão, em seu Art. 5º é categórica em vedar a contratação da gestão de TIC, conforme abaixo:

> *"II - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação. Parágrafo único. O apoio técnico aos processos de planejamento e avaliação da qualidade das Soluções de Tecnologia da Informação poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade."*

Entende-se que a gestão e o controle dos serviços devem sempre ser dos órgãos, porém a operação ou construção de algumas soluções podem ser terceirizadas e é isso que acontece em todos os órgãos da Administração Pública. Como garantir que os prestadores de serviço terceirizados estão executando e operando os serviços da maneira mais adequada e resguardando a confiabilidade, integridade, disponibilidade e segurança dos serviços e recursos de TIC à sociedade?

4.1. Direitos e deveres para o uso da Internet no Brasil

O governo brasileiro publicou em 23 de abril de 2014 a Lei nº 12.965, mais conhecida com Marco Civil da Internet. Direitos como inviolabilidade da intimidade e da vida privada, não fornecimento a terceiros de dados pessoais, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, exclusão definitiva dos dados pessoais e etc, devem ser garantidos individual e socialmente. A Lei dispõe também sobre possíveis responsabilizações dos provedores de serviços.

No tocante a responsabilização sobre a obtenção e manutenção dos dados, o Marco Civil da Internet deixa claro que qualquer agente (governo, setor privado, pessoas físicas e jurídicas) pode ser chamado à responsabilidade por qualquer violação dos direitos descritos naquele instrumento. Neste sentido os gestores das áreas de TIC podem ser responsabilizados e responder por ações ou falhas nas operações dos serviços pelos terceirizados.

4.2. Princípios da Legalidade e Publicidade

A Administração Pública exerce a função de proteção do interesse público. Provendo no tocante à regulação dos interesses da sociedade como um todo e na perspectiva de tutela do interesse público, todos os atos da Administração Pública seguem pré-requisitos que se não observados podem resultar em nulidade do próprio ato com responsabilização do agente que o provocou. Esses critérios ou pré-requisitos, que a Administração Pública deve seguir para a regulação do interesse da sociedade, são conhecidos como **Princípios da Administração Pública**. A Constituição da República no seu Art. 37 é explícita ao determinar que a Administração Pública deverá obedecer a cinco princípios, conforme segue:

> *“Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência...”*

Dois desses princípios são especialmente relevantes à luz da gestão e governança de TIC: Legalidade e Publicidade.

O princípio da Legalidade diz que a Administração Pública só pode atuar quando e como a lei previamente determina. É um conteúdo restritivo onde a ação só é permitida quando prevista em lei. Segundo Alexandrino e Paulo (2017) não basta a inexistência de proibição legal; é necessária a existência de determinação ou a autorização da atuação administrativa na lei. Enquanto que, para o particular ou pessoa jurídica privada, é permitido fazer tudo que a lei não proíbe, para o agente público, além de não fazer o que a lei proíbe, só pode ser feito o que a lei permite ou determina.

O princípio da publicidade tem dois objetivos. O primeiro está ligado à eficácia do ato, de tal modo que seus efeitos só podem ser produzidos houver a publicação. O segundo objetivo é a necessidade de transparência dos atos e ações da Administração Pública. Segundo o art. 5 da Constituição:

> *“XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena*

de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;"

Mas qual a relação desses dois princípios com a as áreas de TIC especificamente? A primeira resposta e a mais óbvia é que as áreas de TIC dos órgãos, como parte integrante da Administração Pública, também deve observar esses princípios em seus atos ou ações. E a segunda é a premissa que se houver normativos e procedimentos, os profissionais terceirizados e agentes públicos não tem a referência de como atuar ou agir em cada possível circunstância.

Em suma, utilizando os princípios da Legalidade e Publicidade, é obrigação dos gestores de TIC e da alta administração dos órgãos que as políticas, normas e procedimentos dos serviços de TIC sejam instruídos e publicados de forma a dar legalidade e publicidade a todas as operações e processos da área de TIC.

Hipoteticamente, se um prestador terceirizado executar qualquer ato ou ação que coloque em risco os dados ou os serviços de governo o mesmo poderá alegar que não tinha orientações de como proceder e até a mesmo a pessoa jurídica poderá alegar ausência de procedimentos estabelecidos para se isentar de possíveis sanções contratuais. Manter no órgão conjunto de políticas, normas ou procedimentos formalizados e publicados ajudará na maturidade da governança e gestão dos recursos de TIC e na melhor prestação dos serviços à sociedade.

5. MARCO REGULATÓRIO

No ordenamento jurídico brasileiro há diversas leis, decretos, instruções normativas e guias que tratam do tema de governança e gestão de TIC. Esse arcabouço jurídico busca orientar os órgãos da Administração Pública na implementação de governança e gestão de TIC de forma a alinhar os recursos e ações de TIC para as necessidades estratégicas de cada pasta governamental. Abaixo estão elencadas algumas das principais regulações sobre o tema.

5.1. Marco Civil da Internet

Publicada em 23 de abril de 2014 a Lei Nº 12.965, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Apesar de não tratar especificamente do assunto governança e gestão de TIC, o Marco Civil da Internet elenca alguns direitos, responsabilidades e obrigações que devem ser consideradas pelos gestores de TIC e que indiretamente influenciam na governança e gestão de TIC e na gestão e execução contratual.

O Art. 3º, nos incisos II, III e VI determina que a proteção da privacidade e proteção dos dados pessoais são princípios do Decreto e estes devem ser observados pelo setor público na obtenção e manutenção dos dados, sob o risco de responsabilização dos agentes de acordo com suas atividades, nos termos da lei.

Cabe destacar que o decreto utiliza o termo: “AGENTES”. Não é feita distinção entre agente público ou privado, ou entre pessoa jurídica ou pessoa física. Todos estão sujeitos a serem responsabilizados, na medida de sua atribuição e

responsabilidade sob a obtenção, gestão e manutenção dos dados de cunho privado ou pessoal.

No Art.7° são descritos mais direitos e garantias de cunho individual e social, tais como inviolabilidade da intimidade e da vida privada, não fornecimento a terceiros de dados pessoais, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, exclusão definitiva dos dados pessoais e etc. O artigo trata também sobre possíveis responsabilizações dos provedores de serviços.

O Art.10 reforça a responsabilidade pela manutenção dos dados pessoais e de comunicação privada determinando que deva ser preservada a intimidade a honra e a imagem. Contudo, o parágrafo 3° diz:

> *"§ 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição."*

É permitido às autoridades administrativas, em outras palavras autoridades públicas, conforme competência legal, ter acesso a informações de formação ou qualificação, filiação e de endereço. Na prática, uma autoridade pública poderá requisitar informações sobre os domínios explicitados.

O Art. 12 explana sobre as possíveis sanções que podem ser aplicadas aos provedores em caso de descumprimento da Lei. As sanções vão de advertência à proibição do exercício de atividades.

O Marco Civil da Internet não traz inovações específicas sobre terceirização dos serviços de TIC na Administração Pública. Alguns tópicos, de maneira interpretativa, poderiam influenciar alguns tipos de contratações. Por exemplo, caso um órgão pretenda terceirizar serviços em nuvem, com infraestrutura totalmente privada, ele deverá obrigatoriamente consultar a Lei na definição dos termos contratuais entre entes públicos e privados.

5.2. Política de Governança Digital

O Decreto Nº 8.638 de 15, de janeiro de 2016 institui a Política de Governança Digital no âmbito dos órgãos e das entidades da Administração Pública Federal.

Este decreto não discorre sobre contratações e relação entre contratante e contratada. No que se refere a terceirização, não foi observado algo de destaque no decreto. Contudo o Art. 3º descreve alguns princípios que devem ser observados pela Administração Pública em seus atos contratuais firmados com o setor privado dentre eles: segurança e privacidade, participação e controle social, governo como plataforma e inovação. O gestor de TIC deve observar a aderência na concepção e construção dos modelos de governança e gestão.

5.3. Política de Dados Abertos

Instituído pelo Decreto Nº 8.777 de 11 de maio de 2016, este normativo trata da instituição de política nacional de dados abertos. O objetivo é disponibilizar dados governamentais livremente para todos (pessoas físicas ou pessoas jurídicas) utilizarem e redistribuir como desejarem, sem restrição de licenças, patentes ou mecanismos de controle. Ele estabelece as seguintes diretrizes:

“Art. 3º A Política de Dados Abertos do Poder Executivo federal será regida pelos seguintes princípios e diretrizes:

I - observância da publicidade das bases de dados como preceito geral e do sigilo como exceção;

II - garantia de acesso irrestrito às bases de dados, as quais devem ser legíveis por máquina e estar disponíveis em formato aberto;

III - descrição das bases de dados, com informação suficiente para a compreensão de eventuais ressalvas quanto à sua qualidade e integridade;

IV - permissão irrestrita de reuso das bases de dados publicadas em formato aberto;

V - completude e interoperabilidade das bases de dados, as quais devem ser disponibilizadas em sua forma primária, com o maior grau de granularidade possível, ou referenciar as bases primárias, quando disponibilizadas de forma agregada;

VI - atualização periódica, de forma a garantir a perenidade dos dados, a padronização de

estruturas de informação e o valor dos dados à sociedade e atender às necessidades de seus usuários; e

VII - designação clara de responsável pela publicação, atualização, evolução e manutenção de cada base de dado aberta, incluída a prestação de assistência quanto ao uso de dados."

Além de observar os princípios contidos no Art. 3º, os órgãos do Executivo Federal deverão manter um Plano de Dados Abertos no qual deverão constar inventário de dados, papéis e responsabilidade sobre a gestão dos respectivos órgãos.

É importante que dentro do órgão esteja claro quem são os responsáveis pelos dados mantidos. Quando pensamos em responsáveis, não devemos considerar apenas os gestores ou servidores da área de TI. O negócio é o real dono do dado ou informação e a área de TIC é o mantenedor (é quem armazena, mantém e disponibiliza), mas conhecer e determinar o valor de negócio do dado ou informação é responsabilidade das áreas finalísticas.

Aproveitando a determinação legal de se manter um Plano de Dados Abertos, seria interessante ampliar esse conceito nas instituições públicas de forma tal que, além do plano, fosse produzido e mantido um instrumento para gestão e operação dos dados mantidos em bancos de dados.

5.4. Contratação de Soluções de Tecnologia da Informação pelos Órgãos

A principal referência para contratação de soluções de TIC pela Administração Pública Federal é a Instrução Normativa N° 4, de 11 de setembro de 2014 do Ministério do Planejamento, Desenvolvimento e Gestão, comumente conhecida como IN04. Como instrumento obrigatório para a execução do processo de contratação, a IN04 estabelece um processo de planejamento, contratação e execução contratual.

