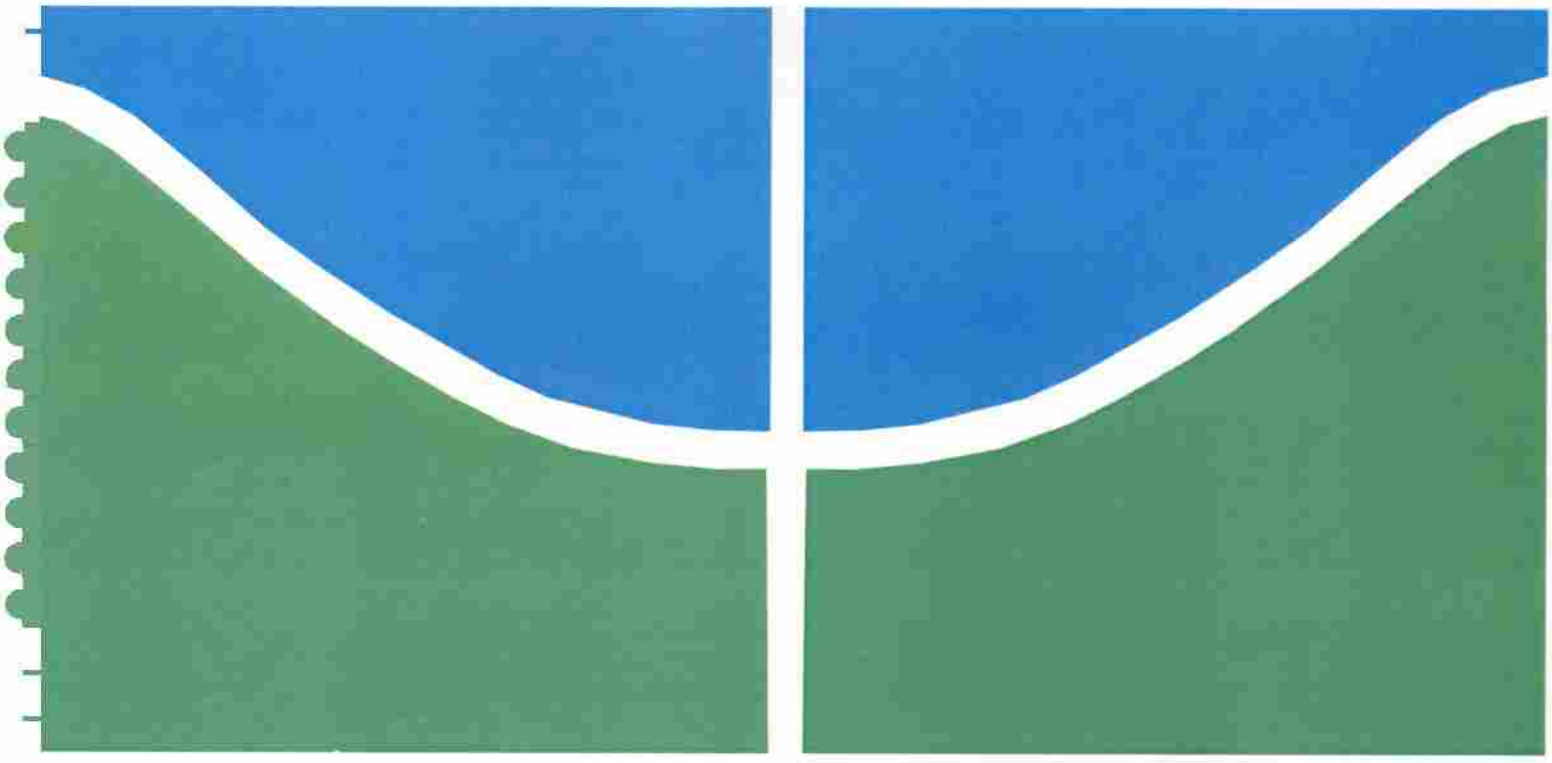

GERENCIAMENTO DE INFRAESTRUTURA DE TI: ABORDAGEM ACERCA DA ESTRUTURA DE TI DE UMA AGÊNCIA REGULADORA

REGINALDO LIRA DE ARAÚJO

MONOGRAFIA DE ESPECIALIZAÇÃO DO CURSO DE GESTÃO EM TECNOLOGIA DA INFORMAÇÃO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GERENCIAMENTO DE INFRAESTRUTURA DE TI: ABORDAGEM ACERCA DA ESTRUTURA DE TI DE UMA AGÊNCIA REGULADORA

REGINALDO LIRA DE ARAÚJO

ORIENTADORA: MSc ELIANE CARNEIRO SOARES

MONOGRAFIA DE ESPECIALIZAÇÃO DO CURSO DE GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.008/2017
BRASÍLIA/DF: JULHO – 2017

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GERENCIAMENTO DE INFRAESTRUTURA DE TI: ABORDAGEM ACERCA DA ESTRUTURA DE TI DE UMA AGÊNCIA REGULADORA

REGINALDO LIRA DE ARAÚJO

MONOGRAFIA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO.

APROVADA POR:

ELIANE CARNEIRO SOARES
MESTRA, UNB/ENE (ORIENTADORA)

EDNA DIAS CANEDO
DOUTORA, UNB/ENE (EXAMINADORA EXTERNA)

LAERTE PEOTTA DE MELO
DOUTOR, UNB/ENE (EXAMINADOR EXTERNO)

BRASÍLIA/DF, 24 de julho de 2017

FICHA CATALOGRÁFICA

Araújo, Reginaldo Lira de.
Gerenciamento de infraestrutura de TI: abordagem acerca da estrutura de TI de uma Agência Reguladora [Distrito Federal], 2017.
61p., 210 x 297mm (ENE/FT/UnB, Especialização, Engenharia Elétrica, 2017).
Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.

1. Sistemas de Informação
2. Governança de TI
3. Gestão de TI
4. Infraestrutura de TI
5. Gestão de Continuidade
I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Araújo, Reginaldo Lira de. (2017). Gerenciamento de infraestrutura de TI: abordagem acerca da estrutura de TI de uma Agência Reguladora. Monografia de Especialização, Publicação UnBLabRedes.MFE.008/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 61p.

CESSÃO DE DIREITOS

AUTOR: Reginaldo Lira de Araújo
TITULO DA TESE: Gerenciamento de infraestrutura de TI: abordagem acerca da estrutura de TI de uma Agência Reguladora.
GRAU / ANO: Especialista / 2017

É concedida à Universidade de Brasília permissão para reproduzir cópias desta dissertação de especialização e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte dessa dissertação de mestrado pode ser reproduzida sem autorização por escrito do autor.

Reginaldo Lira de Araújo

Reginaldo Lira de Araújo
QI 31 Lotes 2/4 Bloco 4 Apartamento 405
Edifício Jardins Life – Guará 2
CEP: 71.065-310 - Brasília - DF
Tel. 55 – 61 – 99159-8300 / reginaldo.lira@gmail.com

RESUMO

GERENCIAMENTO DE INFRAESTRUTURA DE TI: ABORDAGEM ACERCA DA ESTRUTURA DE TI DE UMA AGÊNCIA REGULADORA.

Autor: Reginaldo Lira de Araújo
Orientadora: MSc Eliane Carneiro Soares
Gestão em Tecnologia da Informação
Brasília, julho de 2017

A informação é um dos principais ativos de qualquer organização, seja ela pública ou privada. Diante da geração cada vez mais rápida e do volume cada vez maior de dados, torna-se indispensável a utilização de sistemas de informação, suportados por uma complexa infraestrutura tecnológica, para conseguir obter, tratar e analisar esses dados, gerando assim a informação. Nesse contexto e considerando a importância estratégica que a TI tem alcançado, é essencial que se faça a adequada gestão da estrutura e dos investimentos, buscando assim alcançar os melhores resultados dos serviços prestados através de uma Governança de TI bem planejada, implementada e executada.

No âmbito da Administração Pública Federal, é necessário que os órgãos e entidades implantem e executem processos de governança e de gestão de TI, sempre alinhados às leis e aos demais normativos, tendo em vista a devida prestação dos serviços públicos, a maior participação da sociedade, a transparência das ações e a celeridade na execução de suas atividades finalísticas.

ABSTRACT

Author: Reginaldo Lira de Araújo
Supervisor: MSc Eliane Carneiro Soares
Programa de Pós-graduação em Engenharia Elétrica
Brasília, july of 2017

Information is a major asset of any organization, independente of public or private. In view of the ever faster generation and the increasing volume of data, it is indispensable to use information systems, supported by a complex technological infrastructure, to obtain, treat and analyze these data, thus generating the information. In this context, and considering the strategic importance that IT has achieved, it is essential that proper management of the structure and investments is achieved, in order to achieve the best results of the services provided through well-planned, implemented and executed IT Governance.

In the scope of the Federal Public Administration, it is necessary that the organs and entities implement and execute processes of IT governance and IT management, always in line with laws and other regulations, in view of the proper provision of public services, greater participation of society, transparency of the actions and the speed in the execution of its finalistic activities.

SUMÁRIO

1. INTRODUÇÃO 1
1.1. OBJETIVO GERAL 2
1.2. OBJETIVOS ESPECÍFICOS 2
1.3. JUSTIFICATIVA 3
1.4. METODOLOGIA UTILIZADA 3
1.5. ESTRUTURA DA MONOGRAFIA 4
2. EMBASAMENTO TEÓRICO SOBRE O TEMA 5
2.1. DADOS X INFORMAÇÕES 5
2.2. SISTEMAS DE INFORMAÇAO 5
2.3. TECNOLOGIA DA INFORMAÇÃO 6
2.3.1. Hardware 7
2.3.2. Software 8
2.3.3. Tecnologia de gestão de dados 8
2.3.4. Tecnologia de rede e telecomunicações 9
2.3.5. Serviços de Tecnologia / Recursos Humanos 10
2.4. GOVERNANÇA DE TI 10
2.5. GOVERNANÇA NA ADMINISTRAÇÃO PÚBLICA FEDERAL 15
2.6. GOVERNANÇA DE TI NA ADMINISTRAÇÃO PÚBLICA FEDERAL 16
2.6.1. Secretaria De Tecnologia da Informação (STI) 17
2.6.2. Sistema de Administração de Recursos de Tecnologia Da Informação (SISP) 19
2.6.3. Secretaria de Fiscalização da Tecnologia da Informação (SEFTI) 21
3. CENÁRIO DO ESTUDO DE CASO 22
3.1. GERENCIAR A CONTINUIDADE 26
3.1.1. Análise do Impacto do Negócio 28
3.1.2. Análise do risco 29
3.1.3. Estratégia de continuidade do negócio 38
4. RESULTADOS OBTIDOS 44
5. CONCLUSÃO 46
6. REFERÊNCIAS BIBLIOGRÁFICAS 48
A – FORMULÁRIO DE BACKUP 51

Lista de Figuras

Figura 2.1 - Os três papeis fundamentais dos sistemas de informação 6
Figura 2.2 - Componentes de um Sistema de Informação. 7
Figura 2.3 - Influência de TI nos negócios. 11
Figura 2.4 - Desafio da Governança de TI. 12
Figura 2.5 - Motivadores para implantação da governança de TI. 13
Figura 2.6 - Motivadores para implantação da governança de TI. 14
Figura 2.7 - Governança x Gerenciamento. 15
Figura 2.8 - Organograma da STI 18
Figura 3.1 - Eventos e probabilidades de ocorrência. 26
Figura 3.2 - Estágios e atividades da GCSTI. 27

Lista de Tabelas

Tabela 3.1 - Leis e boas práticas referentes a Serviços 23
Tabela 3.2 - Níveis de capacidade do COBIT 5 24
Tabela 3.3 - Implementação simplificada dos processos COBIT 25
Tabela 3.4 - Relação de ativos de TI 28
Tabela 3.5 - Vida útil de ativos de TI segundo a STI. 30
Tabela 3.6 - Mapeamento dos ativos 31
Tabela 3.7 - Avaliação do CPD – Brasília 35
Tabela 3.8 - Avaliação do CPD - Rio de Janeiro 36
Tabela 3.9 - Mídias e tempos de retenção 40
Tabela 3.10 - Categorização de sistemas e serviços. 41
Tabela 4.1 - Equipamentos sem contratos de suporte 44
Tabela 4.2 - Tempo de operação dos ativos 45

1. INTRODUÇÃO

Em um mundo cada vez mais digital, em que os dados e informações propiciam vantagens e oportunidades, os sistemas de informação constituem ferramentas indispensáveis a qualquer organização para a execução de suas atividades, implicando em obtenção de vantagens competitivas, maximização de ganhos e mitigação de riscos.

A Tecnologia da Informação ocupa papel de destaque no dia a dia das empresas, das organizações e do governo. Nesse contexto, o sucesso da aplicação dos sistemas de informação torna-se extremamente dependente do suporte propiciado pela TI, a qual é construída por uma ampla e complexa infraestrutura tecnológica. Tal infraestrutura é composta por diversas tecnologias, como bases de dados, servidores de aplicações, equipamentos de redes e de segurança.

Não bastasse a diversidade de soluções, a cada ano o mercado de tecnologia apresenta novos conceitos e disponibiliza novas ferramentas para a área de TI, como por exemplo as técnicas de virtualização, os serviços em nuvem, contêineres, soluções diversas definidas por *softwares*, enfim, os mais diversos produtos, os quais trazem consigo novas necessidades e desafios como a modernização do parque tecnológico, atualização de conhecimentos e capacidades e novos paradigmas de segurança.

Assim, as integrações tecnológicas de processos através da tecnologia fazem com que o risco que a TI representa para a continuidade do negócio seja altamente visível. Outro ponto de destaque são os custos de manutenção do parque tecnológico, os quais representam uma considerável fatia do orçamento das organizações, tanto na manutenção dos equipamentos como na evolução e substituição dos ativos.

