FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da informação

Luiz Carlos Botelho Junior

Computação em nuvem:

Desenvolvimento e aplicação de método de avaliação para migração de serviços em nuvem

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Luiz Carlos Botelho Junior

Computação em nuvem:

Desenvolvimento e aplicação de método de avaliação para migração de serviços em nuvem

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. (o) Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

B672c BOTELHO JUNIOR, Luiz Carlos

Computação em nuvem: desenvolvimento e aplicação de método de avaliação para migração de serviços em nuvem. / Luiz Carlos Botelho Junior. – Americana: 2016.

55f.

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Profa. Esp. Edson Roberto Gaseta

1. Computação em nuvens I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518

Luiz Carlos Botelho Junior

DESENVOLVIMENTO E MÉTODOS DE APLICAÇÃO DE AVALIAÇÃO PARA MIGRAÇÃO DE SERVIÇOS EM NUVEM

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 05 de Dezembro de 2016.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Fatec Americana

Eduardo Antônio Vicentini (Membro)
Mestre
Fatec Americana

Diogo Robles (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus por me proporcionar tamanha oportunidade de grandes aprendizagens, conquistas e crescimento pessoal.

Agradecer a minha noiva Mirelle Nayara por todo o apoio durante o período do curso. A sua paciência, sabedoria e todo seu esforço em me dar o devido suporte quando necessitava.

A toda a minha família que esteve me mantendo de pé através de seu apoio silencioso.

Ao meu orientador Edson Roberto Gaseta que através de seu respeito e apoio, veio a me auxiliar e participou de cada passo no desenvolvimento deste trabalho, contribuindo com suas ideias e opiniões, pela sua experiência e conhecimento que me incentivou a concluir este trabalho da melhor maneira.

A todos os amigos de classe que me acompanharam nesta jornada, me dando puxões de orelhas quando necessário, mas também me doando um pouco de suas forças para a finalização do trabalho de fato acontecer.

A todos os professores que de alguma maneira ou outra me ajudaram, passando experiências e conhecimentos acadêmicos de forma única e proveitosa.

O meu muito obrigado a cada um que fez de mim uma pessoa academicamente melhor e que igualmente impactou minha vida pessoal.

DEDICATÓRIA

Ao meu Deus que me deu tudo o necessário para que eu pudesse, através de meu esforço, conquistar o que eu até aqui conquistei.

RESUMO

O presente trabalho conceitua pontos importantes para a síntese de um novo método que tem como objetivo avaliar se uma organização está pronta ou não para adotar os serviços em nuvem como parte ou todo modelo de serviços da organização. Através desse trabalho é possível entender os pontos que devem ser analisados para que de fato a organização possa se sentir apta a realizar a migração. A análise é feita baseando-se em requisitos que são diretamente extraídos dos conceitos de funcionamento dos modelos de serviços em nuvem e seus modelos de implantações, bem como do framework COBIT de versão de número 4.1, a ISO 27001:2006 e a Governança de TI. Divido em 3 partes, entre o método principal, processo de controle do Cobit DS5 – Assegurando a segurança dos serviços e o processo de controle PO9 – Avaliar e Gerenciar os riscos de T.I., o método é posto em uma tabela e com base nos requisitos, tanto quanto nos objetivos de controles de cada um dos dois processos do Cobit, foram desenvolvidas questões que, quando respondidas, expõe como resultado o questionamento objetivo do método, que é ou não a possibilidade de migração para qualquer um dos modelos de serviços em nuvem existente. Ao final poderá se observar uma aplicação pratica do método, que fora feita em uma instituição de ensino superior, bem como os dados de resposta e seu nível de maturidade correspondente aos dois processos do Cobit que compõe o método.

Palavras Chave: Computação em nuvem; Governança de T.I.; Segurança da Informação.

ABSTRACT

The present work conceptualizes important points for the synthesis of a new method that aims to evaluate if an organization is ready or not to adopt the cloud services as part or all service model of the organization. Through this work it is possible to understand the points that must be analyzed so that the organization may feel able to carry out the migration. The analysis is based on requirements that are directly extracted from the working concepts of the cloud service models and their deployment models, as well as the COBIT version 4.1 framework, ISO 27001: 2006 and IT governance. Divided into 3 parts, between the main method, the control process of the Cobit DS5 - Ensuring the security of the services and the control process PO9 - Evaluate and Manage the IT risks, the method is put in a table and based on the requirements, As well as in the control objectives of each of the two Cobit processes, questions were developed that, when answered, expose as a result the objective questioning of the method, which is or is not the possibility of migration to any of the existing cloud service models . In the end, a practical application of the method that was done in a higher education institution, as well as the response data and its maturity level corresponding to the two Cobit processes that make up the method can be observed.

Keywords: Cloud computing; IT Governance.; Information Security.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Como grande solução para as organizações nos dias de hoje destaca-se a computação em nuvem, que carrega consigo um modelo de serviços variados e moldado de acordo com as necessidades de cada organização.

Com o aumento considerável das organizações que utilizam sistemas e ferramentas que estão disponíveis na WEB, bem como ferramentas e sistemas que mesmo estando em algum servidor dentro da empresa também pode ser encontrada na WEB, faz assim com que as organizações passem a repensar seu modelo de realizar seu trabalho interno ou externo.

Segundo Veras (2016, p. 8):

> [...] Organizações, em sua grande maioria, possuem um legado, um conjunto de aplicativos que se comunicam de forma precária e dados duplicados. Romper com este passado é um ato de inteligência, mas na maioria dos casos não é uma tarefa trivial, pois a organização está em pleno funcionamento e qualquer migração de sistema ou mesmo atualização pode ser motivo para haver perda de dados e downtime dos aplicativos [...] A infraestrutura, por sua vez, precisa ser repensada, pois com aplicativos construídos para serem acessados por usuários que estão em qualquer lugar do mundo, a infraestrutura baseada em acesso quase que exclusivamente local não serve mais.