O Art. 17 prevê que no planejamento da contratação devem ser descritos os critérios de requisitos da solução, como atribuição do integrante Técnico da Equipe de Planejamento da Contratação, conforme segue:

> *"II - ao Integrante Técnico especificar, quando aplicáveis, os seguintes requisitos tecnológicos:*
>
> *a) de arquitetura tecnológica, composta de hardware, software, padrões de interoperabilidade, linguagens de programação, interfaces, dentre outros;*
>
> *b) de projeto e de implementação, que estabelecem o processo de desenvolvimento de software, técnicas, métodos, forma de gestão, de documentação, dentre outros;*
>
> *c) de implantação, que definem o processo de disponibilização da solução em ambiente de produção, dentre outros;*

d) de garantia e manutenção, que definem a forma como será conduzida a manutenção e a comunicação entre as partes envolvidas;

e) de capacitação, que definem o ambiente tecnológico dos treinamentos a serem ministrados, os perfis dos instrutores, dentre outros;

f) de experiência profissional da equipe que projetará, implementará e implantará a Solução de Tecnologia da Informação, que definem a natureza da experiência profissional exigida e as respectivas formas de comprovação dessa experiência, dentre outros;

g) de formação da equipe que projetará, implementará e implantará a Solução de Tecnologia da Informação, que definem cursos acadêmicos e técnicos, formas de comprovação dessa formação, dentre outros;

h) de metodologia de trabalho;

i) de segurança da informação; e

j) demais requisitos aplicáveis."

Dentre várias determinações ao processo de contratação o art. 18 traz algumas preocupações, conforme segue:

> *“Art. 18. A definição das responsabilidades da contratante, da contratada e do órgão gerenciador do registro de preços, quando aplicável, deverá observar:*
>
> *II - a definição das obrigações da contratada contendo, pelo menos, a obrigação de:*
>
> *c) reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;”*

A IN04 determina que no planejamento da contratação sejam definidos modelos e padrões técnicos e determina a previsão de responsabilização de reparar os danos causados pela terceirizada, demonstrada ou não a intenção por parte do terceiro e também poderão ser responsabilizados os fiscais do contrato. Contudo a IN04 não estabelece quais modelos mais adequados de gestão sobre os serviços terceirizados. Fica a cargo de cada órgão estabelecer no processo de contratação qual o modelo de gestão para o contrato.

5.5. Implantação da Governança de Tecnologia da Informação e Comunicação nos Órgãos

O Ministério do Planejamento, Desenvolvimento e Gestão, por meio da Secretaria de Tecnologia da Informação, editou e publicou a Portaria Nº 19, de 29 de maio de 2017 que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.

A portaria determina aos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP que adotem medidas para implantar, desenvolver e aperfeiçoar a governança de TIC. Descreve e estabelece termos e princípios que devem ser observados nos processos de governança. Especifica atores e responsabilidades que devem ser envolvidos na governança, principalmente nos atos decisórios.

Em complemento a Portaria Nº 19 e com o objetivo de auxiliar os órgãos integrantes do SISP, a SETIC/MP publicou também o **Guia de Governança de TIC do SISP**. De caráter orientativo e não vinculante, o Guia organiza e propõe um modelo de implantação por meio de 10 (dez) práticas:

- Prática 01 - Envolvimento da alta administração com iniciativas de TIC;
- Prática 02 - Especificação dos direitos decisórios sobre TIC;
- Prática 03 - Comitê de TIC;
- Prática 04 - Riscos de TIC;
- Prática 05 - Portfólio de TIC;

- Prática 06 - Alinhamento Estratégico;
- Prática 07 - Sistema de comunicação e transparência;
- Prática 08 - Conformidade do ambiente de TIC;
- Prática 09 - Monitoramento do desempenho da TIC; e
- Prática 10 - Avaliação do uso da TIC.

A Prática 08 – Conformidade do ambiente de TIC - do Guia orienta pela análise da conformidade do ambiente de TIC, conforme segue:

> *"Esta prática está relacionada à análise contínua da conformidade do ambiente de TIC, frente aos marcos regulatórios que regem a administração pública, tais como leis, decretos, instruções normativas, acórdãos, etc."*

Para a implementação da Prática 08, o Guia orienta que há alguns condicionantes como:

- Pessoal com competência para análise de conformidade do ambiente de TIC;
- Existência de estrutura organizacional - ou função equivalente - responsável pela auditoria interna no órgão;
- Existência de políticas e diretrizes organizacionais para a TIC;
- Existência de políticas e diretrizes organizacionais para a TIC; e
- Atuação dos órgãos de controle.

A condicionante “Existência de políticas e diretrizes organizacionais para a TIC” diz que as diretrizes e políticas do órgão para a TIC devem ser consideradas, segue:

> *“Existência de políticas e diretrizes organizacionais para a TIC: as políticas e diretrizes organizacionais para a TIC também devem ser levadas em consideração durante o processo de avaliação da conformidade da área de TIC, pois direcionam a sua atuação. Dessa maneira, a formalização de políticas e diretrizes dos órgãos para a área de TIC como, por exemplo, a Política de GovTIC do órgão, influencia, positivamente, a implementação da prática de governança de TIC.”*

Na Portaria Nº 19 e no Guia de Governança de TIC não existe determinação ou orientação, de maneira explícita e direta, sobre a necessidade de normatizar os processos e operação de TIC.

Enquanto a Portaria Nº 19 determina para os órgãos do SISP a obrigação institucionalizar um modelo de governança, define papeis e responsabilidades, descreve quais princípios e diretrizes o modelo de governança deve seguir; o Guia de Governança de TIC do SISP explana sobre um modelo de governança não obrigatório que pode ou não ser utilizado como referência para os órgãos. Ambas buscam criar um modelo de governança onde o foco maior é envolver a alta administração nas deliberações sobre as ações de TIC.

Seria interessante que nesses instrumentos houvesse uma determinação ou orientação sobre a importância de regular os processos e operações de TIC, espacialmente para os serviços operacionalizados por prestadores terceirizados.

5.6. A Segurança Institucional

O Gabinete de Segurança Institucional (GSI) é órgão da Presidência da República que tem como atribuição:

- Analisar e acompanhar questões com potencial de risco à estabilidade institucional;
- Prevenir a ocorrência e articular o gerenciamento de crises em caso de grave e iminente ameaça à estabilidade institucional;
- Coordenar as atividades de segurança da informação e das comunicações;

O GSI mantém uma série de Normas Complementares que tratam especificamente de segurança de informação e comunicações, conforme é explanado na NC 01/IN01/DSIC/GSIPR de 13 de outubro de 2008:

> *"Estabelecer critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta."*

5.6.1. Controles de Acesso

A Norma Complementar 07/IN01/DSIC/GSIPR de 15 de julho de 2014 tem como objetivo estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF. A NC 07 estabelece uma série de conceitos e processos que auxiliam o a implantação de modelo para gestão do processo de concessão de acesso aos ambientes e serviços de TIC. Dentre as considerações iniciais, NC 07 propõe os seguintes:

- Sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações;
- Processo para A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nos órgãos ou entidades da APF;
- Processo para prévia aprovação pela autoridade responsável pelo órgão ou entidade da APF;
- a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e Comunicações dos órgãos ou entidades da APF;
- estabelecer regras específicas para credenciamento de acesso de usuários aos ativos de informação em conformidade com a legislação vigente, e em especial quanto ao acesso às informações em áreas e instalações consideradas críticas.

O item seis da NC 07 especifica e orienta uma série de recomendações no que se refere ao acesso lógico nos órgãos. Especificamente para gestão dos serviços operacionalizados por terceirizados os seguintes tópicos se destacam:

- Responsabilizar o usuário pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de Termo de Responsabilidade (Modelo - Anexo A).
- Os órgãos ou entidades da APF, em suas áreas de competência, estabelecem regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.
- Utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.
- O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade públicas será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

A NC 07 orienta pela criação de normas e procedimentos que regule o processo de concessão de acesso lógico aos recursos de TIC. A norma utiliza o termo “Usuário” que especifica como:

> *“Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do*

responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade."

Assim todos os processos e procedimentos para gestão e controle de acessos desenvolvidos pelos Órgãos da APF deve prevê tratativas com terceirizados.

O item sete de NC 07 orienta para providências específicas aos usuários como: estabelecer formulário específico de Termo de Responsabilidade a ser difundido e assinado individualmente pelos usuários e definir regras específicas para autorização de acesso e credenciamento dos usuários em conformidade com a classificação dos ativos de informação.

5.6.2. Inventário e Mapeamento de Ativos de Informação

O processo de classificação dos ativos de informação também é muito importante, pois o nível de acesso e os procedimentos para concessão e exclusão de acesso devem variar conforme a criticidade dada a cada ativo. Para esse processo atividade, a Norma Complementar Nº 10/IN01/DSIC/GSIPR de 30 de janeiro de 2012 trata especificamente do processo de inventário e mapeamento de ativos de informação.

A NC 10 define *Ativos de Informação* como:

"meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram

esses meios, e também os recursos humanos que a eles têm acesso."

É interessante que a NC 10 utiliza o termo "*recursos humanos"* e o inclui no rol de ativos de informação. Assim pode-se inferir que os profissionais terceirizados também podem ser classificados ou incluídos como ativo de informação e, assim, devem ser "inventariados". O termo "*recursos humanos"* pode ser aplicado também aos usuários dos órgãos. O principal critério a ser utilizado é quais usuários tem acesso a quais ativos de TIC críticos.

A NC 10 descreve uma série de etapas no processo de inventário e mapeamento de ativos de Informação como:

- Coleta de informações gerais dos ativos de informação;
- Detalhamento dos ativos de informação;
- Identificação do(s) responsável(is) – proprietário(s) e custodiante(s) - de cada ativo de informação;
- Caracterização dos contêineres dos ativos de informação;
- Definição dos requisitos de segurança da informação e comunicações dos ativos de informação;
- Estabelecimento do valor do ativo de informação;

Para cada ativo de informação NC 10 recomenda identificar o(s) responsável(is) – proprietário(s) e custodiante(s). A NC 10 descreve o proprietário e custodiante como:

"refere-se a parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é

> *responsável primário pela viabilidade e sobrevivência dos ativos de informação...”*
>
> e
>
> *“refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação;”*

Especificamente para esses atores fica claro que o proprietário do ativo deve ser servidor do órgão ou detentor de cargo ou função de confiança da APF. Já para o custodiante não fica claro qual é exatamente e necessariamente a posição ou função desse indivíduo no órgão. Analisando pelo termo colocado: *“qualquer indivíduo ou estrutura do órgão ou entidade da APF...*”. Seria aceitável, pelo termo colocado pela NC 10, que um profissional terceirizado que operacionalize um serviço de TIC poderia ser custodiante de algum ativo de TIC.

5.6.3. Tratamento Da Informação

O Gabinete de Segurança Institucional da Presidência da República publicou a Norma Complementar nº 20 de 15 de dezembro de 2014 que trata de instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação.