Esse cenário, por si só tão complexo, torna-se ainda mais desafiador quando se trata de fazer TI no âmbito da Administração Pública Federal (APF). O Governo Federal Brasileiro, há vários anos, faz intenso uso de recursos de tecnologia da informação na prestação dos serviços públicos, visando, entre outros resultados, a uma maior participação da sociedade, maior transparência de suas ações e celeridade na execução de suas atividades finalísticas. Nesse sentido, há de se considerar os diversos fatores que norteiam e regulam a atuação dos agentes públicos, como o atendimento aos Acórdãos, Leis, Instruções Normativas e demais regulamentos. Assim, mais do que fazer TI, é necessário fazê-lo respeitando os vários princípios instituídos, como a legalidade e a eficiência.

Dessa forma, no âmbito da Administração Pública Federal é necessário que os órgãos e entidades implantem e executem processos de governança e de gestão de TI, sempre alinhados às leis e aos demais normativos, tendo em vista primordialmente o interesse público.

1.1. OBJETIVO GERAL

O objetivo geral desse trabalho é analisar o cenário de determinado Agência Reguladora, órgão integrante do Sistema de Administração de Recursos de Tecnologia da Informação (SISP), e propor diretrizes, ações e melhorias que propiciem uma gestão mais eficiente da infraestrutura de TI, tendo em vista a continuidade dos serviços de TI.

1.2. OBJETIVOS ESPECÍFICOS

Entre os objetivos específicos encontra-se:

- Levantar e estudar os principais normativos associados à Tecnologia da Informação (TI) emitidos para os órgãos da Administração Pública Federal;
- Levantar e estudar as boas práticas relacionadas;
- Verificar e analisar a infraestrutura de TI da Agência Reguladora, tendo em vista as boas práticas e legislação;
- Propor ações e melhorias na infraestrutura de TI de forma a prover um ambiente resiliente e preparado para sustentar a continuidade dos serviços por ela suportados;
- Fornecer subsídio para o planejamento das respectivas contratações de TI.

1.3. JUSTIFICATIVA

A gestão da continuidade da infraestrutura tecnológica é de extrema importância para as organizações na medida em que ela suporta todos e quaisquer serviços que façam uso dos recursos de TI. Dessa maneira, a gestão da continuidade da infraestrutura de TI está diretamente relacionada à gestão da continuidade dos serviços de TI.

Ao contrário da iniciativa privada, que possui liberdade para investir e manter sua infraestrutura tecnológica da forma que desejar, os atos executados pelos agentes da Administração Pública são vinculados a todo um arcabouço legal, que determina as formas e mecanismos de contratação, os quais restringem e até mesmo vedam a utilização de determinadas tecnologias. Assim, é necessária a utilização não só de *frameworks,* boas práticas e referências técnicas, como também a obediência aos devidos princípios legais.

1.4. METODOLOGIA UTILIZADA

O presente estudo de caso tem como referência a infraestrutura tecnológica de determinada Agência Reguladora, pertencente à APF (Administração Pública Federal) e integrante do SISP (Sistema de Administração de Recursos de Tecnologia da Informação) na condição de órgão seccional.

A metodologia utiliza como base o Quadro de Referência para Gestão de TIC proposto pelo SISP, em específico as definições do aspecto Serviços, no qual são elencados os modelos de boas práticas a serem utilizados como referência pelos órgãos e entidades da APF. Dentre as referências, neste presente trabalho destacam-se o COBIT e o ITIL.

Utilizando-se o COBIT no contexto da Agência, são analisados os níveis de maturidade dos 10 (dez) processos elencados no referido Quadro de Referência para Gestão de TIC. Considerando que a partir do primeiro nível os processos já se encontram implementados e alcançados os seus propósitos, serão abordados apenas os processos incompletos, ou seja, aqueles considerados com nível 0 (zero) de capacidade.

Após a triagem dos processos, será utilizado o ITIL, guia de boas práticas para gestão de serviços de TI, para que se desenvolva o respectivo serviço e o seu gerenciamento. Os preceitos estabelecidos pelos processos serão observados e analisados tendo como referência a realidade da infraestrutura de TI da Agência. Nessa esteira serão consideradas, em conjunto, as Orientações e Instruções Normativas emanadas pela Secretaria de Tecnologia da Informação (STI) do Ministério do Planejamento, Desenvolvimento e Gestão (MP), de forma a se considerar os fundamentos legais, boas práticas, orientações e vedações que

envolvam a gestão da infraestrutura de tecnologia da informação no contexto do Governo Federal.

1.5. ESTRUTURA DA MONOGRAFIA

A primeira parte da monografia discorre sobre a importância dos dados e informações para as organizações, como os sistemas de informação são utilizados para tratar e utilizar essas informações e a dependência cada vez maior dos sistemas de informação com relação à estrutura de Tecnologia da Informação.

São apresentados os componentes principais que compõem a TI e a crescente necessidade de que o uso e os investimentos em tecnologia estejam cada vez mais alinhados aos objetivos estratégicos do negócio. Assim, temos a governança de TI, cuja responsabilidade pertence ao alto escalão da organização e que atua em um nível estratégico – tático. Inserido nesse contexto, há a gestão ou gerenciamento de TI, cuja atuação se dá em um nível operacional.

Considerando o foco do projeto, voltado a tratar a TI dentro do cenário da Administração Pública Federal, são abordadas as iniciativas do Governo Federal com relação ao uso da tecnologia de forma a atender aos cidadãos, levando em conta o interesse público, a economicidade, transparência, entre outros fatores. São definidos os principais Órgãos e Secretarias da estrutura federal que atuam legislando e regulando a atuação dos demais órgãos e entidades com relação ao uso da TI.

Finalmente, é realizada uma análise da infraestrutura de TI de da Agência, responsável por prestar suporte a todos os seus sistemas de informação. A análise é feita com foco na continuidade dos serviços de TI, tendo como base as melhores práticas apresentadas pelo *framework* ITIL e as Leis, Instruções e Acórdãos emitidos sobre os temas. São propostas ações e melhorias de forma a mitigar ou mesmo tratar os pontos que podem provocar a descontinuidade da infraestrutura de TI e respectivamente dos serviços por ela suportados.

2. EMBASAMENTO TEÓRICO SOBRE O TEMA

2.1. DADOS X INFORMAÇÕES

Antes de se falar em Tecnologia da Informação, é importante que se defina a diferença entre dados e informações. Conforme Rossini e Palmisano (2006), dado é o elemento que representa eventos ocorridos na empresa ou circunstâncias físicas, antes que tenham sido organizados ou arranjados de maneira que as pessoas possam entender e usar. Informação é o dado configurado de forma adequada ao entendimento e à utilização pelo ser humano. Já para Laudon e Laudon (2007), informação quer dizer dados apresentados em uma forma significativa e útil para os seres humanos, ao passo que dados, ao contrário, são sequências de fatos ainda não analisados, representativos de eventos que ocorrem nas organizações ou no ambiente físico, antes de terem sido organizados e arranjados de uma forma que as pessoas possam entendê-los e usá-los.

As informações, geradas com a organização e estruturação dos dados, são tidos como um dos principais ativos de qualquer organização. A partir deles é possível obter conhecimentos, fundamentais para a execução de atividades estratégicas, como processos de tomada de decisões, obtenção de vantagens competitivas, entre outros.

2.2. SISTEMAS DE INFORMAÇAO

De forma a suportar a crescente quantidade de dados e informações geradas e disponíveis, é necessária a utilização de meios e recursos que permitam o uso das informações de forma eficiente, eficaz e efetiva, dentro das necessidades, áreas de atuação, portes e complexidades de cada organização.

Nesse contexto, surgem os sistemas de informação. O'Brien (2004) define os três papéis vitais que os sistemas de informação podem exercer em uma empresa:

- Suporte de processos e operações de negócios;
- Suporte de tomada de decisão pelos seus empregados e gerentes;
- Suporte das suas estratégias para vantagem competitiva.

Conforme a Figura 2.1, os papéis fundamentais interagem entre si e a qualquer momento cada um dos processos pode fornecer ou receber dados dos demais. Essa integração, com o consequente fluxo livre de informação, traz flexibilidade e escalabilidade ao negócio.

Segundo O'Brien (2004), um sistema de informação pode ser qualquer combinação organizada de pessoas, *hardware*, *software*, redes de comunicação, recursos de dados e

políticas e procedimentos que armazenam, restauram, transformam e disseminam informações em uma organização.

Figura 2.1 - Os três papeis fundamentais dos sistemas de informação

Fonte: O'Brien (2004)

Há, de fato, um inter-relacionamento entre todos os componentes dentro de um sistema de informação, o que significa que não se trata apenas de recursos tecnológicos, mas também de outros elementos, como o organizacional e humano, que trabalham em conjunto na busca de soluções para os desafios e problemas dos ambientes organizacionais.

Todavia, embora não seja o único elemento, atualmente a tecnologia da informação desempenha um papel crucial no contexto dos sistemas de informação. Considerando-se a enorme quantidade de dados disponíveis e a velocidade cada vez maior com que se espera que as informações sejam obtidas, trabalhadas, utilizadas e disponibilizadas, é inconcebível não se prever a utilização de componentes tecnológicos no contexto dos sistemas de informação.

2.3. TECNOLOGIA DA INFORMAÇÃO

A Figura 2.2 ilustra um modelo conceitual que demonstra os elementos necessários para que um sistema de informação receba recursos (dados) como entrada e os transforme em produtos (informações).

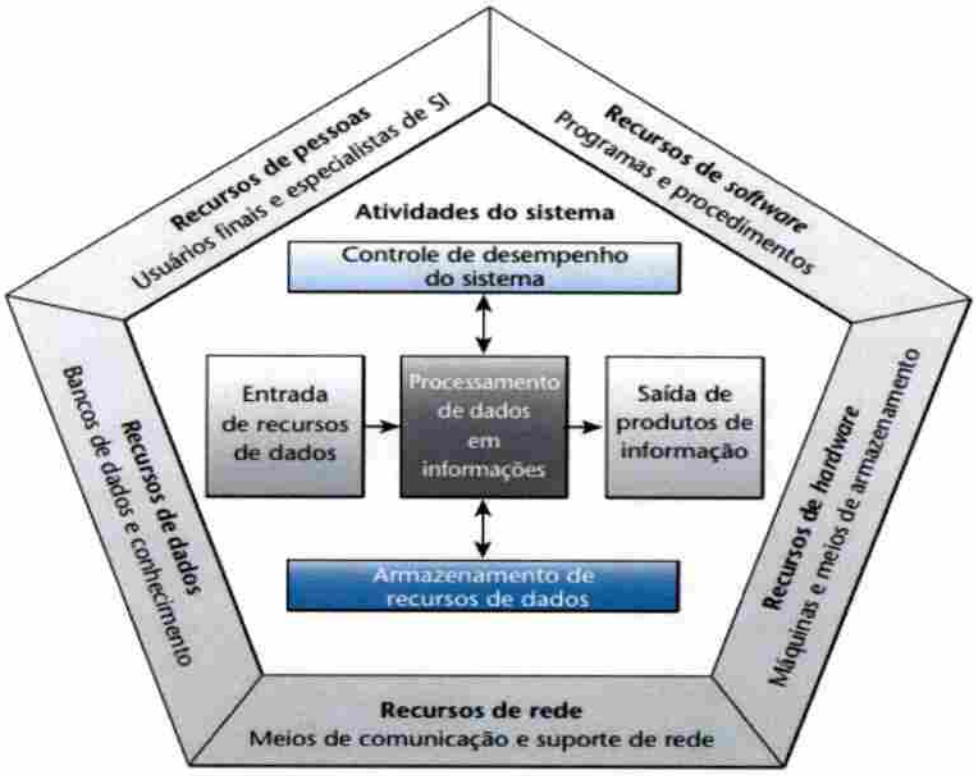

Figura 2.2 - Componentes de um Sistema de Informação.

Fonte: O'Brien (2004)

Para O'Brien (2004), um sistema de informação depende de recursos de pessoas (usuários finais e especialistas de SI), *hardware* (máquinas e meios de armazenamento de dados), *software* (programas e procedimentos), dados (bases de dados e conhecimento) e redes (meios de comunicação e suporte de rede) para realizar a entrada, processamento, saída, armazenamento e para controlar as atividades que convertem os recursos de dados em produtos de informação.

Laudon e Laudon (2007) define o conceito de infraestrutura de tecnologia da informação (TI) como sendo a base, ou plataforma, que sustenta todos os sistemas de informação da empresa, e composta por cinco elementos principais: *hardware*, *software*, tecnologias de gestão de dados, tecnologias de rede e telecomunicações e serviços (pessoas necessárias para operar e gerenciar os outros componentes da infraestrutura de TI).

2.3.1. *Hardware*

Para Laudon e Laudon (2007), o *hardware* consiste na tecnologia para processamento computacional, armazenamento, entrada e saída de dados. Esse componente inclui grandes

mainframes, servidores, computadores de médio porte, computadores pessoais e *laptops*, assistentes digitais pessoais (PDAs) de mão e dispositivos moveis que dão acesso a dados corporativos e à Internet. Inclui, também, equipamentos para reunir e registrar dados, meios físicos para armazenar os dados e dispositivos para a saída da informação processada.

2.3.2. *Software*

De acordo com O'Brien (2004), *software* refere-se a todos os conjuntos de instruções de processamento da informação. Esse conceito genérico de *software* não inclui apenas os conjuntos de instruções operacionais chamados programas, que controlam diretamente o *hardware* do computador, mas também os conjuntos de instruções de processamento de informação denominados procedimentos de que as pessoas necessitam. São exemplos de recursos de *software*:

- *Software* de sistema, como o programa de sistema operacional, o qual controla e suporta as operações de um sistema de computador. Microsoft Windows e Linux são dois exemplos de *softwares* de sistemas.
- *Software* de aplicação, que são programas que orientam o processamento de determinado uso de computadores por usuários finais. Como exemplo, Microsoft Word, Excel, etc.
- Procedimentos, que são instruções de operação para as pessoas que usarão um sistema de informação. Exemplos disso são as instruções para o preenchimento de um formulário ou uso de um pacote de *software*.