Sendo assim, entende-se que a possível migração para o serviço de nuvem deve ser feita através de um planejamento e análise do impacto que pode ocasionar à organização, podendo ser ele benéfico ou não. Alguns dos pontos importantes que uma organização deve saber é que mesmo que seus serviços não estejam mais sendo executados dentro de seu espaço físico, estes necessitam de uma gestão, já que o mesmo gera dados e informações.

Taurion (2009, p.58) afirma que “A adoção de uma nova tecnologia deve estar plenamente sincronizada com os objetivos estratégicos da empresa. [...] Claro que existem riscos e muitas vezes tecnologias que parecem promissoras se desvanecem rapidamente”.

Como objetivo geral, foi desenvolvido um método de migração que entregue como resultado se a organização está apta ou não para ir para algum serviço em nuvem.

O objetivo específico do desenvolvimento e aplicação do método é integrar conceitos importantes como, governança de T.I., aplicando através do framework Cobit 4.1, versão esta escolhida por conta de sua ainda grande utilização no mercado por parte de auditores e organizações, apoiando-se também a ISO 27001:2006. O método carrega consigo requisitos extraídos tanto da computação em nuvem e seus modelos de serviço, como também de dois processos do Cobit 4.1.

O trabalho foi estruturado em 7 capítulos, sendo que o primeiro uma breve introdução sobre o trabalho.

O segundo capitulo teve como objetivo conceituar o que é informação e seu valor para organização.

No terceiro capitulo é conceituado a governança de T.I., bem como o framework Cobit 4.1 atrelado a ISO 27001:2006, que serve como objeto de aplicação e maior entendimento da importância da governança de T.I.

No quarto capitulo é apresentada a conceituação da computação em nuvem, abordando suas principais características, seus modelos de serviços e modelos de implantação. Neste capitulo também é possível observar alguns benefícios.

No quinto capitulo tem-se a explicação do desenvolvimento do método, bem como todo material que o mesmo traz, extraído a partir dos conceitos anteriormente abordados.

No sexto capitulo é apresentado o estudo de caso que possui a aplicabilidade do método, bem como os resultados extraídos após ser aplicado.

As considerações finais sobre a elaboração do trabalho estarão no sétimo capitulo.

2 INFORMAÇÃO

A informação nos dias de hoje é de vital importância para qualquer organização e seu negócio. Com o crescimento das tecnologias atuais e surgimento de novas e a necessidade do aumento na velocidade de implementar soluções ágeis, fica de forma muito clara o quão importante é saber manusear a informação e tirar dela o seu melhor.

A informação é um elemento crucial não só para a sobrevivência, mas também para sua habilidade de progressão. Com isto, as organizações arquitetaram políticas, normas, procedimentos e processos afim de orientar as ações no sentido de amparar a Segurança da informação. (ARAUJO, 2015, p.03)

Sendo assim a informação é encarada atualmente, e não poderia ser diferente, como um dos recursos mais importantes de uma organização, contribuindo decisivamente para a sua maior ou menor competitividade. De facto, com o aumento da concorrência tornou-se vital melhorar as capacidades de decisão a todos os níveis.

Segundo a ISO/IEC 27001:2006 (2006), um dado não possui um valor antes do mesmo ser processado devidamente, e somente após ser processado gera a informação. Logo, um conjunto de dados processados é uma informação. Sendo assim o dado não pode gerar conhecimento até que ele sofra o processamento que irá gerar a informação e assim o conhecimento.

Ainda segundo a ISO/IEC 27001:2006 (2006), a informação tem o mesmo valor de importância como qualquer outro ativo importante e é imprescindível que a mesma seja devidamente protegida, pois é essencial para o negócio da organização. Considera-se o ativo de informação como sendo um dos recursos mais importantes de uma organização, e a mesma pode elevar ou diminuir a competitividade da organização.

2.1 INFORMAÇÃO PARA A ORGANIZAÇÃO

Para um melhor manuseio da informação que circula dentro da empresa e está alocada dentro dela é necessária uma melhor classificação de importância e uma segurança trabalhada sobre esta mesma classificação.

Freitas (2006) diz que é necessário conhecer o negócio da organização, compreender seus processos e atividades realizadas e, a partir deste momento, iniciar a sua classificação, estabelecendo algumas definições como:

- **Classificação:** atividade pela qual a atribuirá o grau de sigilo as informações, sejam meios magnéticos, impressos e etc.;
- **Proprietário:** profissional de uma determinada área responsável pelos ativos de informação da organização;
- **Custodiante:** profissional responsável por assegurar que as informações estão de acordo com o estabelecido pelo proprietário da informação;
- **Criptografia:** codificação que permite proteger documentos contra acessos e/ou alterações indevidas;
- **Perfil de acesso:** Definições de direitos de acesso as informações, transações, em meios magnéticos ou impressos de acordo com a necessidade de uso de cada usuário.

De acordo com Araújo (2015) após os critérios de informações estarem adequadamente definidos e implementados, deverá ser determinada a classificação que será utilizada e os controles de segurança adequada. Deverá ser levada em conta fatores especiais, incluindo exigências legais. A classificação deve ser de fácil compreensão de modo que a diferenciação entre as mesmas não seja de forma alguma excessivas.