A NC 20 afirma que os órgãos da Administração Pública produzem e tratam informações importantes e fundamentais para a gestão pública e tomada de decisão e, como tal, nas disposições gerais da referida norma, é atribuída a responsabilidade ao agente público pala salvaguarda da informação. Conforme abaixo:

> *"É dever do agente público salvaguardar a informação sigilosa e a pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal."*

A NC 20 é genérica sobre o tratamento da informação. Orienta sobre como tratar a informação no processo de produção uso e recepção, porém não trata especificamente de informação manutenida no ambiente de TIC.

6. PRINCIPAIS MODELOS E REFERÊNCIAS DE BOAS PRÁTICAS

Existem diversos modelos de referências e boas práticas de gestão e governança de TIC que são reconhecidas no mercado. A expressão “boas práticas” é derivada do inglês “*best practice”* que consiste basicamente em uma melhor forma de alcançar o melhor resultado. Há diversas boas práticas para diversas áreas ou profissões. Especificamente para gestão e governança de TIC destacam-se Control Objectives for Information and related Technology (CobiT®), IT Infrastructure Library-ITIL V3, Project Management Body of Knowledge (PMBOK) dentre outros.

Além das boas práticas existem também as conhecidas normas ISO. A ***International Organization for Standardization*** é uma entidade que reúne especialista de 162 (cento e sessenta e dois) países que aprovam normas internacionais em várias áreas de interesses como econômico e técnico. O Brasil, por meio da Associação Brasileira de Normas Técnicas (ABNT), é membro fundador da International Organization for Standardization (Organização Internacional de Normalização - ISO), da Comisión Panamericana de Normas Técnicas (Comissão Pan-Americana de Normas Técnicas - Copant) e da Asociación Mercosur de Normalización (Associação Mercosul de Normalização - AMN) e é também membro da International Electrotechnical Commission (Comissão Eletrotécnica Internacional - IEC).

Os modelos, as boas práticas e as normas ISO também devem ser objeto de consulta e referência para os órgãos da Administração Pública na condução das ações e atividades de gestão e governança de TIC. Tal entendimento é explícito na Nota Técnica Nº 7 - Sefti/TCU, conforme segue:

> *"Ademais, existem frameworks genéricos, que podem apoiar as organizações públicas na tarefa de implementar processos e práticas de governança de TI, tais como o Cobit 5 e os guias publicados por órgãos governantes superiores (ex.: Guia de Comitê de TI do Sisp), entre outros."*

Vamos verificar em algumas dessas normas o que exatamente tratam sobre normatizações processos e operações de TIC.

6.1. Modelo Corporativo para Governança e Gestão de TI da Organização

Lançado pela Information Systems Audit and Control Association (ISACA) em 1996, o Control Objectives for Information and Related Technologies (COBIT) é uma boa prática de mercado que especifica um conjunto de objetivos de controle para ajudar a comunidade de auditoria financeira a lidar melhor com ambientes relacionados a TI.

Em sua 5º versão, as boas práticas para os processos de gestão e governança, previstas no COBIT, buscam **alinhar a TI com o negócio**. O COBIT 5 faz clara distinção entre gestão e governança:

> *"A governança garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de*

> *decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.*
>
> *A gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos."*

O COBIT 5 não detalha especificamente sobre quais tipos de normatizações devem ser implementadas nem quais tipos de processos, serviços ou operações devem ser normatizados. Contudo, algumas citações ou referências que chamam a atenção.

O COBIT especifica 05 (cinco) princípios para implantação de governança e gestão TIC, são eles:

- 1º Princípio: Atender às Necessidades das Partes Interessadas
- 2º Princípio: Cobrir a Organização de Ponta a Ponta
- 3º Princípio: Aplicar um Modelo Único Integrado
- 4º Princípio: Permitir uma Abordagem Holística
- 5º Princípio: Distinguir a Governança da Gestão

Para o 1º Princípio: Atender às Necessidades das Partes Interessadas o COBIT 5 propõe que os Objetivos de TI devem estar relacionados aos Objetivos Corporativos.

"Os resultados de TI não são obviamente o único benefício intermediário necessário para a consecução dos objetivos corporativos. Todas as demais áreas funcionais de uma organização, tais como finanças e marketing, também contribuem para a consecução dos objetivos corporativos, mas no contexto do COBIT 5 somente as atividades e os objetivos de TI são considerados"

Utilizando 05 (cinco) dimensões da metodologia *Balanced Scorecard de TI (BSC)*[1]: Financeira, Cliente, Interna, Treinamento e Crescimento. O Cobit 5 lista objetivos da informação e tecnologia relacionada, conforme figura 3.

Figura 3: Dimensão BSC por Objetivo da Informação

Figura - 6: Objetivos de TI		
Dimensão BSC de TI	Objetivo da Informação e Tecnologia Relacionada	
Financeira	01	Alinhamento da estratégia de negócios e de TI
	02	Conformidade de TI e suporte para conformidade do negócio com as leis e regulamentos externos
	03	Compromisso da gerência executiva com a tomada de decisões de TI
	04	Gestão de risco organizacional de TI
	05	Benefícios obtidos pelo investimento de TI e portfólio de serviços
	06	Transparência dos custos, benefícios e riscos de TI
Cliente	07	Prestação de serviços de TI em consonância com os requisitos de negócio
	08	Uso adequado de aplicativos, informações e soluções tecnológicas
Interna	09	Agilidade de TI
	10	Segurança da informação, infraestrutura de processamento e aplicativos
	11	Otimização de ativos, recursos e capacidades de TI
	12	Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia
	13	Entrega de programas fornecendo benefícios, dentro do prazo, orçamento e atendendo requisitos
	14	Disponibilidade de informações úteis e confiáveis para a tomada de decisão
	15	Conformidade de TI com as políticas internas
Treinamento e Crescimento	16	Equipes de TI e de negócios motivadas e qualificadas
	17	Conhecimento, expertise e iniciativas para inovação dos negócios

[1] Metodologia de medição e gestão de desempenho desenvolvida em 1998 pelos professores da Harvard Business School (HBS) Robert Kaplan e David Norton.

Fonte: ISACA. COBIT 4.1. São Paulo, 2007.

Dos objetivos da informação e tecnologia relacionada, listados na figura 3, especificamente para os serviços de TIC terceirizados, os seguintes objetivos devem ser observados pelos gestores da área de TIC no processo de contratação e execução contratual:

- 07 - Prestação de serviços de TI em consonância com os requisitos de negócio;
- 08 - Uso adequado de aplicativos, informações e soluções tecnológicas;
- 10 - Segurança da informação, infraestrutura de processamento e aplicativos;
- 12 - Capacitação e apoio aos processos de negócios através da integração de aplicativos e tecnologia;
- 15 - Conformidade de TI com as políticas internas;
- 16 - Equipes de TI e de negócios motivadas e qualificadas;
- 17 - Conhecimento, expertise e iniciativas para inovação dos negócios.

O COBIT elenca objetivos de tecnologia de informação que devem ser atendidos e lança os seguintes questionamentos que auxiliam os gestores ou profissionais da área de TIC no entendimento do que as necessidades de TIC devem atender. Para a gestão e governança dos serviços operacionalizados por terceirizados, as seguintes perguntas de referência do COBIT são importantes:

- Como posso gerenciar o desempenho de TI?

- Como faço para criar e estruturar da melhor forma o meu departamento de TI?
- Qual é a minha dependência de fornecedores externos? Quão bem os contratos de terceirização de TI estão sendo gerenciados? Como faço para obter garantia dos fornecedores externos?
- Quais são os requisitos (de controle) da informação?
- Considerei todos os riscos de TI?
- Estou conduzindo uma resiliente e eficiente operação de TI?
- Como utilizar os recursos de TI de forma mais eficaz e eficiente?
- Quais são as opções de terceirização mais efetivas e eficientes?
- Tenho pessoal suficiente para TI? Como faço para desenvolver e manter sua capacitação, e como controlo seu desempenho?
- Como faço para obter garantia do funcionamento de TI?
- As informações que estou processando estão bem protegidas?
- Quão crítica é TI para a sustentação da organização? O que fazer se ela não estiver disponível?

As perguntas sugeridas pelo COBIT são muito pertinentes ao tema proposto. Utilizando esses questionamentos como referências é possível, minimamente, inferir sobre os instrumentos e mecanismos de controles necessários para uma operação do ambiente de TIC.

Principalmente para os serviços de TIC que são operacionalizados por profissionais terceirizados é importante definir e documentar os processos de trabalho do início ao fim.

6.2. Gerenciamento de Serviços de TIC

Prover os serviços de TIC com qualidade e flexíveis para manter constante alinhamento com o negócio ainda é desafiador para qualquer área ou setor de TIC. Desenvolvido pela Office of Government Commerce (OGC) a IT Infrastructure Library (ITIL) (Filho, 2012) é um conjunto de boas práticas para gerenciamento de serviços.

A ITIL, de maneira genérica, orienta como tratar os processos de TIC e pode ser utilizado por qualquer empresa ou órgão. Publicada em 2007, A ITIL descreve as atividades necessárias e os objetivos esperados para cada processo encontrado na TI, mas a ITIL não detalha como a organização deve implementar as atividades. Isso porque o é necessário que cada organização se estruture conforme suas necessidades específicas. O conceito por trás dos processos da ITIL é o ciclo de vida do serviço.

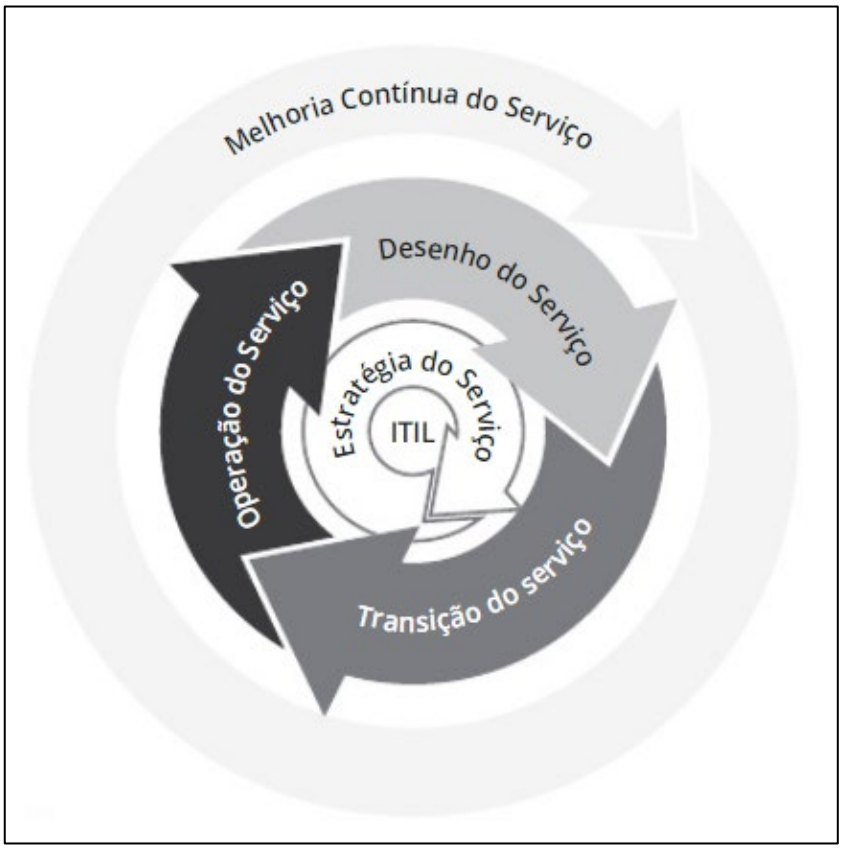
Com o foco no ciclo de vida, a ITIL se estruturou em 05 (cinco) livros que aborda especificamente cada ciclo de vida. São eles:

- Estratégia do Serviço;
- Desenho de Serviço;
- Transição de Serviço;
- Operação de Serviço;
- Melhoria de Serviço Continuada.