2.3.3. Tecnologia de gestão de dados

Para O'Brien (2004), o conceito de dados como um recurso organizacional resultou em várias mudanças na organização moderna. Os dados capturados primeiramente por meio de uma transação comum são agora armazenados, processados e analisados por aplicativos de *software* sofisticados capazes de revelar relações complexas sobre vendas, clientes, concorrentes e mercados.

Os recursos de dados dos sistemas de informação geralmente são organizados, armazenados e acessados por uma variedade de tecnologias gerenciais de recursos de dados em:

- Bancos de dados que armazenam dados processados e organizados.
- Bases que guardam o conhecimento em uma variedade de formas, como fatos, regras e exemplos de casos a respeito de práticas de negócios bem-sucedidas.

Laudon e Laudon (2007) menciona que um sistema de gestão de banco de dados (DBMS – *database management system*) é um *software* específico usado para criar, armazenar, organizar e acessar dados a partir de um banco de dados. O DBMS livra o programador ou usuário final da tarefa de entender onde e como os dados estarão realmente armazenados, separando as visões lógica e física dos dados. A visão lógica apresenta os dados tal como seriam vistos por usuários ou especialistas da empresa, ao passo que a visão física os mostra como estão realmente organizados e estruturados nos meios de armazenamento físico.

2.3.4. Tecnologia de rede e telecomunicações

De acordo com Laudon e Laudon (2007), a tecnologia de rede e telecomunicações proporciona conectividade de dados, voz e vídeo a funcionários, clientes e fornecedores. Isso inclui tecnologia para operar as redes internas da empresa, serviços prestados por companhias telefônicas ou de telecomunicações, e tecnologia para operar *sites* e conectar-se com outros sistemas computacionais por meio da internet.

O'Brien (2004) menciona que as tecnologias de telecomunicações e redes, como internet, intranets e extranets, são essenciais para o êxito de negócios eletrônicos e das operações comerciais eletrônicas de todos os tipos de organizações e de seus sistemas de informação baseados em computador. As redes de telecomunicações são formadas por computadores, processadores de comunicações e outros dispositivos interligados por meios de comunicações e controlados por *softwares* de comunicações.

O conceito de recursos de rede enfatiza que as tecnologias e redes de comunicações são um componente fundamental de todo sistema de informação, e incluem:

- Meios de comunicações: Como cabo paralelo-trançado, cabos coaxiais e de fibra óptica, micro-ondas, celular e tecnologias de satélite.
- Infraestrutura de rede: essa categoria genérica destaca que muitos *hardwares*, *softwares* e tecnologias de dados são necessários para dar suporte a operação e uso de uma rede de comunicações. Exemplos incluem processadores de comunicações, como modems, *switches* e roteadores, além de *software* de controle de comunicações, como sistema operacional de rede e programas navegadores para internet.

2.3.5. Serviços de Tecnologia / Recursos Humanos

As empresas precisam de pessoas para operar e gerenciar os componentes da infraestrutura de TI e também para ensinar os funcionários a usar essas tecnologias em suas atividades diárias.

As pessoas são componentes essenciais para a operação bem-sucedida de todos os sistemas de informação. Os recursos humanos incluem usuários finais e especialistas de Sistemas de Informação (SI).

- Usuários finais (também chamados usuários ou clientes) são as pessoas que usam um sistema de informação ou a informação que este produz. Podem ser consumidores, vendedores, engenheiros, funcionários, contadores ou gerentes, e são encontrados em todos os níveis de uma organização. Na verdade, a maioria de nós é usuária final de sistema de informação, e a maioria dos usuários finais em negócios é composta de trabalhadores do conhecimento, isto é, pessoas que passam a maior parte do seu tempo comunicando e colaborando em equipes e grupos de trabalho, criando, usando e distribuindo informação.
- Especialistas de SI são pessoas que desenvolvem e operam sistemas de informação, o que inclui analistas de sistemas, desenvolvedores de *software*, operadores de sistemas e outras pessoas de SI de cunho gerencial, técnico e administrativo. Em suma, os analistas de sistemas projetam o sistema de informação com base nas exigências de informações de usuários finais; os desenvolvedores de *software* criam programas de computador baseados nas especificações de analistas de sistemas; e os operadores de sistema ajudam a controlar e fazer funcionar grandes sistemas de computador e redes.

2.4. GOVERNANÇA DE TI

Resta claro que os diversos tipos de organizações dependem dos seus sistemas de informação para o alcance de resultados, obtenção de vantagens competitivas, melhoria da gestão interna, entre outros. Os sistemas de informação, por sua vez, são incapazes de atender de forma satisfatória a todos os requisitos e necessidades impostos pelas organizações sem a devida utilização da infraestrutura de tecnologia da informação.

Conforme Fernandes & Abreu (2014), outro ponto a se considerar é que as "ilhas" de sistemas de informação estão terminando. As integrações tecnológicas de processos através da tecnologia da informação (aplicações e infraestrutura computacional e de comunicação

de dados) fazem com que o risco que a TI representa para a continuidade do negócio seja altamente visível. Uma estrutura de TI mal administrada pode permitir a ocorrência de problemas e incidentes, os quais podem provocar uma gama de consequências, como vazamento de informações, perda de dados, indisponibilidades de sistemas, entre outros. Tais situações costumam provocar danos à imagem, credibilidade e reputação das organizações, perdas financeiras e prejuízos de diversos tipos, incorrendo em sanções nas mais diversas esferas, conforme pode ser visto na Figura 2.3.

Empresa	Data	Ocorrência
AT&T	Abril de 1998	Atualização da versão do sistema prevista para ser realizada em 6 horas levou 26 horas. Custo de US$ 40 milhões em descontos nas faturas de serviço devido ao não cumprimento de acordos de nível de serviço celebrados com os seus clientes finais.
eBay	Junho de 1999	Indisponibilidade durante 22 horas devido à falha no sistema. Custo estimado entre US$ 3 e 5 milhões em receitas e declínio de 26% no valor das ações.
Hershey's	Setembro de 1999	Falhas no sistema devido à estratégia de implementação de nova versão. Custo não estimado com o atraso no envio de encomendas, 12% de redução nas vendas do trimestre e diminuição de 19% no lucro líquido do trimestre em relação ao mesmo período do ano anterior.

Figura 2.3 - Influência de TI nos negócios.

Fonte: Filho (2011)

Outro ponto de destaque refere-se aos custos envolvidos nas aquisições e no suporte de todo o parque tecnológico. Os gastos com equipamentos, licenças, *softwares* e suporte constituem boa parte dos orçamentos das empresas, organizações e entidades governamentais. Conforme o site eletrônico http://cio.com.br, "*os gastos com TI no Brasil devem atingir R$ 236,1 bilhões em 2017, um aumento de 2,9% comparado a 2016, de acordo com a última previsão feita pelo Gartner*". Tanto as instituições privadas quanto as públicas realizam altos investimentos, sem utilizar, na maioria das vezes, todo o potencial que a TI pode proporcionar no alcance de seus objetivos.

Dessa forma, considerando os riscos e custos envolvidos que a Tecnologia da Informação constitui para os negócios, o grande desafio das organizações públicas e privadas, conforme Gaseta (2011), é gerenciar adequadamente a estrutura de TI e direcionar os investimentos

em TI de forma adequada, buscando atingir os melhores resultados dos serviços prestados pela TI, por meio de uma Governança de TI bem planejada e implementada, conforme demonstra a Figura 2.4.

Figura 2.4 - Desafio da Governança de TI.

Fonte: Gaseta (2011)

Há várias definições para Governança de TI. Para a ISO/IEC 38500 (ABNT, 2009), a Governança de TI é o sistema pelo qual o uso atual e futuro da TI são dirigidos e controlados. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar planos. Inclui a estratégia e as políticas de uso da TI dentro da organização.

De acordo com Gaseta (2011), a governança de TI é definida como uma estrutura de relacionamento e processos para dirigir e controlar uma organização, afim de atingir os objetivos corporativos, adicionando valor ao negócio e equilibrando os riscos em relação ao retorno do investimento em TI e seus processos. Tais estruturas e processos buscam garantir que a TI contribua para que os objetivos e estratégias da organização assumam seu valor máximo, de forma a controlar a execução e a qualidade dos serviços de TI em benefício da organização.

Conforme cita Fernandes & Abreu (2014), a Governança de TI deve:

- Promover o alinhamento da TI ao negócio, tanto no que diz a aplicações como à infraestrutura de serviços de TI.
- Garantir a continuidade do negócio contra interrupções e falhas.
- Promover o alinhamento da TI a marcos de regulação externos e outras normas.

De forma geral, os principais motivadores para a implantação da governança de TI podem ser vistos na Figura 2.5.

Motivador	Informações	Riscos
Gastos altos com TI.	▪ Desvalorização e desatualização muito rápida de recursos de TI. ▪ Dificuldade de gestão de bens de TI. ▪ Alocação inadequada dos recursos de TI. ▪ Demora no processo de escolha, aquisição e entrega de soluções de TI. ▪ Orçamento de TI insuficiente.	▪ Diminuir lucratividade da organização. ▪ Perda de desempenho das funções de TI e dos negócios da organização.
Desalinhamento entre as necessidades de negócio e a infraestrutura de TI da organização.	▪ Infraestrutura de TI superestimada ou subestimada. ▪ Tempo de implementação das soluções de TI não atinge a expectativa dos usuários das áreas de negócios da organização.	▪ Fluxo de informação truncado devido a processos não implementados por TI. ▪ Falta de alinhamento entre a área de TI e de negócios, proporcionando baixa eficiência operacional.
Decisões de TI tomadas de forma isolada.	▪ Área de TI não é vista na organização como estratégica. ▪ Falta de integração entre as áreas de negócio e a área de TI.	▪ Serviços entregues sem a qualidade desejada. ▪ Desconhecimento das necessidades de novos serviços de TI para atendimento adequado ao negócio.
A segurança da informação não existe ou não é difundida adequadamente na organização.	▪ Indisponibilidade de informação sobre os proprietários dos dados dos sistemas e permissões necessárias para a manipulação dos dados. ▪ Indefinição de uma política de segurança.	▪ Informações podem não ser confiáveis e íntegras, pois não existe controle sobre elas, gerando perdas significativas para a organização. ▪ Perda de credibilidade.
A contratação de serviços de terceiros não atende às necessidades de TI.	▪ Os contratos com terceiros não são firmados de forma adequada, acarretando dificuldade no relacionamento. ▪ A estratégia para a terceirização dos serviços de TI não atende às necessidades dos clientes e dos objetivos de negócio.	▪ Quebra de contrato pode causar interrupção de serviços de TI. ▪ Serviços de TI estratégicos estão sob o controle de terceiros, ocasionando problemas de continuidade dos serviços de TI. ▪ Perda do controle dos serviços de TI.

Figura 2.5 - Motivadores para implantação da governança de TI.

Fonte: Gaseta (2011)

Governar a tecnologia da informação é responsabilidade da alta administração, no tocante à liderança, definição das estruturas organizacionais e processos, de forma a garantir que a TI possa suportar e alavancar as estratégias e objetivos da corporação. Dessa forma, a governança atua no âmbito estratégico da organização.

A Gestão é responsável pelo planejamento, criação, execução e monitoramento das atividades em consonância com a orientação definida pela área de governança afim de atingir

os objetivos corporativos. Em geral, é uma responsabilidade da gerência executiva, sob a liderança do CEO da empresa.

A governança de TI não pode ser dissociada da gestão de TI. De fato, essas duas disciplinas compreendem atividades e estruturas organizacionais diferenciadas, bem como possuem propósitos e objetivos distintos. O COBIT versão 5, framework de governança corporativa de TI, define alguns princípios, entre eles o de "separar a gestão da governança", cada um deles com atividades e objetivos bem específicos. A Figura 2.6 deixa claro essas diferenças, mostrando os objetivos e atividades de cada uma:

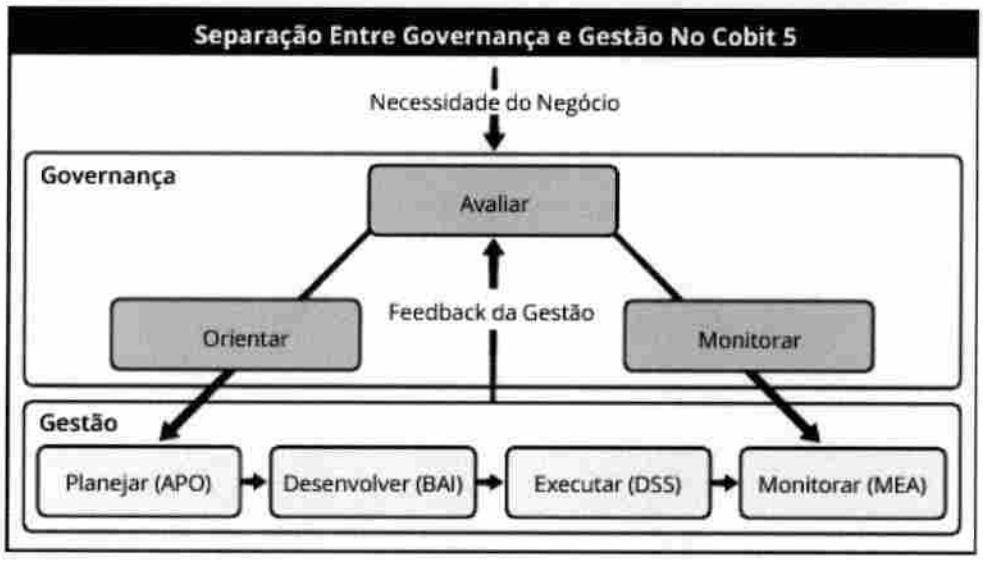

Figura 2.6 - Motivadores para implantação da governança de TI.