Araújo (2015) salienta que três níveis podem ser suficientes para uma boa pratica de classificação da informação:

- **Classe 1: Informação Pública**

São informações que qualquer colaborador pode ter o acesso, ou seja, não possui nenhum tipo de sigilo. Assim sendo não se é investido em recursos de proteção nas mesmas. Caso informações caracterizadas desta forma, publica, forem divulgadas não trarão impactos para o negócio ou para a empresa.

Exemplos: Demonstrações financeiras quando publicadas em algum jornal são públicas, porem quando ainda dentro do setor financeiro são confidenciais.

- **Classe 2: Informação Interna**

São informações que os acessos externos devem ser evitados, porém quanto aos dados se tornarem públicos, não acaba se convertendo em um nível de criticidade a organização. Neste modelo de classe a integridade dos dados é importante a nível vital.

Exemplos: Valores de benefícios pagos a seus funcionários são de níveis internos, porém quando divulgados de forma a se tornar um dado conhecido exteriormente, não traz riscos a organização.

- **Classe 3: Informação Confidencial**

São informações que devem possuir acesso restrito internamente e quando esta for, de alguma forma exteriorizada, a organização corre um risco grande de comprometimento das operações, podendo causar perdas financeiras e também de competitividade.

Exemplo: Dados pessoais de clientes ou estratégias de mercados, quando vazadas exteriormente o nível de criticidade é máximo.

2.2 SEGURANÇA DA INFORMAÇÃO

Com o fluxo gigantesco de informações, mesmo estas sendo classificadas da melhor forma possível pela organização, fica evidente que é apenas uma parte do papel a ser desempenhado sobre as informações, anteriormente vistas como um dos bens, se não o mais, valioso para a organização.

As informações utilizadas para os processos e atividades que contribuem na continuidade do negócio é um recurso de interesse não apenas da própria organização, mas sim também das concorrências e de organizações externas. E, para evitar o acontecimento de algum evento inesperado como roubo, perda, acesso indevido, modificação não autorizada, que poderá afetar e trazer prejuízos, é necessário a aplicação de segurança da informação sobre os dados da organização.

> Segurança da informação é o conjunto de orientação, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

> Segurança da Informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos da informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas. (FONTES, 2006)

Segundo Campos (2007) um sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade.

Quando se trata de falar em segurança da informação, considerações necessitam ser feitas em relação a estes três princípios básicos, já que qualquer comprometimento de um desses princípios, quer dizer um comprometimento da segurança.

Figura 1: Pilares da Segurança da Informação

FONTE: Elaborado pelo autor, 2016

- **Confidencialidade**

De acordo com a NBR ISSO/IEC 27002 (2005) confidencialidade se diz respeito a garantir que somente pessoas autorizadas irão ter acesso a informação. Em contraponto ocorrendo acesso por uma pessoa não autorizada, de forma intencional ou de forma não intencional, a quebra de confidencialidade é concretizada. Os danos quanto à quebra desse sigilo acarretam danos grandiosos a organização ou uma pessoa física ligada a mesma.

- **Integridade**

Conforme a NBR ISSO/IEC 27002 (2005) a integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento.

Para Dantas (2011) a garantia da integridade passa pela não permissão de alteração, modificação ou destruição da informação, fazendo assim com que ela permaneça consistente e legitima.

> Contribui para perda da integridade as inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alteradas para se ter acesso a informações restritas [...]. (DANTAS, 2011).

- **Disponibilidade**

De acordo com a NBR ISSO/IEC 27002 (2005) a disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. “Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação. ” (DANTAS, 2011).

3 GOVERNANÇA DE T.I.

Para uma empresa ser bem-sucedida em seu ramo, ou mesmo entre outras que não pertençam ao mesmo seguimento, não necessita somente de ter boas ideias que incluam, por exemplo; inovações, bom relacionamento de funcionário e empregador; Todos os principais setores da alta administração necessitam de uma estruturação solida e uma conversação entre si. E essa esbarra nos gestores financeiros e gestores da tecnologia da informação.

De acordo com Weill e Ross (2006) para uma melhor governança do TI, ela passa pela governança financeira e corporativa da empresa. A divisão de responsabilidade de ambos e seu comprometimento em realiza-los da melhor maneira possível é de vital importância para que a empresa se desenvolva e atinja seus objetivos de negócio.

De acordo com João Perez professor da FGV (Fundação Getúlio Vargas) Governança de TI é:

> [...] um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, aperfeiçoar a aplicação de recursos, reduzirem os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios.

Weill e Ross (2006) diz a governança de TI ser "[...] a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização da TI. ".

Ainda Barbosa *et al.* (2011) salienta que a Governança de TI se trata de integração de diversos processos que colaborando entre si dando suporte a gestão, como por exemplo: CRM (*Customer Relationship Management*), ERP (*Enterprise Resourse Planning*), BI (*Bussiness Intelligence*) e SCM (*Supply Chain Management*), que são metodologias de gestão corporativas dos recursos de TI.

Para se empregar a governança de TI existem alguns frameworks de boas práticas que através de seus objetivos de controles e seus processos, é possível a empregabilidade da governança de TI em uma empresa.

3.1 COBIT

O COBIT (*Control Objectives for Information and related Technology*) é um framework focado em governança de TI mantido pela ISACA (*Information System Audit and Control Association*) que por sua vez é formado por mais de 180 empresas de TI ao redor do mundo, administrando certificações de segurança, governança, auditoria e risco, internacionalmente reconhecidas. O COBIT é mantido e distribuído pelo ITGI (*IT Governance Institute*) – Instituto de governança de TI.