Além dos 05 (cinco) livros que contemplam o ciclo de vida, a ITIL possui um sexto livro que trata de explanar sobre conceitos e entendimentos do termo ciclo de vida; é livro Introdução ao ciclo de vida do serviço.

Para entender como funciona o ciclo de vida é recorrente a análise da figura 4 abaixo, conforme segue:

Figura 4: Ciclo de Vida do Serviço



Fonte: ITIL. Disponível em: < https://www.portalgsti.com.br/2016/10/o-ciclo-de-vida-do-servico-de-ti-da-itil.html >. Acesso em: 25 dez.2018.

A Estratégia do Serviço é o início de todo o processo da ITIL, é na estratégia do serviço que a TI da organização deve estruturar as necessidades com os objetivos da organização. É nessa fase que a TI deve garantir alinhamento com o negócio mitigando as demandas, as oportunidades e os riscos, a decisão por terceirizar ou não e qual será o retorno para o negócio.

Após a execução do ciclo de estratégia, inicia-se o ciclo Desenho do Serviço. Nesse ciclo a TI, com base nas informações levantadas na estratégia, projeto o serviço necessário. Deve ser considerado no desenho o Acordo de Nível de Serviço (ANS), os riscos, os fornecedores capacitados e qual a infraestrutura necessária.

O ciclo Transição de Serviço tratará das ações necessárias para minimizar os impactos para a organização quando os serviços entrarem em produção, ou seja, quando os serviços forem disponibilizados aos usuários.

Para a Operação do Serviço a área de TIC deve se preocupar em manter os serviços disponíveis com os critérios desenhados para as necessidades do negócio. Assim, é necessário que a TI esteja preparada para tratar ou atender, nesse ciclo de vida, os incidentes, os problemas e demais solicitações dos usuários de negócio.

Por último temos o ciclo de vida que busca aumentar a qualidade dos serviços fornecidos sempre com o objetivo de agregar mais valor ao negócio. O ciclo Melhoria de Serviço Continuada deve preocupar-se em analisar se o serviço em operação continua alinhado com a estratégia organizacional.

O controle e o equilíbrio, através do ciclo de vida dos serviços, asseguram quando a demanda do negócio muda, os serviços podem ser adaptados respondendo de forma eficiente.

O ciclo de vida Desenho do Serviço tem como objetivo, entre outros, projetar uma infraestrutura segura, resiliente e identificar e gerenciar os riscos. Para alcançar esses objetivos o ITIL propõe alguns processos que fazem parte do Desenho do Serviço.

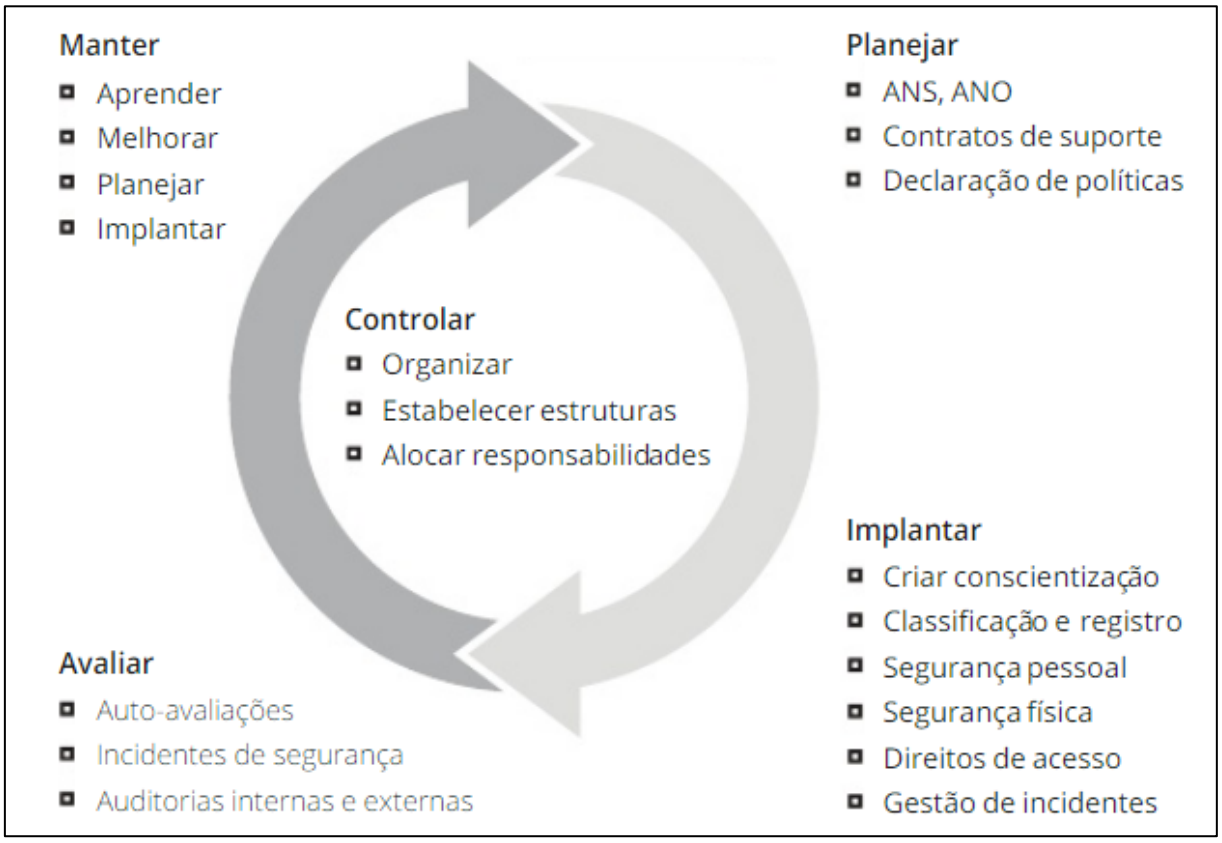
6.2.1. Gerenciamento de Segurança da Informação

O objetivo deste processo é controlar a provisão da informação e evitar o uso não autorizado. Tem como referência três conceitos básicos: confidencialidade,

integridade e disponibilidade (CID), o gerenciamento de segurança de informação busca garantir fornecimento da informação de maneira correta, completa e confiável.

Baseado na ISO/IEC 27001[2] , o ITIL estabelece uma estrutura de etapas para implantação de um sistema para gerenciamento da segurança da informação conforme figura abaixo:

Figura 5: Etapas para implantação de um sistema para gerenciamento da segurança



Fonte: https://www.itsmnapratica.com.br/tudo-sobre-itil/ . Acesso em 11 abr. 2019

As etapas preveem diversas atividades e dentre aquelas existem duas que podem dar um norte ao processo de governança dos serviços operacionalizados por terceirizados. São eles: alocar responsabilidades, estabelecer e controlar documentação, criar conscientização, direito de acesso. Fazendo um paralelo com

[2] ISO 27001 (Information Security Management) – Gerenciamento da segurança da informação – especificação com Diretriz para Uso. (Cobit 4.1, 2007).

essas atividades, pode-se inferir que para cada serviço operacionalizado deve ser estabelecido quem são os responsáveis em nível de gestão e operação. Para cada serviço operacionalizado dever ser documentado o processo de gestão e operação. E principalmente, após definir os responsáveis e estabelecer a documentação, é necessário constante processo de conscientização.

6.2.2. Gerenciamento de Fornecedor

Segundo Filho (2012) esse processo tem como objetivo assegurar que os serviços são gerenciados para suportar as metas de serviços de TIC e as expectativas de negócio.

Uma das atividades previstas é gerenciar o desempenho do contrato e do fornecedor, onde o objetivo é controlar a operação e a entrega de produtos. Também é recomendado no processo que haja um contrato formalmente estabelecido com responsabilidades e metas claras.

O processo Gerenciamento de Fornecedor previsto no ITIL V3 é bem superficial em comparação com os processos de planejamento de contratação e gerenciamento da contratação, previstos nos processos da Instrução Normativa N° 4, de 11 de setembro de 2014 do Ministério do Planejamento, Desenvolvimento e Gestão. Para as contratações de serviços e recursos de TIC com a Administração Pública Federal é obrigatório a execução dos processos da IN04 e como já foi explanado, a IN04 não estabelece modelos de gestão e nem indicadores para a execução contratual.

7. DOS CRIMES E DAS PENAS

A Constituição da República Federativa do Brasil de 1988 é bem taxativa sobre o reconhecimento do crime. Em seu Art. 5º discorre:

> *“ XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;”*

Se não existe lei que tipifique o ato cometido como um crime e se não existe a tipificação de pena para o crime praticado, o autor do ato não responderá pelo ato ou não será punido pelo mesmo.

O Código Penal Brasileiro admite três tipos de pena, que são de privativas de liberdade, restritivas de direitos e de multa. O autor de ato criminoso está passível de prisão, perdas de direitos político ou civil e multa.

O Código Penal Brasileiro possui uma seção que trata especificamente dos crimes praticados por funcionário pública contra a administração em geral e há dois artigos que trata, ou, relacionam-se com os serviços de TIC, conforme seguem:

> *“Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000))*

Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)"

e

"Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)

Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)

Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.(Incluído pela Lei nº 9.983, de 2000)"

Em análise a esses dois artigos primeiramente fica claro que os crimes tipificados só podem ser cometidos por "***Funcionário Público***" e o Código Penal tipifica o termo no Art. 327, conforme abaixo:

"Funcionário público

Art. 327 - Considera-se funcionário público, para os efeitos penais, quem, embora

transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

§ 1º - Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública. (Incluído pela Lei nº 9.983, de 2000)

§ 2º - A pena será aumentada da terça parte quando os autores dos crimes previstos neste Capítulo forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público. (Incluído pela Lei nº 6.799, de 1980)"

A princípio os crimes e penas tipificados nos artigos 313-A e 313-B não podem ser imputados a profissionais terceirizados já que os mesmos não são funcionários públicos ou as empresas em que estão contratados não executam atividade típica da Administração Pública.

Já para os agentes públicos, os artigos os alcançam sem sombra de dúvidas já que em totalidades são funcionários públicos de carreira ou são funções de confiança e comissionadas.