Fonte: Reis (2015)

Contudo, a criação de um sistema de governança efetivo requer que as disciplinas de governança e gestão interajam de forma estruturada. A efetividade da governança de TI é mensurada pelo desempenho das atividades de gestão executadas nas áreas tática e operacional, numa relação de *feedback* de gestão. Assim, a governança trabalha dentro de um ciclo, no qual não apenas direciona e alinha as ações de TI, como também recebe indicadores de resultados de processos, produtos e serviços de TI, validando o seu grau de contribuição para os objetivos e estratégias do negócio, como a entrega de benefícios, otimização de custos e riscos. Na Figura 2.7 vemos a relação que temos entre Governança Corporativa, Governança de TI e Gestão de TI.

Figura 2.7 - Governança x Gerenciamento.

Fonte: http://portal.tcu.gov.br/comunidades/governanca-de-ti/entendendo-a-governanca-de-ti/

2.5. GOVERNANÇA NA ADMINISTRAÇÃO PÚBLICA FEDERAL

A Instrução Normativa conjunta MP/CGU 01/2016 conceitua governança no setor público da seguinte forma:

> "Compreende **essencialmente os mecanismos de liderança**, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade. "

Ao contrário das entidades e organizações privadas, cujas ações e princípios de governança se pautam por princípios como ganho de competitividade e maximização dos lucros, as ações do Governo Federal dão maior ênfase a outros princípios e ações, como por exemplo a transparência, *accountability*, economicidade, prestação do serviço público, atendimento aos cidadãos, etc.

O modelo de governança no âmbito da Administração Pública é concretizado e desenvolvido através de todo um arcabouço legal, constituído por um conjunto de instruções normativas, resoluções e legislações específicas. Como exemplo temos a Instrução Normativa Conjunta

MP/CGU 01/2016, a qual, em seu artigo 21, define os princípios de boa governança a serem seguidos pelos órgãos e entidades do Poder Executivo Federal:

- Liderança: deve ser desenvolvida em todos os níveis da administração. As competências e responsabilidades devem estar identificadas para todos os que gerem recursos públicos, de forma a se obter resultados adequados;
- Integridade: tem como base a honestidade e objetividade, elevando os padrões de decência e probidade na gestão dos recursos públicos e das atividades da organização, com reflexo tanto nos processos de tomada de decisão, quanto na qualidade de seus relatórios financeiros e de desempenho;
- Responsabilidade: diz respeito ao zelo que se espera dos agentes de governança na definição de estratégias e na execução de ações para a aplicação de recursos públicos, com vistas ao melhor atendimento dos interesses da sociedade;
- Compromisso: dever de todo o agente público de se vincular, assumir, agir ou decidir pautado em valores éticos que norteiam a relação com os envolvidos na prestação de serviços à sociedade, prática indispensável à implementação da governança;
- Transparência: caracterizada pela possibilidade de acesso a todas as informações relativas à organização pública, sendo um dos requisitos de controle do Estado pela sociedade civil. As informações devem ser completas, precisas e claras para a adequada tomada de decisão das partes interessas na gestão das atividades; e
- *Accountability*: obrigação dos agentes ou organizações que gerenciam recursos públicos de assumir responsabilidades por suas decisões e pela prestação de contas de sua atuação de forma voluntária, assumindo integralmente a consequência de seus atos e omissões.

2.6. GOVERNANÇA DE TI NA ADMINISTRAÇÃO PÚBLICA FEDERAL

O Governo Federal Brasileiro, há bastante tempo, adota intensamente recursos de tecnologia da informação na prestação dos serviços públicos, visando, entre outros resultados, a uma maior participação da sociedade, maior transparência de suas ações e celeridade na execução de suas atividades finalísticas. Dessa forma, no âmbito da Administração Pública Federal (APF), é necessário que as organizações busquem implantar os processos de governança e de gestão de TI que sejam exigidos por leis e demais normativos, de forma a garantir conformidade com o marco regulatório aplicável. Busca-se assim evitar certas situações,

como a priorização de investimentos em TI que não estejam 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, falhas de segurança da informação, entre outros.

Conforme definição do TCU, a governança de TI é a parte da governança corporativa que busca assegurar que o uso da TI agregue valor ao negócio com riscos aceitáveis. Com esse objetivo, a governança de TI tende a evitar ou mitigar deficiências ainda comuns na gestão de uma instituição, como processo de planejamento inadequado, recorrência de projetos malsucedidos e contratações que não alcançam seus objetivos, as quais, no contexto da APF, refletem-se em perda de qualidade e de eficiência de serviços públicos prestados à sociedade.

Na estrutura administrativa federal, são definidos os Órgãos Governantes Superiores de TI (OGS), responsáveis por definir diretrizes, normas, padrões de TI para um segmento específico da APF. Fazem parte dos OGS, entre outros órgãos, a Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão (STI/MP) e o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

2.6.1. Secretaria De Tecnologia da Informação (STI)

A Secretaria de Tecnologia da Informação (STI), pertencente à estrutura do Ministério do Planejamento, Desenvolvimento e Gestão (MP), é o órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Foi criada em dezembro de 2015, a partir da reestruturação dos órgãos internos do Ministério do Planejamento. É sua responsabilidade propor políticas e também planejar, coordenar, supervisionar e orientar normativamente as atividades de gestão dos recursos de tecnologia da informação, governo digital e segurança da informação no âmbito do sistema.

Entre as atividades da secretaria estão a governança e gestão do SISP, padronização e transformação digital dos serviços públicos, acessibilidade digital, abertura de dados, incentivo ao uso de *software* público, manutenção e ampliação da Infovia e a divulgação da Política de Governança Digital a partir da Estratégia de Governança Digital (EGD), documento com validade entre 2016 e 2019.

Para desempenhar suas funções, a STI está estruturada em três departamentos, o Departamento de Governo Digital – DEGDI, Departamento de Governança e Sistemas de

Informação – DEGSI e o Departamento de Infraestrutura de Serviços de Tecnologia da Informação – DEIST, conforme o organograma presente na Figura 2.8:

Figura 2.8 - Organograma da STI

Fonte: Brasil (2016)

O Decreto n.º 8.818 enumera as seguintes competências para os departamentos da Secretaria:

Art. 22. Ao Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação compete:

I - Normatizar, promover e coordenar ações junto aos órgãos do SISP quanto à:

a) infraestrutura de tecnologia da informação e de seus serviços; e

b) definição de processos e procedimentos de contratações de soluções de tecnologia da informação;

II - Gerir a infraestrutura tecnológica da rede de comunicação da administração pública federal; e

III - promover estudos e ações visando a:

a) inovação, interconexão e disponibilização de infraestrutura e de novos serviços de dados, voz e imagem aos órgãos e entidades da administração pública federal; e

b) disseminação da segurança da informação e comunicação no âmbito da administração pública federal.

Art. 23. Ao Departamento de Governança, Sistemas e Inovação compete:

I - Normatizar, promover e coordenar ações junto aos órgãos do SISP quanto a:

a) governança e gestão de tecnologia da informação;

b) inovações e modelos tecnológicos;

c) gestão de pessoas em tecnologia da informação; e

d) sistemas de informação; e

II - Exercer apoio executivo à Comissão de Coordenação do SISP.

Art. 24. Ao Departamento de Governo Digital compete:

I - Coordenar, disciplinar e articular a implantação de ações integradas de governança digital na administração pública federal;

II - Promover e coordenar ações relacionadas à expansão da prestação de serviços públicos por meios digitais na administração pública federal;

III - promover e coordenar ações de sistematização e disponibilização à sociedade de dados e informações relacionados às ações da administração pública federal;

IV - Promover a transparência ativa e a participação da sociedade no ciclo de políticas públicas por meios digitais; e

V - Definir, publicar e disseminar padrões e normas em governo digital e coordenar a sua implementação.

2.6.2. Sistema de Administração de Recursos de Tecnologia Da Informação (SISP)

As ações de Governança de TI no âmbito do Governo Federal Brasileiro são representadas pelo Sistema de Administração de Recursos de Tecnologia de Informação (SISP).

O SISP foi instituído pelo Decreto nº 1.048, de 21 de janeiro de 1994, e atualizado pelo Decreto nº 7.579, de 11 de outubro de 2011 (que revogou o Decreto anterior), com o objetivo de organizar a operação, o controle, a supervisão e a coordenação dos recursos de informação e informática da administração direta, autárquica e fundacional do Poder Executivo Federal. Seu objetivo central é alcançar os objetivos previstos para a área de TI alinhados às ações governamentais, com mais eficiência, eficácia e economicidade no emprego dos recursos públicos previstos para área.

O SISP promove a integração e a articulação entre os programas de governo, projetos e atividades na definição de políticas, diretrizes e normas para a gestão dos recursos de TI. Estimula o uso racional dos recursos de tecnologia da informação, o seu desenvolvimento e aprimoramento, a padronização, a integração, a interoperabilidade, a normalização dos serviços de produção e disseminação de informações, de forma desconcentrada e descentralizada.

Por meio de sua Central de Serviços (C3S), o sistema atua em oito eixos temáticos centrais, sendo eles: governança de TI, padronização tecnológica, *software* público, contratações de TI, serviços de rede, segurança da informação, interoperabilidade e governo eletrônico, além

de realizar o acompanhamento e melhoria da política de gestão de pessoas vinculadas à área de TI.

A estrutura do SISP é composta da seguinte forma:

- Órgão Central: Secretaria de Tecnologia da Informação/MP.
- Comissão de Coordenação: formada pelos representantes dos Órgãos Setoriais, presidida pelo representante do Órgão Central.
- Órgãos Setoriais: representadas por seus titulares, as unidades de administração dos recursos de tecnologia da informação dos Ministérios e dos órgãos da Presidência da República.
- Órgãos Seccionais: representadas por seus titulares, as unidades de administração dos recursos de tecnologia da informação das autarquias e fundações.
- Órgãos Correlatos: representados pelos seus titulares, as unidades desconcentradas e formalmente constituídas de administração dos recursos de tecnologia da informação nos Órgãos Setoriais e Seccionais.

Há um conjunto de instruções normativas, padrões e especificações, emanadas pela STI, com o apoio da Comissão de Coordenação do SISP, que constituem importantes instrumentos para reforçar a Governança de TI nos órgãos setoriais e seccionais do SISP, conforme abaixo:

- Instrução Normativa 04 da SLTI, que define requisitos para contratações de serviços de TI, as quais estão condicionadas à existência de um Plano Diretor de Tecnologia da Informação.
- Metodologia de gerenciamento de projetos do SISP.
- Guia para elaboração do PDTI do SISP.
- Padrões para o Governo Eletrônico como:
    - e-MAG – Modelo de Acessibilidade de Governo Eletrônico.
    - Padrões de Interoperabilidade de Governo Eletrônico.
    - e-PWG – Padrões Web em Governo Eletrônico.
    - Indicadores e Métricas para Avaliação de e-Serviços.
    - Diretrizes para criação de domínios.
    - Guia Livre – Referência de Migração para *Software* Livre

2.6.3. Secretaria de Fiscalização da Tecnologia da Informação (SEFTI)

Um dos papéis atribuídos ao Tribunal de Contas da União (TCU) é o de fiscalizar e normatizar o uso da tecnologia da informação na Administração Pública Federal. Para exercer essa atividade, conta com a Secretaria de Fiscalização da Tecnologia da Informação (SEFTI), à quem, no cumprimento de sua finalidade de fiscalizar a gestão e o uso de recursos de tecnologia da informação pela Administração Pública Federal, compete:

- Realizar fiscalização ou avaliação por meio de acompanhamento, levantamento, inspeção, auditoria ou monitoramento;
- Planejar, coordenar e controlar as fiscalizações relativas à sua área de especialização, inclusive orientando e supervisionando as demais equipes envolvidas;
- Instruir, para apreciação do Tribunal, os processos referentes às fiscalizações sob responsabilidade da secretaria;
- Realizar pesquisas, desenvolver ou disseminar métodos, técnicas e padrões para fiscalização de tecnologia da informação, juntamente com a Secretaria Adjunta de Normas e Procedimentos (Adnor);
- Representar ao relator quando tomar conhecimento de irregularidade ou ilegalidade que possa ocasionar dano ou prejuízo à administração pública;
- Desenvolver outras atividades inerentes à sua finalidade.

A SEFTI coordena a realização de fiscalizações em Governança de TI, nos sistemas informatizados da Administração Pública Federal, nas iniciativas do Governo Eletrônico, na gestão dos recursos de tecnologia da informação, em editais de licitação, em contratos e em processos de aquisições diretas.

3. CENÁRIO DO ESTUDO DE CASO

O estudo de caso em questão refere-se à gestão de infraestrutura de TI no âmbito de uma Agência Reguladora, pertencente à estrutura da Administração Pública Federal. Tal entidade, caracterizada legalmente como Autarquia Especial, se enquadra na condição de órgão seccional do SISP, devendo assim, entre outras obrigações, cumprir e fazer cumprir, por meio de políticas, diretrizes, normas e projetos seccionais, as políticas, diretrizes e normas emanadas do Órgão Setorial do SISP a que está vinculada.

Em sua quase totalidade, os órgãos e entidades do Executivo Federal terceirizam as operações de suas infraestruturas de tecnologia da informação. De fato, essa situação encontra amparo em vários normativos, entre eles o Decreto 2.271/1997, o qual dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional. Já em seu parágrafo 1º do 1º artigo, o Decreto elencou as atividades de informática na relação de serviços que devem ser preferencialmente objetos de execução indireta:

> "Art. 1º No âmbito da Administração Pública Federal direta, autárquica e fundacional poderão ser objeto de execução indireta as atividades materiais acessórias, instrumentais ou complementares aos assuntos que constituem área de competência legal do órgão ou entidade.
>
> § 1º As atividades de conservação, limpeza, segurança, vigilância, transportes, informática (grifo nosso), copeiragem, recepção, reprografia, telecomunicações e manutenção de prédios, equipamentos e instalações serão, de preferência, objeto de execução indireta."