O COBIT fornece aos gestores, auditores e usuários de TI um conjunto de medidas, indicadores, processos e melhores práticas para ajuda-los a maximizar os ganhos do uso da TI e o desenvolvimento da governança de TI. Atualmente o COBIT se encontra em sua quinta versão contando com uma arquitetura formada por quatro domínios: Planejar e organizar, adquirir e implementar, entregar e suportar, monitorar e avaliar.

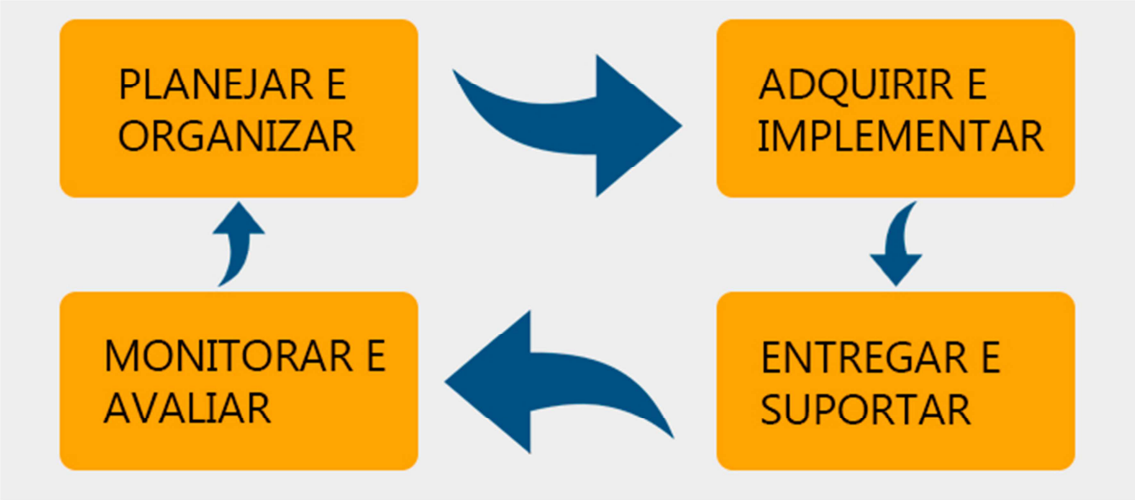
Ferreira e Araújo (2008) apontam o COBIT como sendo um modelo que visa estruturar o TI e molda-lo de acordo para que possa suporta-lo a partir de controles internos que possibilitaram mensurar o desempenho e gerenciar os riscos associados ao mesmo. Tendo como modelo de gerenciamento a nível estratégico, suas estruturas de controles são padronizadas e aceitas mundialmente em qualquer que seja o setor de negócios, principalmente em segmentos financeiros.

3.1.1 Estrutura do COBIT

O objetivo do COBIT é de proporcionar a gestão como uma modelo de governança de TI que irá ajudar a controlar e gerir informações e tecnologias relacionadas. O Framework explica como os processos de TI podem entregar a informação que a empresa realmente necessita para atingir os seus objetivos. Esta entrega que é controlada através de 34 objetivos de controle, um para cada processo em especifico, contidas nos quatros domínios. O framework identifica qual dos setes critérios de informação (eficácia, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade) bem como quais os recursos de TI (pessoas, aplicações, tecnologias, instalações e dados) são importantes para que o TI apoio devidamente os negócios e que o mesmo consiga

alcançar seus objetivos. O ITGI definiu como os quatros domínios da seguinte forma ilustrada na Figura:

Figura 2 - O ciclo PDCA do Cobit 4.1



Fonte: Adaptado pelo autor (COBIT 4.1)

Ferreira e Araujo (2008) explanam os quatro domínios:

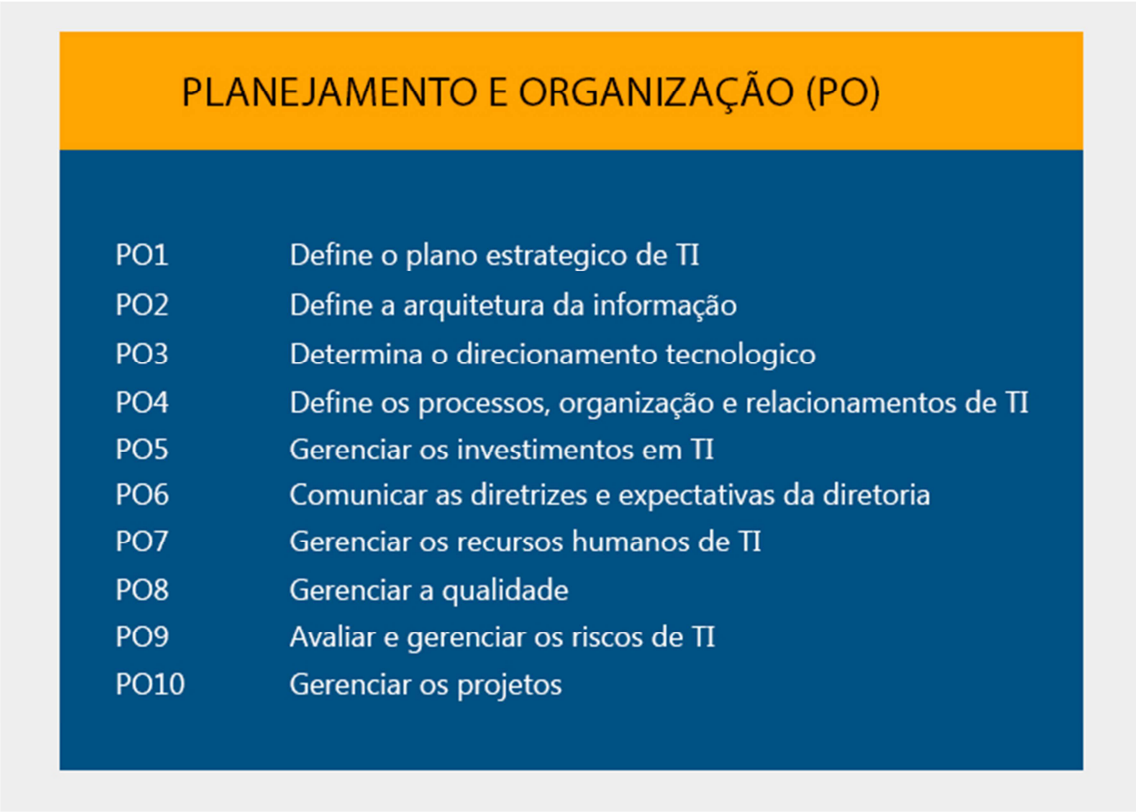
A. Planejamento e Organização (PO)