O Art. 313 – A inicia colocando com os termos “*Inserir ou facilitar”*. Porém o Código Penal não tipifica o que especificamente significa o termo “facilitar”. Em um processo penal ficaria a critério do agente da denúncia ou ao juízo causa interpretar, ao caso específico, a amplitude ou o alcance do termo “facilitar”. Seria possível inferir que, por exemplo, um gestor de TIC que não crie instrumentos ou mecanismos de gestão e controle de um determinado serviço de TIC, pode ser responsabilizado criminalmente por possível ato cometido pelo prestador terceirizado.

Outro termo descrito no respectivo artigo é “c*om o fim de obter vantagem indevida para si ou para outrem ou para causar dano”,* a autorizada denunciante ou jurídica deverá demonstrar o objetivo do ato. Uma possível falha cometida por um terceiro, culposamente, que resulte em dano à sociedade, poderia resultar em processo criminal? E o agente público, poderia responder por ato culposo, ou seja, sem intensão, do profissional terceirados.

Já no Art. 313-B o Código Penal sugere um processo de “*autorização*” a figura de uma “*autoridade competente*” para modificar ou altera os sistemas. Pode-se inferir que qualquer ação que resulte em modificação, mais conhecido como manutenção evolutiva, nos sistemas de informação deve ser autorizada por autoridade responsável pelo sistema. Mas a Código Penal não especifica quem é essa autoridade.

O Código Penal não alcança os profissionais terceirizado, pois os artigos se aplicam apenas aos Funcionários Públicos, claramente tipificados no Código. A a lei de licitações e contratos, Lei 8666/93, possui uma seção que trata de sanção administrativa e dos crimes e penas. Porém, nenhum dos artigos tratam de

culpabilidade ou responsabilização do profissional terceirizado pela execução dos serviços.

As tipificações dos crimes e as penas previstas alcançam apenas a pessoa jurídica. E os crimes previstos basicamente são os que atentam contra a lisura do certame licitatório. O único artigo que poderia ser aplicado a possível falha na execução do serviço seria o Art.87, segue:

> *"Art. 87. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar ao contratado as seguintes sanções:*
>
> *I - advertência;*
>
> *II - multa, na forma prevista no instrumento convocatório ou no contrato;*
>
> *III - suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos;*
>
> *IV - declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida*

sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior."

É necessário especificar em contrato quais atos poderiam ser passíveis de aplicação de sanção e qual sanção será aplicada a cada ato.

8. DIFICULDADES NA IMPLEMENTAÇÃO DA GOVERNANÇA E GESTÃO

A implementação ou implantação de um modelo de gestão e governança não é fácil e é muito complexo. Os modelos de gestão e governança devem alcançar os vários níveis de atuação da organização do estratégico ao operacional e no operacional deve alcançar prioritariamente os serviços que são operacionalizados por profissionais terceirizados.

Diversos fatores dificultam a implantação de um modelo de gestão e governança adequado aos órgãos da Administração Pública e esses representam sérios riscos aos serviços públicos prestado à sociedade, vejamos.

8.1. Ausência de interesse da alta gestão

A alta gestão dos órgãos da Administração Pública é formada, com raras exceções, por indicações puramente políticas. E na ânsia de mostrarem resultados para justificar os seus cargos ou funções, muitos gestores não querem submeter seus projetos a um modelo de gestão e governança. Entrelinhas, consideram os processos de TIC demasiadamente tecnicistas e burocrático. Assim, é comum numa ordem, ou canetada, um gestor determinar quebras de protocolos ou processos sem querer nem escutar e entender as consequências do ato.

8.2. Ausência de objetivos estratégicos ou programas institucionais

O modelo político brasileiro tende a ser imediatista. Políticas e projetos de governo saem da cartola dos políticos e são comunicados aos órgãos pela imprensa e já com data para implementação. Impossível os órgãos desenharem programas e projetos com metas e indicadores confiáveis e robustos em médio e longo prazo.

Impossibilita a reflexão interna sobre o objetivos e estratégias para entrega do serviço público. Essa modelo impacta diretamente nas áreas de TIC, pois não é possível traçar um plano diretor adequado, não é possível focar em entrega de soluções completas e integradas e muito mesmo, pensar e implementar em um modelo de gestão e governança adequado.

8.3. Quantitativo insuficiente de pessoal TIC

Já foi demonstrado no item 3.1 que o quantitativo de servidores públicos distribuídos nos órgãos da administração. Muitos órgãos da Administração Pública Federal não possuem carreiras de TIC e a distribuição não uniforme dos que tem agrava ainda mais o cenário. Uma evidência disso é a distribuição dos servidores do cargo de Analista em Tecnologia da Informação (ATI).

Cargo do quadro do Ministério do Planejamento, agora Ministério da Economia, o ATI possui atribuições, conforme abaixo:

> *"de planejamento, supervisão, coordenação e controle dos recursos de tecnologia da informação relativos ao funcionamento da administração pública federal, bem como execução de análises para o desenvolvimento, implantação e suporte a sistemas de informação e soluções tecnológicas específicas, especificação e apoio à formulação e acompanhamento das políticas de planejamento relativas aos recursos de tecnologia da informação, entre outras.*

Os servidores ocupantes do cargo de ATI, além de exercerem as atividades centralizadas na SLTI/MP, também podem ***atuar de forma descentralizada nos diversos órgãos que fazem parte do SISP****. Atualmente, os ATIs estão em exercício no Órgão Central, nos Órgãos Setoriais, que são os Ministérios e os órgãos da Presidência da República, nos Órgãos Seccionais, que são as Autarquias e Fundações, além dos Órgãos Correlatos, que são definidos como unidades desconcentradas e formalmente constituídas dos recursos de TI nos Órgãos Setoriais e Seccionais. Há ainda servidores que atuam no desenvolvimento de consultorias de projetos específicos nos órgãos do Sistema."*

Segundo informação disponibilizada no portal do Ministério, a distribuição dos ATI nos órgãos integrantes do SISP é conforme tabla abaixo:

Tabela 1:Distribuição dos ATI nos órgãos do SISP

ÓRGÃO DE EXERCÍCIO	ATI
MINISTERIO DO PLANEJAMENTO	188
PRESIDENCIA DA REPUBLICA	27
MINISTERIO DA JUSTICA	18
MINISTERIO DO DESENV SOCIAL E COMB FOME	17
MINISTERIO DA FAZENDA	16
MINIST.DA CIENCIA, TECNOLOGIA E INOVACAO	15
MINIST.DA AGRICULTURA,PECUARIA E ABAST.	14
MINIST.DO DESENV.INDUST.E COMER.EXTERIOR	11
MINISTERIO DA SAUDE	11

MINISTERIO DA INTEGRACAO NACIONAL	9
MINISTERIO DOS TRANSPORTES	9
MINISTERIO DAS RELACOES EXTERIORES	9
MINISTERIO DA EDUCACAO	8
MINISTERIO DO TRABALHO E EMPREGO	8
MINISTERIO DO MEIO AMBIENTE	7
MINISTERIO DA DEFESA	7
MINISTERIO DAS CIDADES	7
MINISTERIO DA CULTURA	6
MINISTERIO DE MINAS E ENERGIA	6
MINISTERIO DOS DIREITOS HUMANOS	5
MINISTERIO DO ESPORTE	5
FUNDACAO ESCOLA NACIONAL DE ADM. PUBLICA	5
ADVOCACIA-GERAL DA UNIAO	5
INSTITUTO DO PATR.HIST.E ART. NACIONAL	5
INSTITUTO NAC. DE COLONIZ E REF AGRARIA	5
INSTITUTO CHICO MENDES CONSERV.BIODIVER.	4
CONSELHO ADMINIST.DE DEFESA ECONOMICA	4
MINISTERIO DO TURISMO	3
INST. BR. MEIO AMB. REC. NAT. RENOVAVEIS	3
FUNDACAO NACIONAL DO INDIO	3
FUNDO NACIONAL DE DESENVOLV. DA EDUCACAO	3
DEPARTAMENTO NAC.DE INFRAEST. DE TRANSP.	3
INSTITUTO FEDERAL DE BRASILIA	2
DEPARTAMENTO NAC. DE PRODUCAO MINERAL	2
SUP.DE DESENVOLVIMENTO DO CENTRO OESTE	2
EMPRESA BRAS. DE SERVICOS HOSPITALARES	2
INST.NACIONAL DE EST.E PESQ.EDUCACIONAIS	2
INSTITUTO BRASILEIRO DE MUSEUS	2
FUNDACAO NACIONAL DE SAUDE	2
FUND COORD APERF PESSOAL NIVEL SUPERIOR	2
AGENCIA BRASILEIRA DE INTELIGENCIA	2
CONSELHO NAC.DE DESEN.CIEN.E TECNOLOGICO	2
INSTITUTO DE PESQUISA ECONOMICA APLICADA	2
AGENCIA ESPACIAL BRASILEIRA	1
AGENCIA NACIONAL DE AVIACAO CIVIL	1
DEPARTAMENTO DE POLICIA FEDERAL	1
GOVERNO DO ESTADO DO RIO DE JANEIRO	1
AGENCIA NACIONAL DE ENERGIA ELETRICA	1
AGENCIA NACIONAL DE AGUAS	1
GOVERNO DO DISTRITO FEDERAL	1
FUNDACAO CULTURAL PALMARES	1
Total Geral	**476**

Fonte:https://www.governodigital.gov.br/transformacao/sisp/nucleo-de-gestao-de-pessoas/analista-em-tecnologia-da-informacao-ati

Como demonstrado, distribuição dos ATI é completamente irregular e injustificável aos olhos da sociedade. Como justificar, por exemplo, o Ministério do Planejamento possuir no seu quadro 188 servidores enquanto que o Ministério da Saúde tem 11, o Mistério da Educação tem 8 e o Ministério da Justiça tem 18. Claro que cada órgão desse tem sua importância na concepção dos serviço e atendimento às necessidades da sociedade, mas aos olhos da sociedade, pela importância das pastas de saúde, educação e segurança, nada justifica.