Na esteira da legislação vigente, a Agência terceirizou, através do devido processo licitatório, a operacionalização de sua infraestrutura de TI. Em relação à supervisão da execução dos serviços, o Tribunal de Contas da União estabelece:

> "O exercício dos papéis de planejamento, de definição, de coordenação, de supervisão e de controle das atividades de informática nos órgãos e entidades públicos federais é privativo de seus quadros próprios, nos termos do DL200/67 e dos acórdãos do TCU. Portanto, a Administração deve tomar as providências para assegurar os meios necessários para realizar, de forma independente e competente, o planejamento, a especificação, a supervisão e o controle da execução dos serviços de informática contratados, mediante o preenchimento de cargos."

No âmbito da supervisão e controle da execução dos serviços de TI, diversos processos de gestão de TI foram definidos no Termo de Referência, processos esses alinhados às definições propostas pelo SISP, os quais deveriam ser estabelecidos para subsidiar a governança de TI por parte da entidade e consequente alinhamento às estratégias corporativas estabelecidas pela Alta Administração.

O SISP define diversos aspectos de gestão de TI a serem considerados, referenciando os respectivos normativos, leis e boas práticas aplicáveis.

No total, o SISP aborda 18 aspectos, a saber:

1. Aprendizagem, Conhecimento e Inovação
2. Arquitetura Corporativa
3. Contratações de Soluções de TIC
4. Cultura, Ética e Comportamento
5. Dados e Informação
6. Governo Eletrônico e Digital
7. Infraestrutura de TIC
8. Monitoramento das ações de TIC
9. Orçamento de TIC
10. Pessoas
11. Planejamento de TIC
12. Portfólio, programas e projetos de TIC
13. Processos
14. Qualidade
15. Relacionamentos
16. Segurança da Informação e Comunicações
17. Serviços
18. *Software*

Nesse caso, considerando os conceitos tratados sob o aspecto Serviços, as referências legais e modelos de boas práticas são descritas na Tabela 3.1:

Tabela 3.1 - Leis e boas práticas referentes a Serviços

Fonte: http://www.sisp.gov.br/wikisisp/wiki/quadro_de_referencia_gestaoti

SERVIÇOS	**Legislação e Normas:** Decreto 6.932/2009
	Modelos de boas práticas: ABNT NBR ISO/IEC 20000-1:2011 ABNT NBR ISO/IEC 20000-2:2013 ABNT ISO/IEC TR 20000-3:2011 ABNT ISO/IEC TR 20000-5:2011 COBIT 5 (APO09, BAI04, DSS01, DSS02, DSS03, DSS04, BAI06, BAI07, BAI09, BAI10) Configuration Management Using COBIT 5 CMMI-SRV

	Gespública - Carta de Serviços
	Guia Geral de Serviços - MPS.BR
	Guia de Implementação de Serviços - MPS.BR
	Indicadores e Métricas para Avaliação de e-Serviços
	ISO/IEC TS 15504-8:2012
	ISO/IEC TR 20000-4:2010
	ISO/IEC TR 20000-10:2013
	ISO/IEC TR 90006:2013
	ITIL
	MOF (Microsoft Operations Framework)

Conforme apresenta a Tabela 3.1, a abordagem de gerenciamento de serviços de TI disponibilizada pelo SISP utiliza desde leis e normativos, a um conjunto de boas práticas, guias, normas e frameworks reconhecidos internacionalmente, como é o caso do COBIT 5, ITIL e ISO.

Conforme Fernandes & Abreu (2014), o COBIT 5 adota um modelo de capacidade de processos, em que para cada um de seus processos pode ser realizada uma avaliação para cada um de seus atributos de capacidade. A Tabela 3.2 descreve os seis níveis de capacidade que um processo pode atingir e os atributos de desempenho da capacidade para cada um deles:

Tabela 3.2 - Níveis de capacidade do COBIT 5

Fonte: Fernandes & Abreu (2014)

Nível de Capacidade	Descrição
Nível 0 (Processo incompleto)	O processo não está implementado ou falha no atingimento de seu propósito. Neste nível, há pouca ou nenhuma evidência de qualquer alcance sistemático do propósito do processo.
Nível 1 (Processo executado)	O processo implementado atinge o seu propósito.
Nível 2 (Processo gerenciado)	O processo está implementado de forma gerenciada (planejada, monitorada e ajustada) e seus produtos de trabalho são estabelecidos, controlados e mantidos apropriadamente.
Nível 3 (Processo estabelecido)	O processo está implementado utilizando um processo definido capaz de atingir os seus resultados esperados.

Nível 4 (Processo previsível)	O processo opera dentro de limites definidos para atingir os seus resultados esperados.
Nível 5 (Processo em otimização)	O processo é continuadamente melhorado para atender aos objetivos de negócio atuais e projetos relevantes.

Dos 37 processos apresentados pelo COBIT 5, o quadro de referência de gestão de TI elenca 11 processos para a abordagem de gestão de serviços. Considerando tais processos, foram avaliados os níveis de capacidade para cada um dos processos implementados na Agência. De forma simplificada, foram considerados como implementados os processos que, no mínimo, cumpriam os requisitos para serem categorizados com o nível 1 de capacidade (processos executados). Consequentemente, os processos não implementados foram aqueles que possuíam nível de capacidade 0 (processos incompletos), conforme demonstra a Tabela 3.3:

Tabela 3.3 - Implementação simplificada dos processos COBIT

Processo	Implementado?
APO09 - Gerenciar acordos de serviços	Sim
DSS01 - Gerenciar operações	Sim
DSS02 - Gerenciar requisições de serviços e incidentes	Sim
DSS03 - Gerenciar problemas	Sim
DSS04 - Gerenciar a continuidade	Não
BAI04 - Gerenciar disponibilidade e capacidade	Sim
BAI06 - Gerenciar mudanças	Sim
BAI07 - Gerenciar o aceite e a transição das mudanças	Sim
BAI09 - Gerenciar ativos	Sim
BAI10 - Gerenciar a configuração	Sim

Com o mapeamento dos processos referentes à gestão de serviços de TI, a estratégia adotada foi elevar o nível de capacidade dos processos considerados incompletos para pelo menos o nível 1 de capacidade, de forma que cada um dos processos alcançasse pelo menos seus objetivos, no contexto de um ciclo de melhoria contínua e amadurecimento dos processos. Há uma diferença significativa entre a capacidade de processo nível 1 e os níveis de capacidade mais altos. Conforme estabelece o COBIT 5, o alcance da capacidade de processo nível 1 exige que o atributo de desempenho do processo seja amplamente atingido, o que, de fato, significa que o processo está sendo realizado com sucesso e os resultados esperados estão sendo obtidos pela organização. Neste esquema de avaliação, atingir a capacidade nível 1, mesmo em uma escala de 5, já pode ser considerado uma importante

conquista para a organização. Na prática, cada organização define, com base no custo-benefício e na viabilidade, sua meta ou nível desejado, que muito raramente é um dos mais altos.

Dentre os processos definidos pelo SISP e presentes no Termo de Referência, verificou-se que apenas o processo "Gerenciar a Continuidade" não estava alcançando o seu propósito e dessa forma procedeu-se ao seu estudo e análise diante do cenário da Agência.

3.1. GERENCIAR A CONTINUIDADE

Toda e qualquer organização está sujeita a desastres. As causas de tais ocorrências são as mais variadas possíveis, incluindo desde eventos como incêndios, raios e enchentes até falhas de *software*, falta de energia elétrica, códigos maliciosos, etc. Considerando essas possibilidades, manter um Plano de Continuidade do Negócio é vital para que as organizações consigam reagir e se recuperar diante de situações de desastre. A Figura 3.1 retrata eventos que podem provocar a descontinuidade do negócio e suas probabilidades de ocorrência.

Evento	Percentual
Roubo	36%
Vírus	20%
Ataque de hackers	16%
Falha de hardware e comunicação	11%
Ambiente	7%
Falhas de software	4%
Incêndio/ Enchentes / Força maior	3%
Outros	3%

Figura 3.1 - Eventos e probabilidades de ocorrência.

Fonte: Filho (2011)

Segundo Freitas (2010), continuidade tem a ver com a capacidade da empresa em prever eventos de riscos que possam afetar seriamente o negócio e com a habilidade da empresa em estar preparada para reagir caso esses eventos ocorram.

De acordo com o SISP, continuidade de negócios é a capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

De acordo com o COBIT, o processo Gerenciar a Continuidade visa estabelecer e manter um plano para permitir ao negócio e a TI responder a incidentes e interrupções, a fim de continuar a operação de processos críticos de negócios e serviços de TI necessários e de manter a disponibilidade de informações em um nível aceitável para a organização. Seu objetivo é manter a continuidade da operação de negócios críticos e a disponibilidade da informação a níveis aceitáveis para a organização no evento de uma interrupção

significativa. Para esse processo, o COBIT identifica outros guias relacionados, como o ITIL (gerenciamento de continuidade de serviços de TI).

O Gerenciamento da Continuidade dos Serviços de TI (GCSTI) se enquadra em um cenário maior, o Gerenciamento de Continuidade do Negócio (GCN), sendo um subprocesso deste. De acordo com Filho (2011), o GCN gerencia riscos para assegurar que a organização possa continuar a operar com o nível mínimo especificado em caso de um desastre. O GCSTI é focado nos serviços de TI e assegura que o mínimo de serviços de TI possa ser fornecido no caso de desastre.

O processo de GCSTI pode ser dividido em 4 estágios, a saber:

- Iniciação;
- Requisitos e estratégia;
- Implementação;
- Gerenciamento operacional.

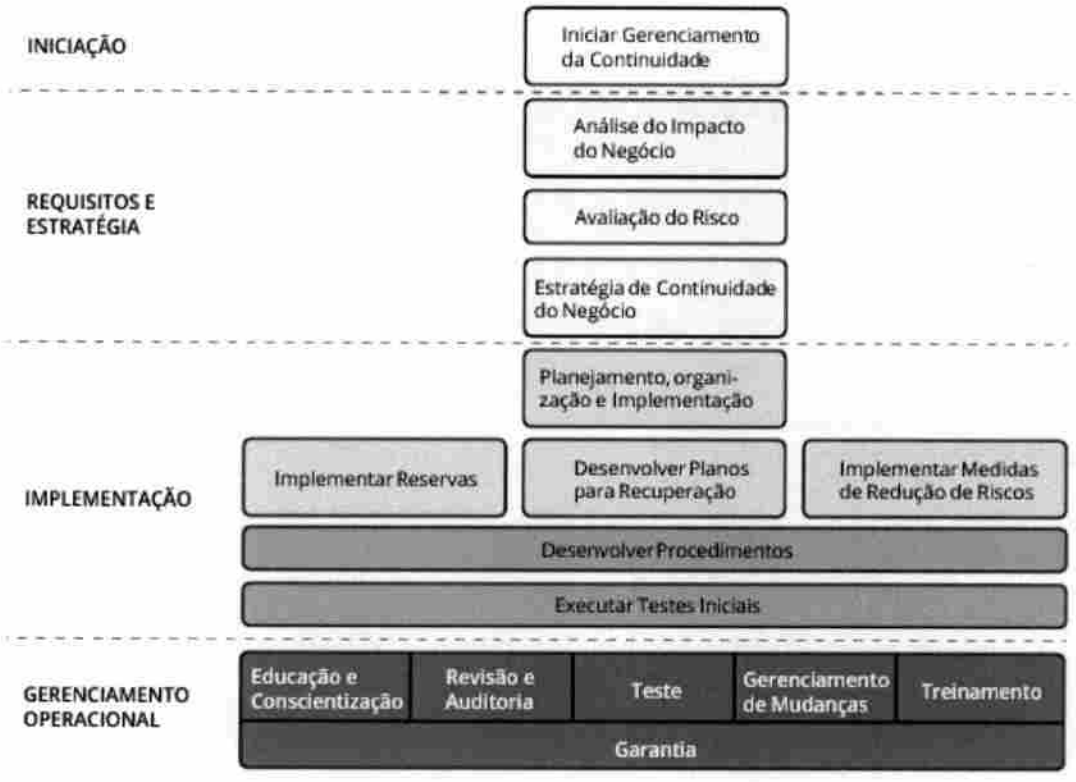

Figura 3.2 - Estágios e atividades da GCSTI.

Fonte: Filho (2011)

O escopo desse estudo de caso restringiu-se a analisar as atividades do estágio "requisitos e estratégia" relacionados com a área de infraestrutura de TI.

3.1.1. Análise do Impacto do Negócio

O objetivo dessa atividade é identificar os serviços críticos ao negócio e os potenciais danos que podem ser causados diante da interrupção desses processos.

Todos e quaisquer serviços viabilizados pela área de TI, sejam críticos à missão do negócio, sejam de suporte às áreas meio, apoiam-se em uma complexa infraestrutura tecnológica composta por elementos computacionais como ativos de redes e telecomunicações, *links* de acesso, sistemas de armazenamento, sistemas de processamento de dados, serviços e aplicações. Dessa forma, a ocorrência de qualquer desastre envolvendo um ou mais desses componentes pode ser extremamente danoso para os sistemas de informação ali hospedados e consequentemente para o negócio. A interrupção em um sistema de armazenamento (*storage*), por exemplo, pode inviabilizar o acesso aos dados da organização, independentemente de todos os demais ativos e recursos estarem operacionais. Percebe-se assim que é fundamental realizar a devida gestão de continuidade de todos os elementos da infraestrutura de TI de forma a permitir a recuperação de sua funcionalidade dentro de prazos aceitáveis para a organização.

No caso da Agência, sua infraestrutura de TI é composta por dois *sites*, localizados em Brasília (DF) e Rio de Janeiro (RJ). Pode-se considerar que a infraestrutura de ambas as localidades é idêntica em termos de equipamentos e capacidades. A Tabela 3.4 descreve os equipamentos e quantidades de ativos por localidade:

Tabela 3.4 - Relação de ativos de TI

Equipamento	Quantidade
Subsistema de armazenamento (*storage*)	1 un.
Chassis de servidores em lâminas	2 un.
Switches SAN	2 un.
Switch Core	1 un.
Switches Topo de *Rack* (ToR)	2 un.