Este domínio se preocupa em identificar de qual maneira a TI contribui para atingir os objetivos de negócios do negócio, se utilizando de estratégias e táticas. A visão precisa ser planejada, gerenciada e comunicada para que haja uma diferença de perspectivas.

De forma resumida, o domínio possui algumas primícias que ajudam a melhor compreensão do domínio e a aplica-lo:

- TI alinhada ao negócio;
- A utilização de recursos de maneira otimizada;
- Entendimento dos objetivos de TI por todos os colaboradores;
- Gerenciamento e compreensão dos riscos de TI;
- As necessidades do negócio são amparadas pelos sistemas de TI;

Figura 3 - Domínio Planejamento e Organização (PO)



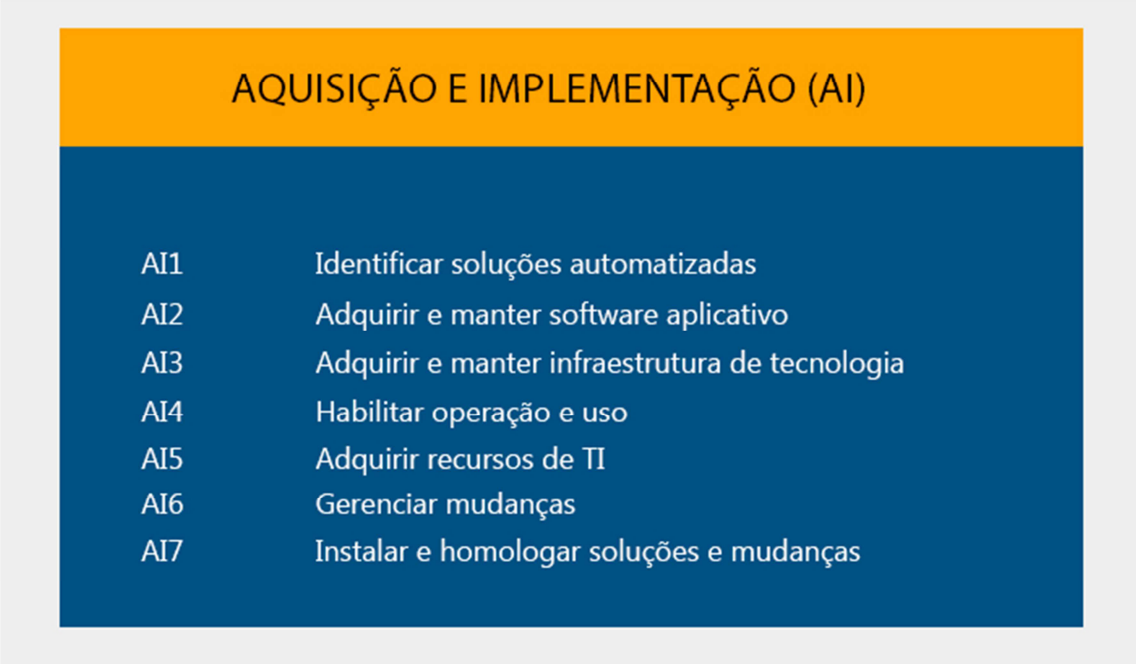
Fonte: Adaptado pelo autor (COBIT 4.1)

B. Aquisição e Implantação (AI)

Neste domino é coberto qualquer alteração em sistemas aplicativos já existentes dentro da organização e visa que a mudança em questão continue a atender o objetivo de negócio. O domínio levanta as seguintes questões:

- As mudanças a serem realizadas estão alinhadas quanto ao prazo e o orçamento, entregando melhores soluções quanto às necessidades do negócio?
- Os novos sistemas após implementados, funcionarão corretamente?
- Toda mudança que será feita, afetara os negócios e suas operações?

Figura 4 - Domínio Aquisição e Implantação (AI)