8.4. Pessoal de TIC Desmotivados e Não Capacitados

O modelo de contratação e gestão de pessoas da Administração Pública é peculiar. Por determinação da Constituição da República, o servidor público deve ser contratado por meio de concurso público e, sendo aprovado e empossado no cargo possui a sonhada estabilidade. Ou seja, produzindo ou não, se dedicando ou não, o servidor pública não pode ser demitido. Conforme a Lei nº 8.112, de 11 de dezembro de 1990, preconiza:

> *"Art. 21. O servidor habilitado em concurso público e empossado em cargo de provimento efetivo adquirirá estabilidade no serviço público ao completar 2 (dois) anos de efetivo exercício. (prazo 3 anos - vide EMC nº 19)*
>
> *Art. 22. O servidor estável só perderá o cargo em virtude de sentença judicial transitada*

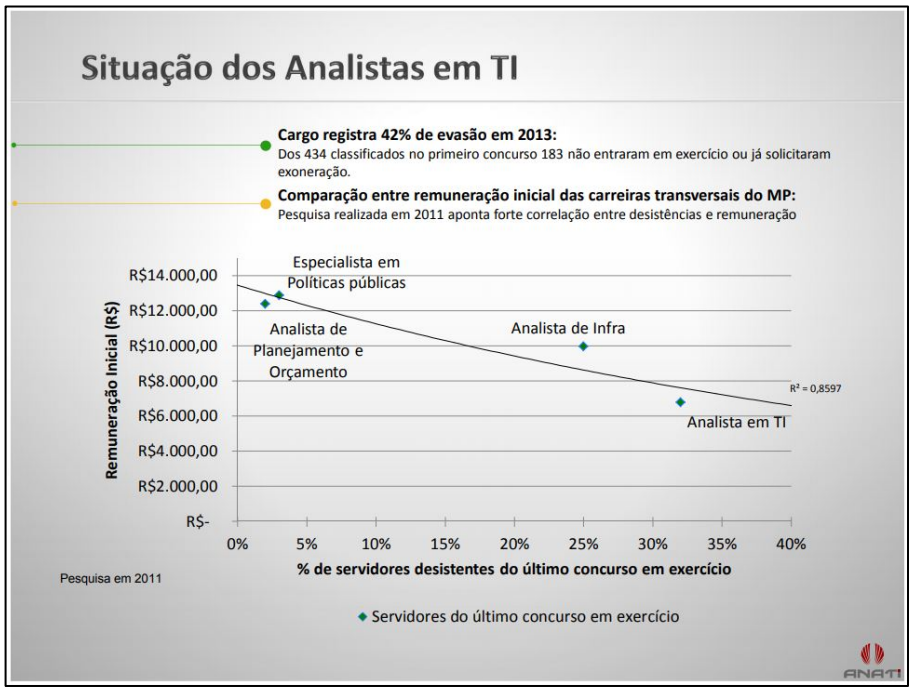
em julgado ou de processo administrativo disciplinar no qual lhe seja assegurada ampla defesa."

Essa legislação não motiva o servidor a melhorar seu desempenho, e consequentemente, não motiva a capacitação. Pois, trabalhando bem ou mal, dificilmente o servidor público é punido.

Além da ausência de motivação negativa, ou seja, o risco de punição, existe também a ausência de motivação positiva. O servidor que se dedica e se capacita para melhorar seu desempenho não recebe bônus pela diferença. Apesar de alguns cargos e carreiras possuírem progressão remuneratória pela capacitação e desempenho, a grande maioria das carreiras ou cargos não possui qualquer tipo de incentivo para o servidor que se destaca. Nem mesmo para assumir funções de chefia ou confiança os méritos profissional e educacional não são levados em conta. Sendo que a maioria das indicações para essas funções são pelo viés político e pessoal de quem indica.

Para os Analistas em Tecnologia da Informação o cenário ainda é pior. A começar pelo cargo em si. Pois não existe uma carreira para os profissionais que ingressarem no cargo de ATI. Soma-se a isso a baixa remuneração frente outras carreiras do Poder Executivo. Segundo a Associação Nacional dos Analistas em Tecnologia da Informação (ANATI) em relatório apresentado a época para Secretaria de Logística e Tecnologia da Informação, o cargo de ATI registrava 42% de evasão em 2013. Conforme figura 6.

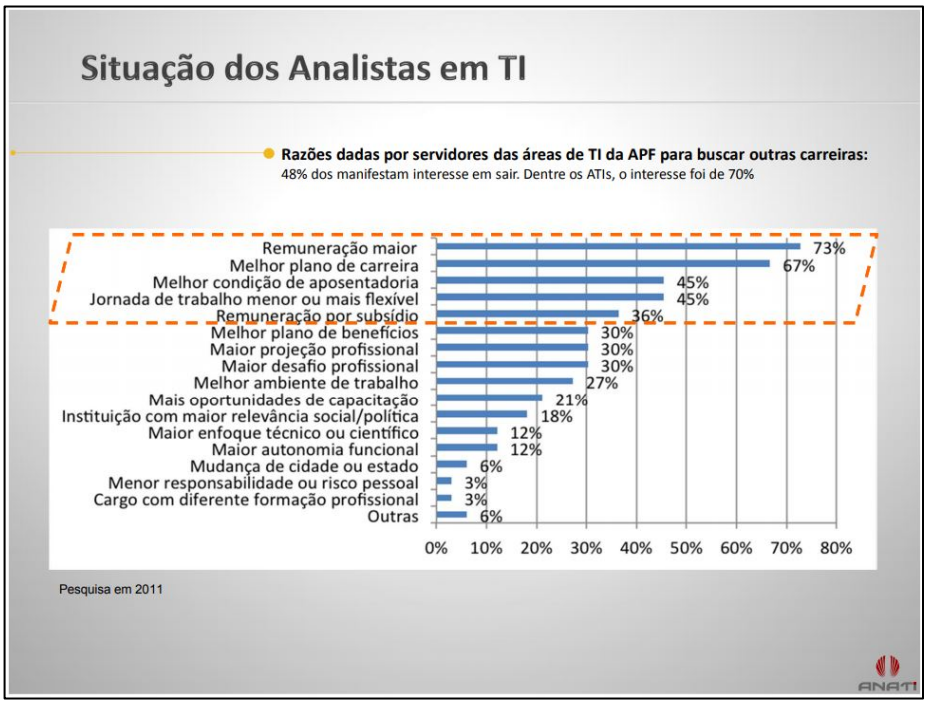
Figura 6: Evasão do Cargo de ATI



Fonte: https://www.anati.org.br/analistas-em-ti-em-numeros

No mesmo relatório a ANATI apresenta os principais motivadores que fazem os servidores ocupante do cargo de ATI buscar outras carreiras, conforme figura 7.

Figura 7: Motivação para a evasão



Fonte: https://www.anati.org.br/analistas-em-ti-em-numeros

A criação e estruturação da carreira de TI trará benefícios ainda no curto prazo, fortalecendo a estrutura de pessoal em TI, resultando no alcance de níveis desejáveis de retenção de recursos humanos e promovendo a melhoria contínua da capacidade de gestão e governança de TI no Poder Executivo Federal. Tal cenário foi objeto do Acórdão TCU 1.200/2014 – Plenário, conforme abaixo:

> *"9.2.6 ao Ministério do Planejamento, Orçamento e Gestão que empregue maior celeridade na análise da proposta de criação da carreira específica de Analista em Tecnologia da Informação (ATI), com remuneração que entender adequada e coerente com a relevância das atribuições*

desenvolvidas, visando reduzir a elevada taxa de evasão dos ocupantes do cargo de ATI, cuja taxa de ocupação do cargo está em torno de 75%, situação que perdurará mesmo após a posse dos novos concursados, em virtude da possível desistência de aproximadamente 25% dos candidatos aprovados no segundo concurso para ATI;"

E posteriormente reforçado pelo Acórdão TCU 2.326/2017 – Plenário, conforme segue:

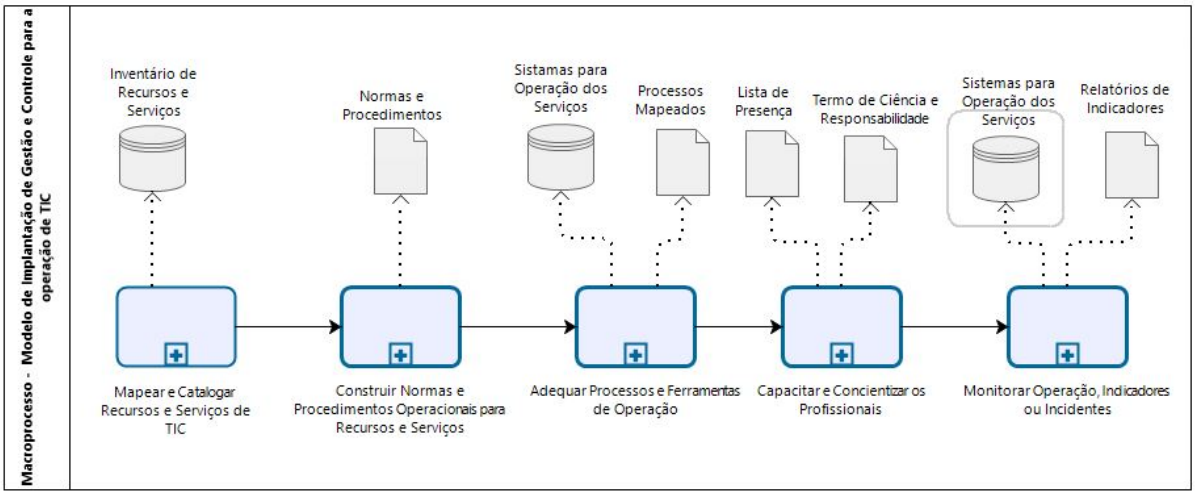
"...determinar à Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão (Setic/MP) , com fulcro no art. 250, inc. II, do RITCU, que execute acompanhamento do cumprimento das ações contidas nas determinações 9.2.1.1 e 9.2.1.2 do Acórdão 1.200/2014-TCU-Plenário a cargo das instituições sob sua jurisdição, em cumprimento ao estabelecido no Decreto 9.035/2017, art. 21, inc. III;"

9. PROPOSTA DE MELHORIA NA GESTÃO E CONTROLE DOS SERVIÇOS

A implantação de modelo de gestão e controle das atividades de operação de TIC é crítico para a governança de TIC. Saber o que é feito, quem faz, como faz e quais indicadores mínimos precisam ser monitorados é o mínimo que um gestor de TIC dos órgãos devem definir.

Frente esse desafio, esta seção propõe um modelo em macroprocesso simplificado com proposta fluxo e de produtos mínimos para implantar um modelo de gestão e controle, conforme figura 5.

Figura 8: Macroprocesso de Gestão e Governança na Operação de TIC



9.1. Mapear e Catalogar os Recursos e Serviços de TIC

O primeiro passo que um gestor de TIC deve fazer ao assumir a frente na área de TIC é conhecer detalhadamente os produtos e serviços que são entregues aos seus clientes, ou usuários. Para gerenciar os recursos e serviços de TIC é necessário entender, definir, e medir os resultados.

O macroprocesso Mapear e Catalogar os Recursos e Serviços de TIC tem por objetivo fazer com que os servidores públicos ou gestores que atuam na área de TIC do órgão conheçam os recursos e serviços de TIC sob sua gestão e responsabilidade. Deverão catalogar, classificar e atribuir responsabilidades aos atores que gerencia e opera os recursos ou serviços.

Como produto esse macroprocesso deverá gerar minimante um Portfólio de Produtos e Serviços de TIC. O Portfólio de Serviço é um produto previsto nos ciclos de vida do ITIL e, pelo ITIL, deve conter:

- Nome;
- Descrição
- Valor Proposto;
- Business Cases;
- Prioridades;
- Riscos;
- Ofertas e Pacotes;
- Custos e Preço.