Os eventuais prejuízos e danos causados à Agência diante da indisponibilidade de seus serviços foram mapeados como sendo:

- Prejuízo à imagem da Agência diante da sua função pública de Agente Regulador e Fiscalizador;
- Perdas em sua capacidade de gestão e controle;

- Prejuízos dos entes regulados, sejam pessoas físicas ou jurídicas, diante da dificuldade de se obter autorizações, declarações, etc;
- Suspensão dos serviços para os clientes internos;
- Riscos operacionais para as atividades das áreas finalísticas.

Dessa forma, uma eficiente gestão de continuidade de serviços de TI está intimamente ligada à capacidade de recuperação das funcionalidades da infraestrutura de TI, após qualquer desastre, dentro de prazos aceitáveis pela organização.

3.1.2. Análise do risco

Segundo Filho (2011), essa atividade analisa a probabilidade de ocorrência de um desastre ou outra interrupção séria no serviço. Além de identificar riscos através da análise de vulnerabilidades e ameaças para os ativos críticos, a atividade se propõe a identificar os contra recursos para manter os riscos controlados ou ainda o desenvolvimento de planos de recuperação.

Na análise de riscos da infraestrutura de TI da Agência, foram mapeados dois aspectos de extrema importância para a continuidade da infraestrutura de TI:

- Vida útil dos equipamentos e contratos de suporte;
- Estrutura do Centro de Processamento de Dados (CPD).

É importante para o processo de análise de risco verificar itens como os contratos de suporte dos ativos, assim como a sua vida útil de funcionamento. A garantia e suporte dos equipamentos são fornecidos pelos respectivos fabricantes, considerando as complexidades de suas soluções e arquiteturas tecnológicas e os respectivos níveis de serviços acordados na contratação. Em diversos casos, os fabricantes realizam inclusive uma monitoração proativa de seus equipamentos, possibilitando que, ao se constatar a eminência de algum defeito ou pane, a devida intervenção seja realizada a tempo de se prevenir qualquer incidente. Em caos mais delicados, há até a presença de técnicos residentes dos fabricantes nas instalações dos clientes para permitir uma atuação mais célere diante de qualquer evento.

Estando vigentes as condições de garantia e/ou suporte, os fabricantes podem realizar a troca de *hardwares* defeituosos, atualizações de microcódigos, entre outros, de forma a manter o equipamento atualizado e operacional, dentro dos níveis de serviço estabelecidos nos contratos. De forma a mitigar os riscos de interrupções nos serviços, é extremamente

importante que os equipamentos e soluções de infraestrutura de TI estejam cobertos por condições de garantia e suporte válidos ao longo de suas expectativas de vida.

Nesse sentido, a Secretaria de Tecnologia da Informação, na Portaria nº 20 de 14 de junho de 2016, dispôs sobre as orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional. Em seu anexo Boas práticas, Orientações e Vedações, a Portaria estabeleceu que os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico. De forma a subsidiar os processos de contratação, os itens 1.4.4 e 1.4.5 do anexo definiram os tempos de vida útil mínima a ser considerada para os equipamentos de TI, demonstrados na Tabela 3.5:

Tabela 3.5 - Vida útil de ativos de TI segundo a STI.

Equipamentos	Vida útil
Ativos de rede, tipo equipamentos wi-fi, *switches* de centro e de borda, roteadores, etc.	5 anos
Servidores de rede, aplicação, equipamentos de *backup*, armazenamento, segurança, entre outros.	No mínimo 5 anos

Além de resguardar o ambiente de TI durante sua vida útil, essa medida possui um fator econômico. De forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens manutenidos se tornam obsoletos. Assim, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco do fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

Dessa maneira, é importante que, dentro de um contexto de continuidade dos serviços de TI, sejam observados os requisitos mínimos de vida útil dos equipamentos para o estabelecimento das suas condições de garantia e suporte e planejamento de suas substituições. Falhas em equipamentos críticos não cobertos por essas condições podem

dificultar ou até mesmo inviabilizar o reestabelecimento dos serviços suportados pela TI, vindo a comprometer as funções vitais do negócio.

O parque tecnológico da Agência foi levantado e mapeado. A Tabela 3.6 exibe os equipamentos estruturantes, os tempos de operação, a existência de cobertura de garantia e os riscos para a continuidade do negócio.

Tabela 3.6 - Mapeamento dos ativos

Equipamento	Tempo de operação	Coberto por Garantia	Risco
Switch Core	>5 anos	Não	Alto
Switches SAN	>5 anos	Não	Alto
Servidores	<5 anos	Não	Médio
Storage	<5 anos	Sim	Baixo

O *switch core* é o equipamento responsável por interconectar os equipamentos de acesso aos servidores e demais equipamentos de rede, propiciando acesso às aplicações, intranet, internet, etc. A descontinuidade de operação do *switch core*, ao desempenhar um papel central na estrutura da rede, representa um alto risco ao negócio. Na avaliação, foram identificados dois riscos referentes a esse ativo:

- O equipamento ultrapassou o tempo de vida útil estipulado, assim a probabilidade de ocorrência de danos de *hardware* além de ser bastante significativa, cresce a cada dia, o que pode vir a provocar a interrupção de acesso aos serviços críticos. Além disso, o fato de não haver contrato de suporte é um impeditivo à substituição de qualquer item de *hardware* defeituoso ou à atualização de microcódigo, o que pode inviabilizar a recuperação do equipamento em caso de dano. Assim, a ação a ser tomada nesse caso é a substituição do equipamento por um ativo mais moderno, com condições de garantia e suporte pelo prazo de 60 meses.
- O equipamento, além de obsoleto, não possui redundância e neste cenário o ativo constitui um ponto único de falha dentro da topologia de rede. Dado que a probabilidade de falha simultânea de dois equipamentos é menor do que a probabilidade de falha individual de um dos ativos, o planejamento da aquisição deve prever a aquisição de um equipamento redundante para o *core* da rede. Os equipamentos devem operar, preferencialmente, em modo de alta disponibilidade, propiciando um ambiente tolerante a falhas, cujas ocorrências se tornam

transparentes para os usuários finais na medida em que não há indisponibilidade dos serviços. Essa composição permite que se obtenham outros benefícios, como balanceamento de carga entre os equipamentos, otimizando o tempo de resposta para as requisições dos usuários finais.

Os *switches* SAN (*Storage Area Network*) operam na estrutura das redes de armazenamento, permitindo o acesso dos servidores a um pool compartilhado de armazenamento presente nos *storages*. As redes de armazenamento são projetadas para serem redes de alta performance, operando com baixa latência e sem perda de dados nas transmissões. Neste ambiente, cada servidor acessa a área de armazenamento como se estivesse diretamente conectado a ele.

Com relação à estrutura da Agência, foi identificado que os dois equipamentos trabalham em estrutura de *fabric*, com interligações redundantes tanto para os servidores quanto para o *storage*. Nessa configuração, os riscos de indisponibilidade dos ativos, e consequentemente dos serviços prestados, é mitigado. Assim, para esses ativos não foram identificados outros riscos que senão a falta de contrato de suporte que permita o eventual apoio do fabricante na ocorrência de algum problema.

Os dois chassis de servidores presentes na estrutura da Agência possuem oito lâminas de processamento cada um. Através do uso de técnicas e *softwares* de virtualização, várias máquinas virtuais são disponibilizadas através de cada uma das lâminas, oferecendo diversas vantagens, entre elas:

- Uso mais eficiente dos recursos de *hardware*, como processamento e memória por exemplo;
- Aprovisionamento de aplicativos e recursos de forma mais célere;
- Gerenciamento do parque tecnológico simplificado;
- Continuidade de negócios e recuperação de desastres.

O *software* virtualizador possui funções que permitem que, em caso de falhas nos hosts físicos, as máquinas virtuais (incluindo sistema operacional, aplicações e dados) sejam migradas para outro host físico sem interrupções ou perdas de dados.

Ao mesmo tempo, os dois chassis, que fornecem alimentação elétrica e arrefecimento ao conjunto de lâminas, operam virtualmente como um único ativo, permitindo que na falha de um deles, as máquinas virtuais continuem a operar normalmente sobre as lâminas do outro chassi.

Considerando-se as características e recursos elencados, percebe-se que a Agência possui uma estrutura de processamento de dados robusta e resiliente. Entretanto, a ausência de suporte do fabricante é um risco que merece ser tratado.

Os *storages* são subsistemas de armazenamento de dados, conectados aos servidores através da rede SAN. Os dados são armazenados em estruturas denominadas RAID (*Redundant Array of Independent Disks*). Um RAID é um grupo de discos físicos independentes que fornece alto desempenho, aumentando o número de unidades usadas para salvar e acessar dados. Um subsistema de disco RAID melhora o desempenho de entrada e saída de dados e a disponibilidade de dados. Para os servidores de dados, esses grupos de discos físicos aparecem como uma única unidade de armazenamento ou várias unidades lógicas. Com a utilização dos sistemas RAID é possível melhorar a disponibilidade do armazenamento de dados e a tolerância a falhas.

Há vários tipos de formações RAID, como o RAID 0, no qual os dados são distribuídos entre os discos, o RAID 1, em que os dados são espelhados entre eles, etc. O acesso aos dados presentes nos subsistemas RAID é realizado através de unidades controladoras, as quais, entre outras funções, gerenciam os processos de leitura e escrita nos grupos de discos.

Conforme o levantamento realizado na Agência, o seu subsistema de armazenamento de dados (*storage*) é novo e coberto por condições de suporte e garantia que possibilitam o apoio e atuação do fabricante. Os principais elementos de cada um dos *storages* são redundantes, como as controladoras RAID, as fontes de alimentação, as interfaces de rede, etc. Os discos são agrupados em formação RAID 6, no qual os blocos de dados, assim como dois blocos de paridade, são distribuídos entre os vários discos do grupo. Tal formação oferece proteção contra falhas de até dois discos, além de alto desempenho de leitura, já que os dados são acessados paralelamente em cada um dos discos. Não obstante, o *storage* conta com discos "*hot spare*", os quais, diante dos primeiros indícios de falha em qualquer disco do array, são acionados para a reconstrução do disco e recomposição do grupo. Todos esses recursos tecnológicos fazem com que o *storage* da Agência seja bastante confiável, resiliente e escalável, representando a sua falha, por si só, um baixo risco para a Agência.

Em resumo, as ações levantadas diante da análise de risco da infraestrutura de TI foram a substituição de equipamentos obsoletos, a aquisição de ativos redundantes e a manutenção ou extensão das condições de suporte e garantia. Em todo caso, a Agência deverá observar os dispositivos introduzidos pela Instrução Normativa MP/SLTI Nº 04/2014, a qual dispões sobre as contratações de soluções de Tecnologia da Informação pelos órgãos e entidades integrantes do SISP. O artigo 4º da IN estabelece que as contratações deverão ser precedidas

de planejamento, elaborado em harmonia com o Plano Diretor de Tecnologia da Informação - PDTI. O PDTI, por sua vez, deverá estar alinhado à EGTIC [1](Estratégia Geral de Tecnologia da Informação e Comunicação) e ao plano estratégico institucional e aprovado pelo Comitê de Tecnologia da Informação do órgão ou entidade.

Outro ponto considerado importante na análise do risco foi com relação à estrutura dos Centros de Processamento de Dados (CPD) da Agência. Todos os equipamentos de TI necessitam que condições mínimas sejam fornecidas pelo ambiente em que estão instalados e operando para o seu perfeito funcionamento. Cada ativo estabelece em seu manual, por exemplo, o intervalo de temperatura em que poderá operar sem prejuízo de performance ou até danos ao próprio equipamento.

O superaquecimento pode fazer com que o equipamento desligue automaticamente ou mesmo seja danificado de forma irreversível.

Tensões elétricas de entrada são informadas, assim como a potência nominal de consumo do equipamento para subsidiar a previsão de carga elétrica. Em caso de subtensão o equipamento não consegue operar de forma regular e no caso oposto, sobretensão, podem ocorrer danos aos componentes elétricos das placas e circuitos do dispositivo.

A umidade é igualmente um fator a ser considerado. A baixa umidade do ar pode gerar carga eletrostática, a qual queima os componentes eletrônicos dos equipamentos, ao passo que a alta umidade pode causar a condensação de água.

Além de todas as considerações acima, o ambiente de processamento ainda deve possuir acesso restrito e supervisionado, de forma a evitar roubos, depredações, vandalismos, etc.

De forma geral, o ambiente do centro de processamento de dados, onde estão instalados os equipamentos, deve fornecer:

- Alimentação elétrica através de *nobreaks* e geradores;
- Climatização do ambiente;
- Cabeamento de dados estruturado;
- Links de comunicação;
- Controle de acesso.

---

[1] **EGTIC encontra-se disponível em https://www.governoeletronico.gov.br/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp/estrategia-geral-de-tic**

A infraestrutura dos Centros de Processamento de Dados dos dois *sites* da Agência foi analisada e os resultados levantados nas Tabelas 3.7 e 3.8. A Tabela 3.7 avalia o CPD localizado em Brasília, ao passo que a Tabela 3.8 avalia o CPD localizado no Rio de Janeiro. Em ambas as tabelas são avaliados os itens de estrutura elétrica, climatização, links de comunicação e controle de acesso, bem como as respectivas análises de risco.