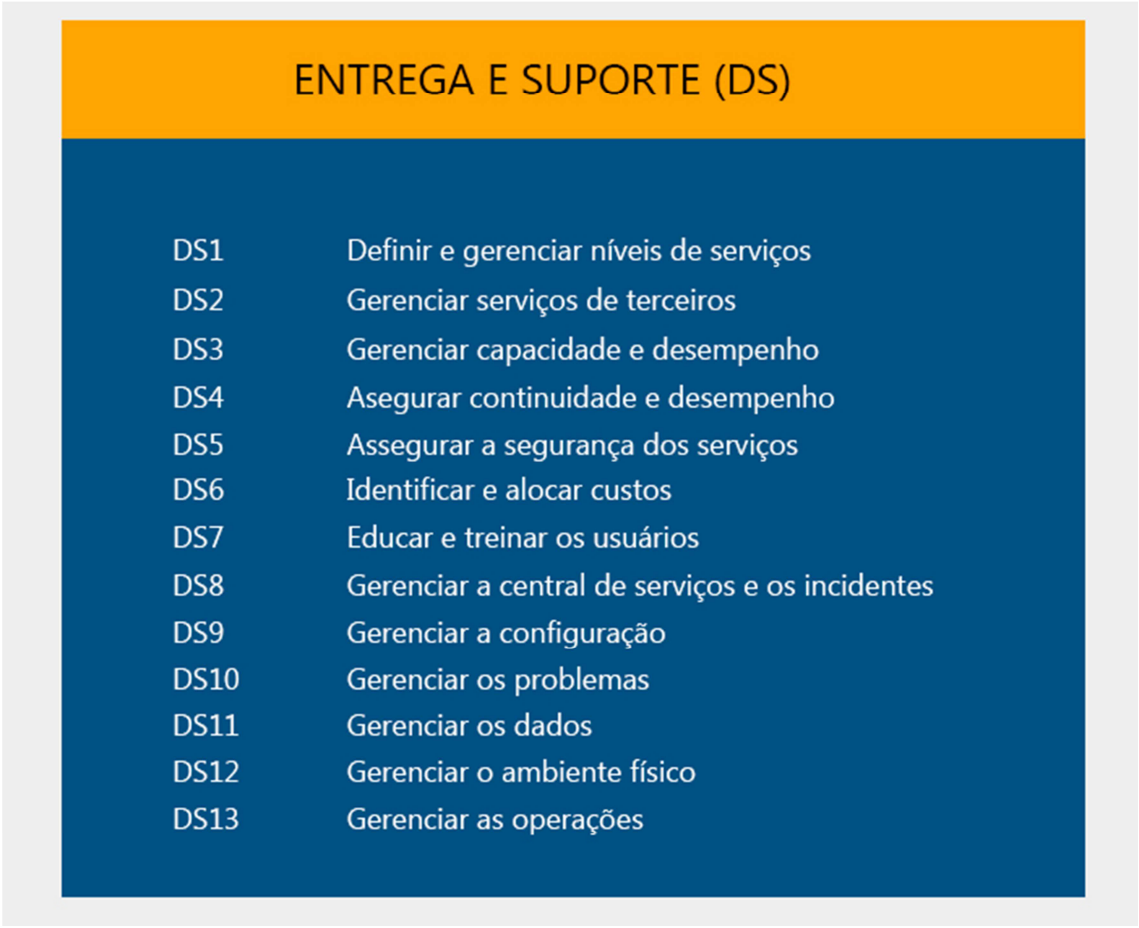
Fonte: Adaptado pelo autor (COBIT 4.1)

C. Entrega e Suporte (DS)

A preocupação deste domínio é com a gestão da segurança da informação e continuidade, assim como suporte ao usuário, gerenciamento de dados e das instalações, bem como a entrega dos serviços solicitados, incluindo o *Service Delivery*. De forma resumida, as questões abaixo ajudam na compreensão e aplicação do domínio:

- A entrega dos serviços de TI está alinhada as prioridades do negócio?
- Há uma otimização dos custos de TI?
- O uso de sistemas informatizados resultara de maneira produtiva e segura por parte da equipe?
- Quando se trata dos principais pilares da segurança da informação (Confidencialidade, integridade e disponibilidade), estes estão postos de forma adequada?

Figura 5 - Domínio Entrega e Suporte (DS)



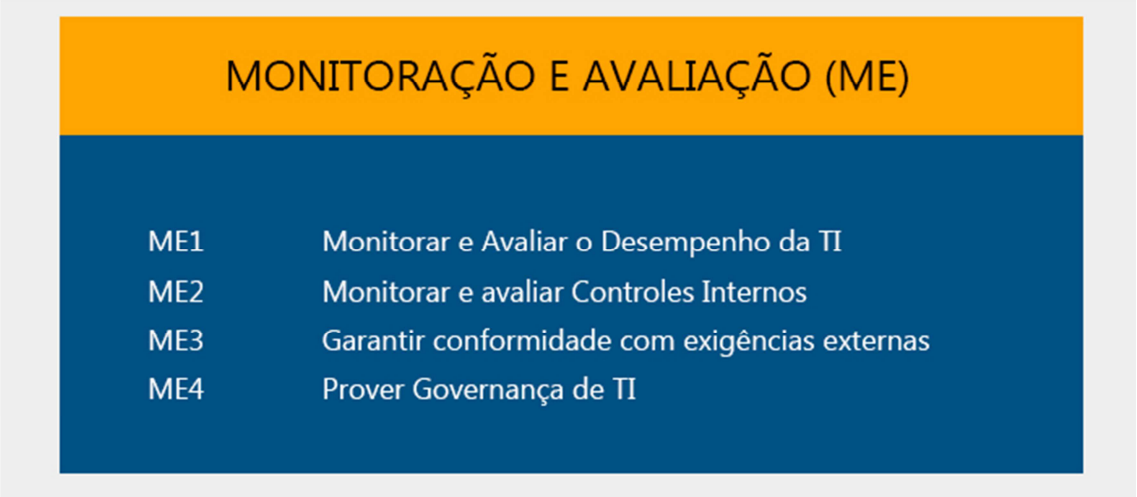
Fonte: Adaptado pelo autor do (COBIT 4.1)

D. Monitoração e Avaliação (ME)

Este domínio diz respeito à qualidade, adequação e a necessidade de todos os processos de TI estarem regularmente sendo auditados. A gestão de performance, monitoração de controles internos e conformidade regulatória também fazem parte do mesmo. Para melhor compreensão do domínio, segue alguns itens:

- Regulares medições da performance da TI;
- Eficiência e efetividade dos controles internos;
- Relação da performance da TI e os objetivos de negócio;
- Reportes e medições de riscos, controles, desempenho e conformidade.