Como proposta para produto do macroprocesso Mapear e Catalogar os Recursos e Serviços de TIC, o Portfólio de Serviços de TIC deverá conter:

- **ID:** Número identificador único que deverá será utilizado para o auto relacionamento entre os recursos e serviços de TIC.
- **Nome do Recurso/Serviço:** Nome claro e objetivo do recurso ou serviço de TIC. Por exemplo: Servidor de e-mail; Criar de Conta de e-mail; Criar Backup de Conta de e-mail e etc.

- **Descrição do Recurso/Serviço:** Descrição sucinta, clara e objetivo do recurso ou serviço de TIC de forma que uma pessoa leiga no assunto consigna compreender. Por exemplo: Servidor de provedor de serviço de e-mail faz é criar uma lista de contas de e-mail, com uma conta para cada pessoa que possa receber um e-mail no servido e etc.
- **Tipo:** Os recursos ou serviços de TIC deverão ser classificados em pelo menos dois tipos: Hardware ou Serviço. Hardware para os recursos de TIC quando for equipamentos fisicamente tangíveis, tipo Servidores de Rede, Switch e etc. E deverá ser classificado como Serviço processos operacionais ou recursos não tangíveis, tipo Links de Acesso à Internet, Máquinas ou Servidores Virtuais, Criar usuário de rede, Sistema de Cadastro de Usuário e etc.
- **Criticidade do Recurso ou Serviço:** Cada recurso ou serviço de TIC deverá ser classificado sua criticidade do ponto de vista de impacto aos processos de negócio. Deverão ser classificados como **CRÍTICO**, quando uma falha ou indisponibilidade pode interromper ou paralisar os processos finalísticos do órgão. E deverão ser classificados como **NÃO CRÍTICOS** quando uma falha ou indisponibilidade não interrompe ou paralisa os processos finalísticos.
- **Área/Unidade Proprietária:** Dever ser descrito qual área ou unidade é dona do recurso ou serviço. A depender do recurso ou serviço as áreas de negócio ou finalísticas serão identificadas, por exemplo para sistemas ou aplicativos que apoiam os processos

finalísticos. Já outros recursos e serviço a área proprietária será, naturalmente, a área de TIC. Por exemplo Link da Acesso à internet a área proprietária sempre será a área de TIC.

- **Proprietário (Nome, Ramal e e-mail):** Deverá ser identificado proprietário do recurso ou serviço de TIC. Proprietário deve ser servidor público de carreira ou ocupante de função de confiança. A depender do recurso ou serviço o proprietário deverá ser pessoa das áreas finalísticas, por exemplo para sistemas ou aplicativos que apoiam os processos finalísticos. Já outros recursos e serviço o proprietário será, naturalmente, pessoa da área de TIC. Por exemplo Link da Acesso à internet o proprietário sempre será a servidor ou gestor da área de TIC. O proprietário é o dono do recurso ou serviço e pode, por exemplo, decidir pelo desligamento do recuso e serviço. Além de ser o responsável pelo contínuo alinhamento com as necessidades do negócio.
- **Custodiante (Nome, Ramal e e-mail):** Deverá ser identificado o custodiante do recurso ou serviço de TIC. Proprietário deve ser servidor público de carreira ou ocupante de função de confiança da área de TIC do órgão. O custodiante é o responsável pela guarda dos recursos e serviços de TIC e deverá garantir disponibilidade, integridade, confidencialidade e autenticidade dos recursos e serviços de TIC, além de, em conjunto com o Proprietário, também ser o responsável pelo contínuo alinhamento com as necessidades do negócio.

- **Responsável Técnico (Nome, telefone e e-mail):** Deve ser identificado a pessoa responsável técnico pelo recurso ou serviço de TIC. Essa pessoa deve possuir conhecimento técnico e é a que põe a mão na massa. Ou seja, a pessoa que sabe qual parafuso apertar para que a máquina volte a funcionar. É o profissional que operacionaliza o recurso ou serviço de TIC. Pode ser servidor público de carreira ou ocupante de função de confiança da área de TIC do órgão, ou, também, pode ser profissional prestador de empresas terceirizadas.
- **Fornecedor (Nome, CNPJ, Nº do contrato, endereço, e-mail, telefone):** Para os recursos e serviços de TIC que são providos por empresas terceirizadas essas devem ser identificadas também.
- **Responsável pelo Fornecedor ou Preposto (Nome, telefone e e-mail):** O responsável pelo fornecedor é a pessoa do quadro da contratada responsável pela interlocução com os gestores ou fiscais do contrato. A Instrução Normativa n° 4, de 11 de setembro de 2014 descreve como "*representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual"*.
- **Recursos e Serviços de TIC Relacionados:** Deverá ser identificado para cada recurso ou serviço de TIC outros recursos ou serviço de TIC que estão relacionados. Como uma matriz, o objetivo é identificar o que uma falha ou indisponibilidade em um

determinado recurso ou serviço de TIC pode impactar em outro. Por exemplo. Falha ou indisponibilidade do servidor de e-mail impactará diretamente os serviços de criação de conta de e-mail, deixando-o indisponível também.

Com esse portfólio construído os gestores, servidores e prestadores de serviços terceirizados terão uma dimensão do tamanho da responsabilidade. Esse portfólio deverá ser disponibilizado preferencialmente em plataforma Web para que todos da área de TIC possa consultar quando necessário. No Apêndice – A consta um exemplo de como poderia ser esse **Portfólio de Recursos e Serviços de TIC**.

9.2. Construir Normas e Procedimentos Operacionais

Com o Portfólio de Recursos e Serviços de TIC em mãos, os gestores da área de TIC precisam institucionalizar minimamente normas e procedimentos. Os gestores da área de TIC dos Órgãos da Administração Pública, por força da lei, são obrigados a seguir os princípios da legalidade e publicidade. Devem normatizar seus processos e atividades em políticas, normas e procedimentos conforme explanado no item 4.2.

É recomendado iniciar pelos recursos e serviços de TIC classificados como CRÍTICOS e que são operacionalizados por profissionais terceirizados, já identificados no macroprocesso Mapear e Catalogar os Recursos e Serviços de TIC como Responsável Técnico.

Uma constante preocupação ao construir os normativos e procedimentos é sempre ter o cuidado de mantê-los alinhados, ou não conflitar, com os normativos

superiores. Ou seja, os normativos e procedimentos devem observar o que diz os decretos, as leis e a Constituição sob o risco de serem declarados nulos.

Quanto aos tipos de documentos que devem ser construídos a Norma Técnica ABNT NBR ISO 9000:2015 (ABNT, 2015), que descreve os conceitos fundamentais e princípios de gestão da qualidade, orienta para três tipos de documentos:

- **Políticas**: Intensões e direção e uma organização expresso formalmente pela alta direção.
- **Normas**: Ajustam as condutas e atividades assegurando as características desejáveis dos recursos e serviços.
- **Procedimentos**: Definem a maneira de agir, método de executar e entregar produtos ou serviços.

O ideal é que os recursos e serviços de TIC possuam Políticas, Normas e Procedimentos, porém com o objetivo de diminuir as barreiras já pontuadas no item 8 ,Dificuldades na Implementação da Governança e Gestão, é aconselhável para este macro processo que minimamente devam ser institucionalizadas as normas e procedimentos.

É importante destacar que o termo “institucionalizado”, empregado aqui, se refere a escrito, aprovado e publicado. A publicação deve ser minimamente em Boletim de Serviço.

Para facilitar o entendimento das normas e procedimentos é interessante que estes sejam complementados com ilustrações, infográficos resumindo tópicos mais críticos ou modelos em processos de negócio.

As normas e procedimentos devem ser disponibilizadas preferencialmente em plataforma Web e de livre acesso a todos do órgão, principalmente aos que atuam na área de TIC.

Para cada norma e procedimento deve ser explícito o fluxo de trabalho e os todos os atores envolvidos para cada recurso ou serviço de TIC. É fundamental estar claro:

- Quem pode solicitar (usuários do órgão, Proprietários, Custodiantes ou Responsáveis Técnicos);
- Como solicitar (ferramentas e mecanismos de requisição);
- Quem autoriza (a depender do recurso ou serviço de TIC);
- Quem executa (Custodiantes ou Responsáveis Técnicos);
- O que entrega (resultado da operação);
- Prazo para entrega (Níveis de Serviço);
- Como Entrega (ferramentas e mecanismos)

9.3. Adequar Processos e Ferramentas de Operação

Este macroprocesso tem por objetivo adequar os processos e ferramentas que são necessários para a operacionalização dos serviços e recursos TIC. Devem atender às necessidades das normas e procedimentos definidos e, preferencialmente, a operação deverá ser sistematizada para diminuir incidência de erros ou quebras de fluxos de trabalhos definidos pelas Normas e Procedimentos definidos e também facilitar o monitoramento dos indicadores.

9.4. Capacitar e Conscientizar os Profissionais

Com foco principal nos técnicos terceirizados, nos Proprietários, nos Custodiantes e nos Responsáveis Técnico dos recursos e serviços de TIC, este macroprocesso busca capacitar e conscientizar todos os atores e usuários que operacionalizam ou utilizam os recursos e serviços de TIC.

Recomendo que para cada norma e procedimento institucionalizado haja workshop ou mesmo treinamentos.

Como produto deste macroprocesso é recomendado que sejam gerados minimamente:

- Termos de Ciência e Responsabilidade: que deverão ser firmados individualmente pelos principais atores envolvidos nos processos descritos em normas e procedimentos e pelos responsáveis pelos recursos e serviços de TIC (Proprietários, nos Custodiantes e nos Responsáveis Técnico);
- Lista de Presença: assinatura de todos presentes no wokshop.

Além do workshop proposto é muito importante que seja implementado um constante processo de conscientização, principalmente na ceara da segurança da informação. Esse processo deverá alcançar todos as pessoas que consome ou utilizar qualquer recurso ou serviços de TIC e, a depender do serviço e recurso, também pode alcançar usuários externos ao órgão. Por exemplo, informativos via e-mails, ao menos uma vez por semana são interessantes.

9.5. Monitorar Operação, Indicadores ou Incidentes

Monitorar a operação e execução dos serviços de TIC é obrigação dos servidores públicos ou gestores que atuam na área de TIC, principalmente para os que são fiscais ou gestores dos contratos com as terceirizadas. Falhas ou erros cometidos por terceirizados que não forem devidamente fiscalizados pode resultar em responsabilização do agente público na esfera administrativa e penal.

Com normativos, procedimento e processos devidamente institucionalizados e implantados é hora de monitorar os indicares para garantir a adequada prestação de serviço ao órgão.

Para cada recurso ou serviço de TIC deve ser verificado:

- Se os indicadores realmente traduzem o que se espera do recurso ou serviço;
- Se os contratos vigentes preveem os indicadores definidos como instrumento de fiscalização. Pode ser necessário repactuar ou mesmo realizar novas contratações.

O monitoramento deve ser constante e a frequência vai depender de cada recurso ou serviço de TIC.