Tabela 3.7 - Avaliação do CPD – Brasília

Site: Brasília		
Item avaliado	Resultados	Risco
Estrutura elétrica	Constatou-se que a alimentação elétrica dos equipamentos é realizada por quatro equipamentos *nobreak*, com distribuição da carga elétrica entre eles. Cada *rack* possui pelo menos duas tomadas elétricas, identificadas e conectadas a *nobreaks* distintos. Os circuitos providos por cada *nobreak* são ligados a disjuntores próprios. O consumo de carga elétrica dos *nobreaks* está abaixo dos 40%, o que permite a cada *nobreak* manter o fornecimento elétrico no caso de indisponibilidade de outro aparelho. As manutenções preventivas dos *nobreaks* são realizadas semestralmente e estão em dia. Cada fonte redundante dos ativos de TI está conectada a circuitos distintos de *nobreaks* diferentes em cada rack.	Baixo
Climatização	A climatização do ambiente é realizada por três aparelhos de ar-condicionado, modelo split. Não há formação bem definida de corredores de ar-quente e ar-frio, prejudicando a eficiência energética e de refrigeração. Não há controle de umidade ou de partículas em suspensão.	Médio
Links de comunicação	Cada site possui um *link* próprio de saída de internet. Cada site possui dois *links* de comunicação:	Baixo

	• *Link* MPLS, interconectando todos os pontos de presença da Agência em uma topologia *full mesh*. • *Link* de contingência entre os dois *sites*.	
Controle de acesso	O acesso ao CPD é realizado através de chave física, mantida em claviculário. A guarda da chave do claviculário é mantida pelos colaboradores responsáveis pela área de *Data Center*. Em horário não comercial, o acesso é supervisionado pelos seguranças patrimoniais. Não há sistemas de CFTV ou outros sistemas que permitam registrar imagens do acesso ao ambiente.	Médio

Tabela 3.8 - Avaliação do CPD - Rio de Janeiro

Site: Rio de Janeiro		
Item avaliado	Resultados	Risco
Energia	Idem ao de Brasília.	Baixo
Climatização	A climatização do CPD do RJ é realizada por sistema profissional de refrigeração chiller (com utilização de água gelada) e conta com controle da qualidade do ar e controle de umidade.	Baixo
Links de comunicação	Idem ao de Brasília.	Baixo
Controle de acesso	O acesso ao CPD é realizado através de portas com acesso biométrico (impressão digital), com o registro dos dados do acesso. O ambiente é monitorado por sistema CFTV.	Baixo

Conforme se pode verificar, há diferenças estruturais entre os dois *sites*. O CPD do Rio de Janeiro é mais moderno e está instalado em um ambiente de sala segura, contando com toda uma infraestrutura que falta ao CPD de Brasília. Este localiza-se em um edifício com foco eminentemente empresarial e dessa forma teve que receber adaptações para poder receber os equipamentos.

Como forma de redução das ameaças, optou-se por manter os principais sistemas de produção (servidores de aplicação, bancos de dados, etc.) hospedados no CPD do Rio de Janeiro, ao passo que os sistemas de desenvolvimento, homologação e outros sistemas não críticos de produção foram provisionados em Brasília.

Conforme a IN SLTI/MP 04/2014 estabelece, uma das fases necessárias às contratações de soluções de TI é o planejamento da contratação. Uma subfase do planejamento é o Estudo Técnico Preliminar da Contratação (ETPC), no qual são levantadas as necessidades da contratação, soluções disponíveis, entre outros. Assim, considerando a inviabilidade de reestruturação do CPD de Brasília e o custo total de propriedade dos equipamentos de TI já adquiridos, foram levantadas algumas possibilidades com vistas à maximização das oportunidades e subsídio técnico para a confecção do ETPC:

- Contratação de sala segura;
- *Colocation*

A contratação da sala segura se daria para o aproveitamento de um espaço em prédio próprio da Agência, porém sem a infraestrutura necessária para acomodar os equipamentos de TI. A sala segura consiste em um sistema modular, composto por painéis remontáveis, que propicia a proteção física de equipamentos de *hardware*, formando uma espécie de sala dentro de outra sala, completamente independente da estrutura existente e com sistemas de infraestrutura elétrica, climatização e dados próprios. Apesar de ser uma opção bastante interessante, a STI, em sua publicação Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem, vedou a contratação de salas-cofre e salas seguras por órgãos integrantes do SISP, admitindo, porém, solicitações de excepcionalização. Nesse contexto, caso essa opção seja considerada viável e oportuna, o Departamento de TI da Agência deverá formalizar o pedido de excepcionalização, com as devidas justificativas, à apreciação da STI.

Colocation, também conhecido como *co-location* ou *housing*, é uma modalidade de serviço em que uma organização aluga toda uma infraestrutura de *data center* necessária para a instalação e operação de seus servidores. Ou seja, o equipamento pertence ao cliente, fornecendo o *data center* apenas o espaço onde ele será instalado. Com esse tipo de serviço questões de infraestrutura, disponibilidade, segurança e monitoramento ficam a cargo da empresa contratada, que deve fornecer o serviço dentro de níveis mínimos acordados contratualmente, também conhecidos como SLA (*Service Level Agreement*) ou ANS (Acordo Mínimo de Serviço).

Em ambas as possibilidades, é necessário fazer a previsão de *moving* dos equipamentos. Esse serviço consiste em fazer a realocação de todo o ambiente de servidores e equipamentos para um local alternativo, podendo ser um *data center* comercial (co-location), novo prédio ou filial. Neste serviço são realizadas várias etapas para garantir, entre inúmeras outras coisas, a integridade dos ativos físicos bem como o seu perfeito funcionamento após a mudança.

3.1.3. Estratégia de continuidade do negócio

A partir das análises de impacto no negócio e das análises dos riscos, estabelece-se o Plano Estratégico de Continuidade de Serviços de TI. A estratégia de continuidade deve ser balanceada entre a redução de risco e as políticas de restauração. De fato, a eliminação total dos riscos é impossível e dessa forma deve-se planejar ações que ao menos mitiguem a ocorrência de riscos para a organização.

Conforme já exposto anteriormente, uma estratégia utilizada foi manter os dados críticos de produção no ambiente cuja infraestrutura de TI é mais robusta e resiliente, o que no caso da Agência é o site do Rio de Janeiro. Contudo, conforme já visto, manter os dados críticos em um ambiente único não é recomendável em termos de continuidade de negócios. Nesse sentido, foram abordadas duas ações principais:

- *Backup;*
- Replicação de dados.

O *backup* consiste em uma cópia segura e redundante de dados, de forma a propiciar a sua recuperação diante de um incidente ou desastre. Entre os possíveis incidentes podemos citar as falhas de *hardware*, como discos corrompidos, erros humanos intencionais ou não. Até mesmo ataques cibernéticos podem ser considerados, como por exemplo ataques de *ransonware*, nos quais um código malicioso atua criptografando os dados e tornando-os inacessíveis aos seus usuários. Nesses casos, o atacante geralmente solicita uma quantia em dinheiro para poder liberar a chave a ser utilizada para descriptografar os dados.

Em qualquer desses cenários, uma política de *backup* eficiente é necessária para mitigar os riscos e permitir que os dados sejam recuperados e disponibilizados no menor tempo e com a menor perda possível, de acordo com a sua criticidade para o negócio.

Os backups podem ser realizados em volumes distintos de um mesmo conjunto de discos, em equipamentos específicos de backup (utilizando fitas magnéticas ou discos para o armazenamento das cópias) e até mesmo na nuvem.

Toda política de backup deve se ater a dois parâmetros básicos de backup: RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*). O RTO, objetivo de tempo de recuperação, estabelece o tempo máximo de indisponibilidade dos dados que a organização consegue tolerar. Quanto mais crítico forem os dados, mais rápido deve ser o acesso às cópias de segurança e a disponibilização dos dados. Dessa forma, esse parâmetro pode definir o meio de armazenamento onde o backup será salvo e o tipo de backup adotado. Para dados menos críticos podem ser utilizadas fitas magnéticas, cujo custo financeiro é menor, porém com tempos de escrita e de recuperação mais lentos. Dados com maior criticidade devem ser salvos em discos, os quais são muito mais performáticos que as fitas magnéticas, tanto para a realização do backup quanto para a sua recuperação.

Com relação aos tipos de *backup*, os principais são: *full* (completo), diferencial e incremental. O *backup full* faz uma cópia completa dos dados, geralmente na primeira vez em que os dados são copiados ou no início de cada ciclo de backup. O backup diferencial copia todos os dados novos ou alterados desde o último backup full, ao passo que o incremental copia apenas os dados criados ou modificados a partir do último backup realizado, seja esse um backup *full* ou incremental.

Entre esses modos de *backup* há um *tradeoff* entre capacidade de armazenamento e velocidade de recuperação. Um *backup full* permite uma recuperação mais rápida, ao custo de necessitar de maior espaço de armazenamento. O backup incremental é mais eficiente em questão de ocupação de disco, porém seu processo de recuperação é mais lento. O processo diferencial possui características intermediárias entre o *backup full* e o incremental. Assim sendo, o tipo de *backup* a ser implementado deve ser analisado caso a caso, de acordo com as necessidades e requisitos dos dados e aplicações.

O RPO, objetivo de ponto de recuperação, compreende a quantidade mínima de dados que deve ser restaurada ou a quantidade máxima que pode ser perdida durante a restauração. A partir desse parâmetro é estabelecida a frequência com que o *backup* é realizado. Quanto maior a frequência do *backup*, menor a quantidade de dados perdidos diante de um incidente ou desastre. De maneira geral, a perda máxima de dados compreende o valor dos intervalos de *backup*.

Outro fator extremamente importante com relação ao *backup* é o tempo de retenção. Devido à necessidade de aderência a normas administrativas, a políticas organizacionais e à legislação, certos dados necessitam ser preservados ou retidos por muitos anos até que possam ser descartados. Assim, é fundamental considerar que o tempo de retenção seja considerado e analisado dentro da política de *backup*.

Analisando o cenário da Agência, houve um período de transição entre de um sistema legado de *backup*, baseado em robôs e fitas magnéticas, para um novo sistema, formado por um subsistema de armazenamento em discos (mecanismo principal de *backup*) e um novo robô de *backup* (mecanismo secundário). A nova solução permitiu ganhos notáveis com relação às janelas de tempo de *backup* do sistema legado, reduzindo drasticamente o tempo desprendido para a conclusão das cópias de segurança. Esse cenário propiciou novas oportunidades, tornando possível o *backup* de vários sistemas cuja realização era inviável no antigo sistema.

Com a possibilidade de se realizar o *backup* de um grande volume de dados que até então não eram protegidos, foram estabelecidas duas fases. Na primeira fase, de forma agilizar a realização de um grande volume de cópias, foram definidas premissas gerais para a execução dos backups, conforme a Tabela 3.9:

Tabela 3.9 - Mídias e tempos de retenção

Propósito	**Ambiente**	**Retenção**	
		Disco	**Fita**
Disaster Recovery	Produção	1 mês	-
	Homologação		
	Desenvolvimento		
Arquivamento	Produção	1 ano	10 anos
	Homologação	6 meses	-
	Desenvolvimento	6 meses	-
Backup **Operacional**	Produção	1 ano	5 anos
	Homologação	6 meses	-
	Desenvolvimento	6 meses	-
RPO		24 h	
RTO		24 h	

Para categorizar cada tipo de serviço, foram utilizadas as seguintes definições:

- *Disaster Recovery*: objetiva restaurar um sistema ou servidor após a ocorrência de um desastre.
- Arquivamento: tem o propósito de manter cópias de segurança de arquivos e registros selecionados para preservação permanente ou de longo prazo.

- *Backup* Operacional: objetiva restaurar pequenas quantidades de arquivos e dados que foram corrompidos ou deletados acidentalmente.

A partir dessa definição, cada tipo de serviço ou sistema foi categorizado, de forma a nortear a política de *backup* a ser implementada, vide Tabela 3.10:

Tabela 3.10 - Categorização de sistemas e serviços.

Sistema / Serviço	**Propósito**
Correio Eletrônico	Arquivamento
Banco de Dados	Arquivamento
Máquinas Virtuais.	*Disaster Recovery*
Servidor de Arquivos	*Backup* Operacional
Aplicações (infraestrutura)	*Disaster Recovery*
Aplicações (dados)	Arquivamento
Logs de auditoria	Arquivamento

Também foi definido um modelo de formulário a ser preenchido para os sistemas mapeados, conforme modelo presente no apêndice "A – FORMULÁRIO DE BACKUP".

Na segunda fase foram utilizados os formulários preenchidos anteriormente para que, juntamente com cada uma das áreas responsáveis, fossem realizados os devidos ajustes referentes ao RTO, ao RPO e aos tempos de retenção.

A política de backup estabelecida passou a contemplar, de forma geral, os seguintes aspectos:

- Preenchimento dos formulários de backup para todos os sistemas implementados, de responsabilidade das áreas requisitante e técnica, de forma a subsidiar a implementação do backup.
- Acompanhamento diário da execução das políticas de backup.
- Gerência semanal da capacidade do sistema.
- Testes semestrais de recuperação de dados, alterando os sistemas ao logo dos meses.
- Planejamento e simulações de *"disaster recovery"* anuais para os principais sistemas.

A replicação consiste em criar réplicas dos dados entre servidores paralelos, de forma a permitir que, em caso de falha de um deles, os dados ainda estejam disponíveis em outra instância, de forma que o negócio não deixe de funcionar.

Conforme Santana (2014) existem dois métodos básicos de replicação, o síncrono e assíncrono. Na replicação síncrona, existe a garantia de que qualquer dado presente em um servidor estará necessariamente armazenado no servidor secundário. Isso ocorre porque toda operação de escrita no servidor principal só é confirmada após ter sido gravada no servidor secundário, o qual pode estar até em uma localidade diferente. Todavia, esse método é extremamente dependente das condições da rede entre os *sites*, como largura de banda disponível, latência de transmissão e *jitter* (variação da latência). De forma geral, a utilização desse método entre *sites* distintos só é possível em contextos de redes metropolitanas (MAN), nas quais os requisitos de rede conseguem ser atendidos.

Na replicação assíncrona, o servidor primário retém o dado já salvo e o replica para o servidor secundário em um segundo momento, geralmente a intervalos de tempos regulares. Ao mesmo tempo que esse método alivia o servidor de impactos de performance, a replicação é sempre desatualizada, o que pode resultar em perdas de dados em caso de falha nos *links* entre os *sites*.