Figura 6 - Domínio Monitoração e Avaliação (ME)



FONTE: Adaptado pelo autor (COBIT 4.1)

3.1.2 Modelo de Maturidade do Cobit

O modelo de maturidade do COBIT 4.1 está baseado no método de avaliação da organização, sendo assim calculado desde o nível de maturidade inexistente (0) a otimizado (5) (ITGI, 2007).

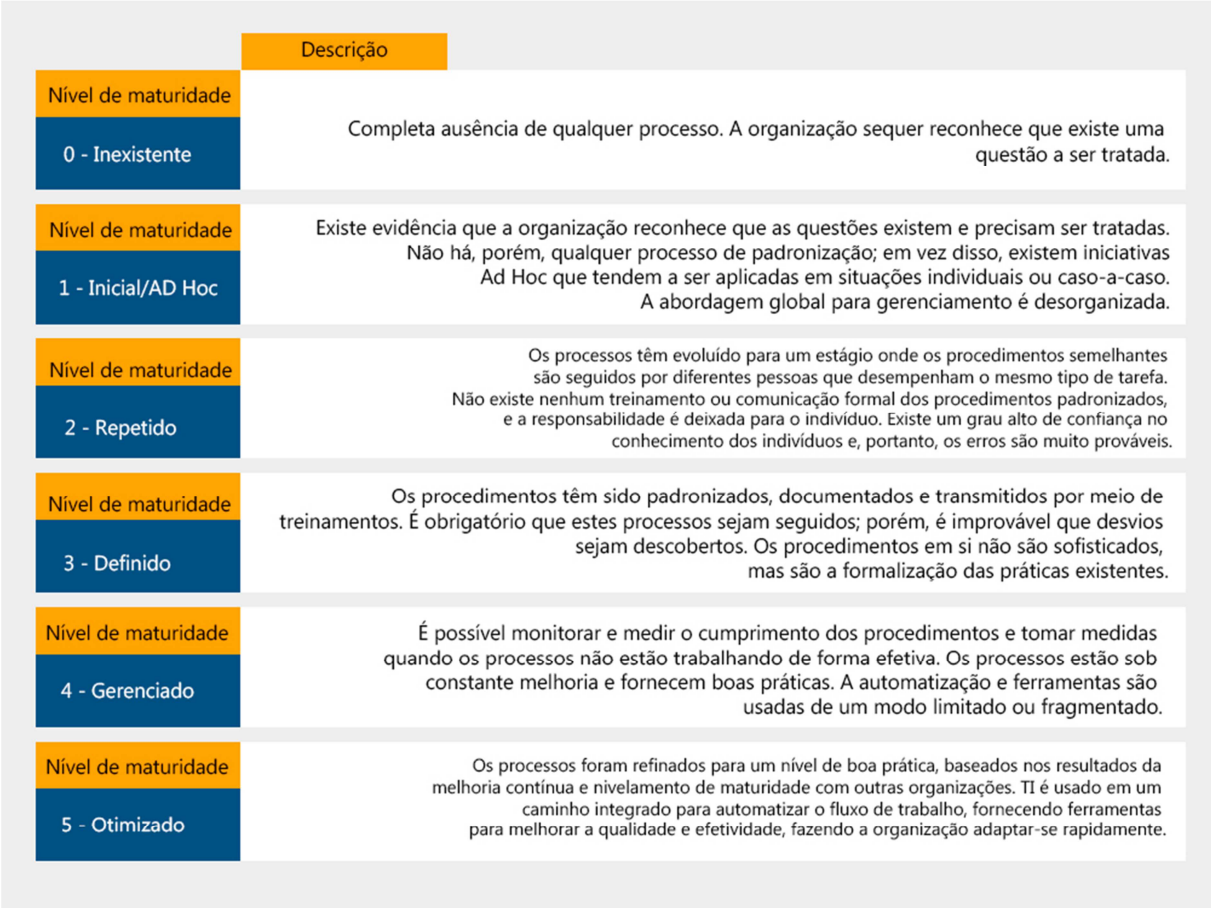
A abordagem de maturidade que tem sua variação entre zero e cinco vem do modelo empregado pelo SEI (*Software Enginnering Institute*), que utilizava o mesmo para a verificação de maturidade a nível de desenvolvimento de software. No COBIT, dentro de cada escala de maturidade, existe uma definição genérica muito similar ao CMM (*Capability Maturity Model*), porém focaliza sua interpretação de acordo com as características do processo de gerenciamento de TI do COBIT. Para cada um dos 34 processos do COBIT existe um modelo especifico, tendo por base a escala genérica.

Para o ITGI (2007) o propósito do modelo de maturidade é identificar onde os problemas estão e como estabelecer prioridades para melhorias, e não simplesmente avaliar o nível de aderência aos objetivos de controle.

Ainda para o ITGI (2007) o modelo de maturidade traz uma vantagem a todos os gerentes auxiliando-os de uma forma de melhor analisar os processos. O modelo traz a facilidade de análise da escala, estimação do que está envolvido e a necessidade ou não de melhorias. A escala de 0-5 é simplificada e mostra a evolução de um processo, desde sua inexistência até a sua otimização.

Na imagem a seguir são apresentadas as descrições para cada nível de maturidade do COBIT 4.1.