A execução desses macroprocessos pode parecer ser onerosa aos olhos dos gestores da área de TIC, porém são fundamentais para conhecer minimamente o tamanho do “problema” quem tem em mãos e, a partir daí, será possível desenhar as melhores estratégias para implantação de um modelo de gestão e governança de TIC.

10. CONCLUSÃO

Gestão e governança de TIC são processos e atividades que oneram muito as áreas de TIC, porém são fundamentais para garantir que os esforços e custos de TIC estejam alinhados aos objetivos estratégicos e que estejam atendendo adequadamente as necessidades das organizações.

Em épocas de transformação digital, os recursos tecnológicos estão cada vez mais integrados e transparentes no cotidiano das pessoas. Microcomputadores, tablets e celulares com capacidade de armazenamento e processamento inimagináveis nos anos 80 ou 90 em conjunto com conectividade à internet em lugares distantes ou remotos, potencializaram exponencialmente os serviços em plataformas tecnológicas e abriram um leque gigantesco de novas oportunidades e negócios.

Os serviços governamentais não estão inertes à transformação digital. Com os cidadãos cada vez mais conectados a cobrança por serviços públicos mais ágeis, transparentes e, principalmente, desburocratizados é a palavra de ordem no governo em todas as esferas de poder.

Porém, não adianta construir palacetes na areia da praia. Se não houver uma base sólida e organizada para orientar e justificar os investimentos de TIC a transformação digital do governo pode se transformar em homéricos prejuízos aos cofres públicos e latente risco à sociedade, considerando a sensibilidade natural peculiar aos dados e informações governamentais.

É agravante a massiva terceirização dos processos e atividades das áreas de TIC. Onde profissionais, prestando serviço por uma empresa terceirizada, sem

vínculo com a administração pública, tem acesso total a irrestrito a dados e informações sob gestão e guarda dos órgãos públicos.

Não que a terceirização por si só represente o risco aos serviços, muito pelo contrário. A terceirização é necessária e, para muitas atividades, representa mais qualidade e economia aos cofres públicos. Seria inviável e antieconômico para o Estado manter e atender todas as atividades necessárias ao dia-a-dia das repartições apenas com servidores públicos de carreira. E isso também se aplica às áreas de TIC dos órgãos da Administração Pública. Não é viável manter todos os processos e atividades de TIC operacionalizados exclusivamente por servidores concursados.

O cerne da questão é garantir que a gestão e governança dos processos e serviços estão sob o controle e domínio dos gestores de TIC. E esses gestores, servidores de carreira ou detentor função ou cargo de confiança com vínculo com a Administração Pública, devem garantir que os serviços e produtos estão sendo executados sob as diretrizes das políticas, normas e procedimentos devidamente definidos institucionalmente e alinhados às necessidades e aos objetivos estratégicos do órgão.

Por mais que os modelos de gestão e governança de TIC não sejam deterministas ou, por mais que os modelos de gestão e governança de TIC não detalhem o que e como normatizar é fundamental para Administração Pública que a manutenção da confidencialidade, da integridade e da disponibilidade dos dados e informações estejam devidamente garantidos.

Os gestores da área de TIC devem ter o domínio de todos os processos e atividades de TCI que são executadas nos órgãos. Os gestores devem ter mapeado

em mãos: o que a área TIC faz, como é solicitado, quem faz, quais indicadores aceitáveis, e quem é o gerente ou proprietário de cada recursos ou serviço.

Já para os profissionais terceirizados que operacionalizam os recursos e serviços de TIC é fundamental conhecer quem pode solicitar, como deve ser solicitado, quem pode autorizar, como entregar, quais são os indicadores de atendimento e, principalmente, o risco de ser responsabilizado pelos seus atos.

Evoluir os serviços, desburocratizar a máquina pública, facilitar o acesso aos serviços e transparecer os indicadores à sociedade são as palavras de ordem na gestão governamental, porém a alta gestão dos órgãos e, em especial, os gestores da área de TIC não devem menosprezar ou subjugar os processos de gestão e governança. Antes de decidir onde e em quê investir os gestores de TIC tem por obrigação consultar os indicadores e orientações da governança de TIC para melhor conduzir os investimentos e para operacionalizar um serviço de TIC os gestores devem verificar se possuem todos os instrumentos necessários para a gestão e garantir a melhor administração do recurso ou serviços de TIC sob sua guarda.

11. REFERÊNCIAS

ALEXANDRINO, Marcelo; PAULO, Vicente. Direito administrativo descomplicado. 26.ed. Brasília: Método, 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 9000:2015 - Sistemas de gestão da qualidade: Fundamentos e vocabulário. Rio de Janeiro: ABNT, 2015.

BRASIL. Código Penal Brasileiro. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 11 abr. 2019.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988 promulgada em 5 de outubro de 1988. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 11 abr. 2019.

BRASIL. LEI Nº 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civil da União, das autarquias e das fundações públicas federais. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8112cons.htm Acesso em: 11 abr. 2019.

BRASIL. NORMA COMPLEMENTAR 01/IN01/DSIC/GSIPR. de 13 de outubro de 2008.Gestão de Segurança da Informação e Comunicações.: Disponível em http://dsic.planalto.gov.br/legislacao/nc_1_normatizacao.pdf Acesso em: 11 abr. 2019.

BRASIL. NORMA COMPLEMENTAR 10/IN01/DSIC/GSIPR de 30 de janeiro de 2012. Estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação. : Disponível em http://dsic.planalto.gov.br/legislacao/nc_10_ativos.pdf Acesso em: 11 abr. 2019.

BRASIL. INSTRUÇÃO NORMATIVA N° 4. de 11 de setembro de 2014. Processo de contratação de Soluções de Tecnologia da Informação: Disponível em; https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/1%20-%20IN%204%20%2011-9-14.pdf Acesso em: 11 abr. 2019.

BRASIL. LEI Nº 12.965 de 23 de abr de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em; http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 11 abr. 2019.

BRASIL. Norma Complementar 07/IN01/DSIC/GSIPR de 15 de julho de 2014. Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_07_revisao_01.pdf. Acesso em: 11 abr. 2019.

BRASIL. NORMA COMPLEMENTAR 20/IN01/DSIC/GSIPR de 15 de dezembro de 2014. Estabelecer diretrizes de Segurança da Informação e Comunicações (SIC). Disponível em: http://dsic.planalto.gov.br/legislacao/copy_of_NC20_Revisao01.pdf Acesso em: 11 abr. 2019.

BRASIL. DECRETO Nº 8.638 de 15 de janeiro de 2016. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

BRASIL. DECRETO Nº 8.777de 11 de maio de 2016: Institui a Política de Dados Abertos do Poder Executivo Federal: Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8777.htm Acesso em 11 abr. 2019.

BRASIL. DECRETO Nº 8.789, de 29 de junho de 2016: Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8789.htm Acesso em 11 abr. 2019.

BRASIL. PORTARIA Nº 19. Dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.: Disponível em: https://www.governodigital.gov.br/transformacao/compras/documentos/portaria-no-19-de-29-de-maio-de-2017-pdf/view Acesso em 11 abr. 2019.

BRASIL. *DECRETO Nº 9.507, de 21 de setembro de 2018*. Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União.: Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9507.htm Acesso em 11 abr. 2019.

BRASIL. **Estratégia de Governança Digital (EGD).** Brasília, DF: Imprensa Nacional, 2018.

CONTROLADORIA-GERAL DA UNIÃO. CGU. *Painel de Gastos de TI*. Ferramenta que apresenta informações sobre os gastos de Tecnologia da Informação do Poder Executivo Federal. Disponível em http://paineis.cgu.gov.br/gastosti/index.htm Acesso em 11 abr. 2019.

CHIARI, Renê. O que é ITIL? Tudo o que você precisa saber sobre o tema: O conteúdo principal s da ITIL. 2016. Disponível em: https://www.itsmnapratica.com.br/tudo-sobre-itil/ . Acesso em 11 abr. 2019.

CRUZ, Cláudio Silva da; FIGUEREIDO, Rejane Maria da Costa; ANDRADE, Edméia Leonor Pereira de. **Processo de contratação de serviços de tecnologia da informação para organizações públi**cas. Brasília: PBQP Software, 2012. 212 p.

CESTARI FILHO, Felício. **ITIL** v. 3 Fundamentos. Rio de Janeiro: RNP/ESR, 2011.

ISACA. *COBIT 4.1.* São Paulo, 2007.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. *Painel de Compras*. Painel de compras governamentais do sistema SIASG. 2018. Disponível em: http://paineldecompras.planejamento.gov.br/QvAJAXZfc/opendoc.htm?document=paineldecompras.qvw&lang=en-US&host=QVS%40srvbsaiasprd04&anonymous=true. Acesso em 11 abr. 2019.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTAO. *Portal Brasileiro de Dados Abertos*. Dados que são livremente disponíveis para todos utilizarem e redistribuírem como desejarem. 2018. Disponível em: http://dados.gov.br/ Acesso em 11 abr. 2019.

SISP. *Guia de Governança de*10 de setembro de 2017 2.0. Guia de Governança do SISP. Disponível em: http://www.sisp.gov.br/govtic/wiki/download/file/Guia_de_Governan%E7a_de_TIC_do_SISP_v_2.0. Acesso em 11 abr. 2019.

TRIBUNAL DE CONTAS DA UNIÃO. (*ACÓRDÃO Nº 1.603-32/08-Plenário de* 13 de agosto de 2008. Levantamento de Auditoria. Disponível em: https://contas.tcu.gov.br/pesquisaJurisprudencia/#/detalhamento/11/838020071.PROC/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/false/1/false Acesso em 11 abr. 2019.

TRIBUNAL DE CONTAS DA UNIÃO. *ACÓRDÃO Nº 2471/2008 - Plenário.* Brasília, 2008.

TRIBUNAL DE CONTAS DA UNIÃO. *ACÓRDÃO Nº 2.308/2010-TCU-Plenário.* Brasília: 2010.

TRIBUNAL DE CONTAS DA UNIÃO. *NOTA TÉCNICA Nº 7 - Sefti/TCU.* Brasília: 2014.

TRIBUNAL DE CONTAS DA UNIÃO. *Levantamento de Governança de TI*. Levantamento da situação de governança de tecnologia da informação (TI) na Administração Pública Federal (APF). 2016. Disponível em: https://portal.tcu.gov.br/governanca/governanca-de-ti/igovti-no-tcu/resultados-2016.htm Acesso em 11 abr. 2019.

APÊNDICE A - PORTFÓLIO DE RECURSOS E SERVIÇOS DE TIC

ID	Nome	Descrição	Tipo	Criticidade	Unidade Proprietária	Proprietário			Custodiante			Responsável Técnico			Fornecedor						Preposto			Recurso/Serviços Relacionados		
						Nome	Fone	E-mail	Nome	Fone	E-mail	Nome	Fone	E-mail	Nome	CNPJ	Nº Cont.	End.	E-mail	Fone	Nome	fone	e-mail	Id	Id	Id...n