Os métodos de replicação garantem maior resiliência a desastres sob o custo de se ter os dados duplicados. Assim, é necessário se aferir o custo-benefício da adoção desse método em termos de capacidade dos dispositivos de armazenamento de dados e da criticidade do sistema.

Além disso, a replicação dos dados não dispensa a realização do backup dos dados. No caso de um eventual incidente, no qual dados de produção sejam sobrescritos erroneamente, tais dados serão replicados entre os servidores, comprometendo a confiabilidade e integridade da informação. Nesse cenário, tão logo seja descoberto o incidente, o procedimento de restauração do backup deve ser acionado, de forma a mitigar os impactos ao negócio.

No caso da Agência, foram levantados os sistemas mais críticos para o seu funcionamento e operação, entre os quais foram elencados o banco de dados Oracle e o sistema SEI. Conforme exposto anteriormente, esses sistemas encontram-se hospedados no site do Rio de Janeiro. Em virtude de os links entre os *sites* não cumprirem os requisitos mínimos necessários para a implementação da replicação síncrona entre eles, optou-se pela replicação assíncrona entre os *sites* do Rio de Janeiro e Brasília, em intervalos regulares de 10 minutos. Além disso, implementou-se o espelhamento dos respectivos dados entre volumes distintos no *storage* do Rio de Janeiro, com a utilização de replicação síncrona. Dessa forma, em caso de uma falha no servidor principal, o serviço pode ser recuperado de forma rápida (*hot standby*). Em situação de desastre completo do site do Rio de Janeiro, os sistemas poderão ser reativados

com uma perda de dados de no máximo 10 minutos, seguindo o padrão de recuperação intermediária ou "*warm standby*".

4. RESULTADOS OBTIDOS

O Estudo de caso analisou a infraestrutura de TI da Agência tendo como referência a gestão de sua continuidade. Foi realizada a análise do impacto que a descontinuidade de qualquer um dos elementos que compõe a infraestrutura de TI representa para o negócio. Na sequência abordou-se a análise dos riscos, aferindo-se as probabilidades de ocorrência de um desastre ou interrupção, as ameaças presentes e as devidas medidas para tratar os riscos e ameaças encontrados. O terceiro passo foi elaborar a estratégia de continuidade do negócio, a qual teve como foco a preservação dos dados e informações armazenados e processados pela infraestrutura tecnológica da Agência.

Entre os resultados encontrados, verificou-se que os principais equipamentos e soluções, em sua maioria, não estavam cobertos por contratos de suporte e garantia dos respectivos fabricantes, conforme pode ser observado na Tabela 4.1.

Tabela 4.1 - Equipamentos sem contratos de suporte

Equipamento	Coberto por Garantia
Switch Core	Não
Switches SAN	Não
Servidores	Não
Storage	Sim

Tal situação consiste em um risco para o negócio, na medida em que a ação dos fabricantes tem importância tanto em caráter proativo quanto reativo. Nas ações proativas os equipamentos são monitorados e, ocorrendo eventos que possam implicar na sua descontinuidade, há a atuação do fabricante de forma a impedir que esse cenário se concretize, quer seja com a troca de componentes, com a atualização de microcódigos, *softwares* etc. Na execução de medidas reativas, ou seja, nas quais já existe uma situação de descontinuidade, a atuação do fabricante é fundamental e importante para que se acelere a recuperação e restauração dos serviços, de acordo com os níveis mínimos de serviço estabelecidos e com o grau de severidade da solução.

Outro resultado observado foi relacionado à vida útil dos principais ativos da infraestrutura. Constatou-se que a maioria já havia ultrapassado o tempo estabelecido como referência de vida útil pela STI, conforme a Tabela 4.2.

Tabela 4.2 - Tempo de operação dos ativos

Equipamento	Tempo de operação
Switch Core	>5 anos
Switches SAN	>5 anos
Servidores	<5 anos
Storage	<5 anos

O risco apresentado por essa situação refere-se à maior probabilidade de falhas físicas, considerando-se que tais equipamentos operam em regime de 24 horas por dia, 7 dias por semana, aumentando assim o risco de descontinuidade. Além disso, há outras questões referentes a desempenho, com o surgimento de novas tecnologias e necessidades de soluções, bem como de segurança, já que após determinado prazo os fabricantes não mais atualizam os códigos dos equipamentos considerados legados, aumentando assim o risco de que vulnerabilidades sejam exploradas e comprometam a continuidade dos serviços.

Finalmente, verificou-se que a estrutura física do Centro de Processamento de Dados de Brasília não cumpria todos os requisitos necessários para atender de forma plena as necessidades de alimentação elétrica, climatização, entre outros fatores, dos equipamentos ali instalados.

Como resultados esperados desse estudo estão a atualização e modernização do parque tecnológico da Agência, com condições de suporte e garantia de pelo menos 60 (sessenta) meses, bem como o devido planejamento da substituição das soluções de acordo com as respectivas expectativas de vida útil. É esperado também que as estratégias de continuidade de negócio, com as devidas implementações das políticas de backup e da replicação dos dados, permitam à Agência se tornar resiliente à perda ou a modificação dos dados, sejam intencionais ou não. Enfim, todas as ações propostas convergem para o objetivo de se garantir a continuidade do ambiente tecnológico e, consequentemente, se garantir a continuidade dos serviços de TI, sempre observando o contexto de governança e gestão de TI da Agência.

5. CONCLUSÃO

A infraestrutura de TI, composta por sistemas de processamento e armazenamento de dados, estruturas de redes e telecomunicações, aplicações e *softwares* constitui elemento fundamental na estrutura de qualquer organização, seja ela privada ou pública. A sua utilização, cada vez maior, faz com que essa infraestrutura se torne um elemento estratégico, considerando que existe uma crescente e inegável dependência com relação ao seu uso. Como toda evolução, a tecnológica não pode ser desprezada, devendo ser assim devidamente governada, em alinhamento aos objetivos de negócio, agregando valor a ele e maximizando as suas oportunidades e mitigando seus riscos.

Nesse contexto, garantir a continuidade dos serviços de TI tem se tornado uma necessidade e não apenas um luxo. No estudo em questão, percebemos como a continuidade da infraestrutura de TI constitui elemento basilar para a continuidade da prestação de todos os serviços que dependem desses recursos. Por serem elementos vitais no complexo conjunto que compõe o parque tecnológico, cada elemento deve ser avaliado em termos dos eventuais impactos causados por sua descontinuidade, dos riscos ao negócio diante dessa situação e, consequentemente, traçadas as devidas estratégias de continuidade.

Na Administração Pública não é diferente e a Tecnologia da Informação tem sido uma ferramenta fundamental na publicidade das ações governamentais, nas iniciativas de transparência, na prestação de serviços públicos, bem como no atendimento das necessidades e interesses da população. Nessa esfera, é necessário observar um conjunto de Leis, Instruções Normativas, Acórdãos e Regulamentos que regem os órgãos e entidades com relação ao devido uso da TI no ambiente do serviço público.

O Governo Federal já se posicionou favoravelmente à adoção do modelo de computação em nuvem, publicando o documento "Boas práticas, orientações e vedações para contratação de Serviços de Computação", vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, documento este com força normativa legal. Tal modelo permite o acesso a recursos computacionais compartilhados em um ambiente de alta disponibilidade e acessibilidade, trazendo uma série de benefícios. A tendência é que os Órgãos Federais passem a fazer uso cada vez maior dos recursos disponibilizados na nuvem, reduzindo assim as suas infraestruturas locais de TI. Todavia, independentemente do cenário de computação utilizado, seja em nuvem, seja em uma infraestrutura própria, sempre se deve analisar os riscos da descontinuidade dos serviços e infraestrutura de TI. Igualmente importante e necessário é estabelecer estratégias para agir pronta e adequadamente diante de desastres e

eventos que possam provocar a descontinuidade da TI, de forma que se consiga retornar os serviços no menor tempo possível e com o menor esforço necessário.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Brasil. Decreto n.º 8.818, de 21 de julho de 2016. Diário Oficial da União, 22 julho 2016.

Brasil. Decreto-Lei nº 200, de 25 de fevereiro de 1967. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Presidência da República, 1967

Brasil. Ministério do Planejamento, Desenvolvimento e Gestão. Portaria nº 20, de 14 de junho de 2016 / Ministério do Planejamento, Desenvolvimento e Gestão, Secretaria de Tecnologia da Informação. -- Brasília: MP, 2016.

Brasil. Ministério do Planejamento, Orçamento e Gestão. Planejamento Estratégico da Secretaria de Tecnologia da Informação 2016 – 2019 / Ministério do Planejamento, Orçamento e Gestão, Secretaria de Tecnologia da Informação. -- Brasília: MP, 2016.

Brasil. Tribunal de Contas da União. Acórdão 1.145/2011-TCU-Plenário.

Brasil. Tribunal de Contas da União. Organização do sistema de governança de tecnologia da Informação (TI): Nota Técnica 7/2014 Sefti/TCU / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2015

Brasil. Ministério do Planejamento, Desenvolvimento e Gestão; Controladoria Geral da União. Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio 2016 – Brasília MP/CGU, 2016.

Brasil. Tribunal de Contas da União. Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública / Tribunal de Contas da União. Versão 2 - Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014.

Fernandes, Aguinaldo Aragon; Fernandes, Vladimir Ferraz de Abreu. (2014). Implantando a governança de TI: da estratégia à gestão dos processos e serviços. 4 ed. Rio de Janeiro: Brasport.

Filho, Felício Cestari. (2011). Gerenciamento de Serviços de TI. Rio de Janeiro: RNP/ESR.

Freitas, Marcos André Dos Santos. (2010). Fundamentos do Gerenciamento de serviços de TI: preparatório para a certificação ITIL V3 Foundation. Rio de Janeiro: Brasport.

Gaseta, Edson Roberto. (2011). Fundamentos de Governança de TI. Rio de Janeiro: RNP/ESR.

Laudon, K.; Laudon, J. (2007). Sistemas de informação gerenciais. 7 ed. São Paulo: Pearson Prentice Hall.

O'Brien, J. (2004) Sistemas de informação e as decisões gerenciais na era da internet. 2 ed.

São Paulo: Saraiva.

Reis, Luiz Claudio Diogo. (2015). Fundamentos do COBIT 5. Rio de Janeiro: RNP/ESR.

Rosini, Alessandro Marco; Palmisano, Ângelo. (2006). Administração de Sistema de Informação e a Gestão do Conhecimento. São Paulo:Pioneira Thomson Learning.

Santana, Gustavo Alessandro Andrade. (2014). Data Center Virtualization Fundamentals. Indianapolis, IN: Cisco Press.

WEB:

http://cio.com.br/noticias/2016/10/26/gastos-com-ti-no-brasil-devem-atingir-r-236-1-bilhoes-em-2017/ (acessado em 10/03/2017).

http://www.datacenterdynamics.com.br/focus/archive/2016/06/o-data-center-e-import%C3%A2ncia-da-climatiza%C3%A7%C3%A3o (acessado em 14/04/2017).

https://www.governoeletronico.gov.br/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp/seguranca-da-informacao/conceitos-e-definicoes (acessado em 05/04/2017).

http://portal.tcu.gov.br/comunidades/governanca-de-ti/entendendo-a-governanca-de-ti/ (acessado em 10/03/2017).

http://www.vert.com.br/blog-vert/por-que-investir-em-colocation-para-expandir-seu-data-center/ (acessado em 17/04/2017).

http://www.vmware.com/br/solutions/virtualization.html (acessado em 10/04/2017).

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/ebook/gated-vmw-ebook-virtualization-essentials.pdf (acessado em 10/04/2017).

APÊNDICES

A – FORMULÁRIO DE BACKUP

Modelo de formulário desenvolvido para levantamento de requisitos de backup.

Serviço/Sistema:

Versão: Data da solicitação: 09/05/2017

Responsáveis pelo Serviço/Sistema

Equipe Responsável (ANAC):

Equipe responsável (Terceirizada):

Documentos de referência:
(Link, Manuais, etc.)

Ambiente:	Selecionar ou digitar...		
Finalidade:	Disaster Recovery		
Hostname:		Endereço IP:	
Sistema Operacional:	Windows Server 2012	Tipo:	○ Físico ◉ Virtual

Itens para backup no host

Tipo do item	Caminho *(Diretório/arquivos/Database/etc)*
Diretório/Arquivo	

Especificar exclusões: (exemplo: *.tmp; *.log)	N/D				
Janela desejável para realizar o backup	Início:	00:00:00	**Volume de dados**	Inicial:	1 GB
	Fim:	01:00:00		Previsão Cresc./Mensal:	100 MB
Procedimento/Script Pré-Backup:	N/D				
Procedimento/Script Pós-Backup:	N/D				

Requisitos de Negócio do Backup

Tempo Retenção - Disco: ○ Dias ○ Semanas ○ Meses ○ Anos ○ Ver informações adicionais

Tempo Retenção - Fita: ○ Dias ○ Semanas ○ Meses ○ Anos ○ Ver informações adicionais

RPO - Recovery Point Objective: h Recovery Time Objective: h

Mídia Armazenamento: Disco Guarda Fitas:

☐ Replicação entre Sites Sentido da replicação: ○ DF -> RJ ○ RJ -> DF

Especificações do backup - Preenchimento pelo especialista

Nome do especialista

Localidade: RJ - Rio de Janeiro Modalidade: BK - Backup

Mídia: DD - Data Domain Ambiente: Selecionar...

Host	Objeto do backup	Caminho do objeto
	Selecionar...	

Tipo	Frequência	
Selecionar...	DIA - Diário	☐ Dom ☐ Seg ☐ Ter ☐ Qua ☐ Qui ☐ Sex ☐ Sab

Grupo Schedule: Selecionar ou digitar...

Hora prevista de início Retenção: Selecionar... Pool