Figura 7- Níveis de Maturidade do COBIT 4.1



Fonte: Adaptado pelo autor (ITGI, 2007, p.19)

3.2 A ABNT NBR ISO/IEC 27001

A norma é a referência internacional e também o padrão para uma melhor gestão da Segurança da Informação, bem como a ISO 9001 é a referência quando se trata de certificação de gestão de qualidade (ISO 27001, 2006).

A norma correu por entre milhares de profissionais ao longo dos anos que contribuíram com seu know-how e empregaram sua experiência desde nível inicial até a um nível maduro. Assim a mesma tende a sempre estar em evolução e melhorias.

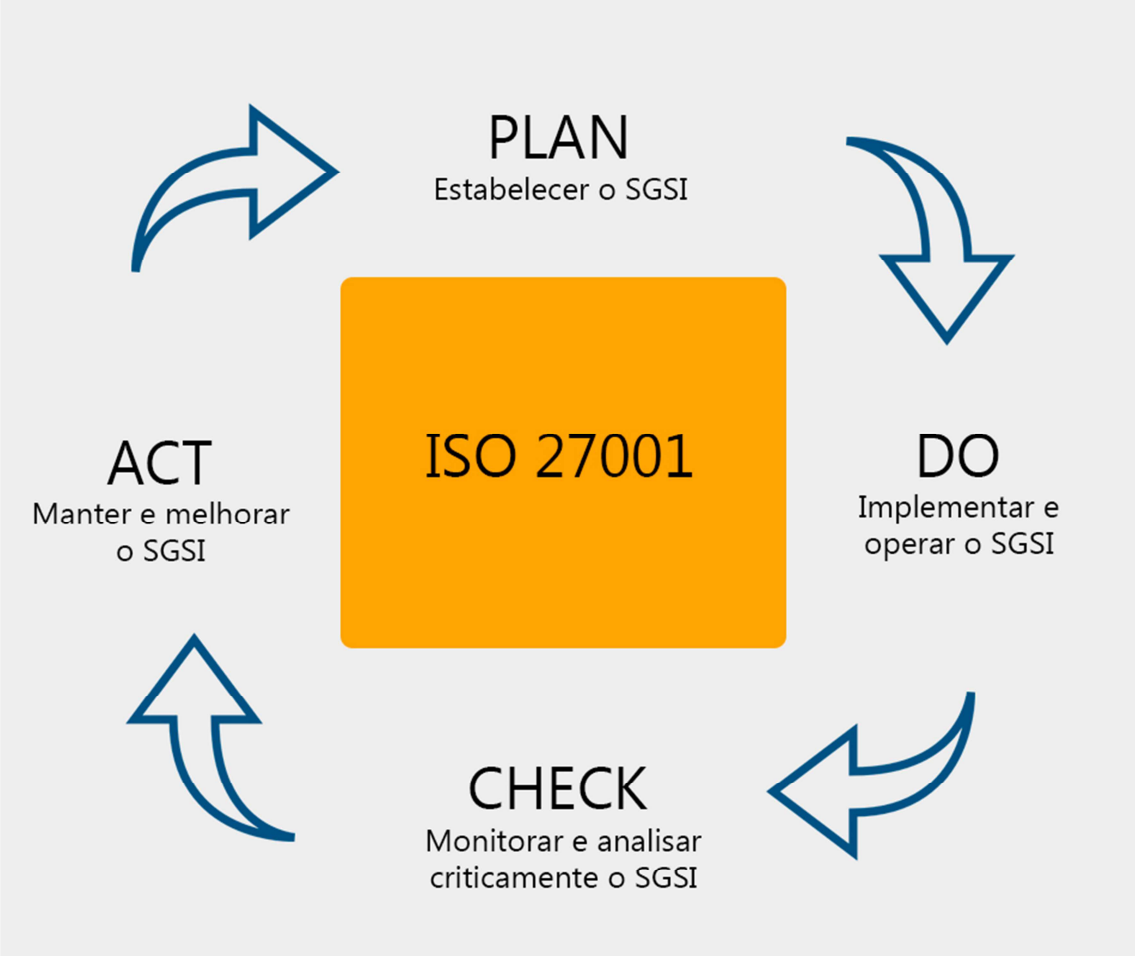
De acordo com ISO 27001:2006 (2006) a norma tem como princípio geral a adoção pela organização de processos, controles e um conjunto bem especifico de

requisitos que tem como objetivo mitigar e gerir adequadamente o risco da organização.

De acordo com ISO 27001:2006 (2006), “A adoção serve para que as organizações adoptem por um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação. ”

A norma ABNT NBR ISO/IEC 27001 adota o ciclo denominado PDCA (Plan, Do, Check, Act) que visa estruturar os processos que estão envolvidos no SCGI (Sistema de Gestão da Segurança da Informação). O PDCA é uma ferramenta de gerencia que possibilita realizar uma melhoria continua de processos e soluções de problemas.

Figura 8 - Ciclo PDCA da ISO 27001



Fonte: Adaptado pelo autor (ISO 27001:2006, 2006)

4 COMPUTAÇÃO EM NUVEM

O conceito surgiu em 1961, quando John MacCarthy, professor, sugeriu que em um futuro não muito distante a computação e aplicações especificas poderiam vir a ser vendidas não somente como um serviço, mas como também um modelo de negócio. A ideia se popularizou nos anos de 1960, mas logo em meados de 1970 a ideia desapareceu. Mas, no entanto, no século 20 aconteceu uma revitalização e o termo computação em nuvem teve seu surgimento no meio da tecnologia (RITTINGHOUSE e RANSOME, 2009).

A disponibilização dos recursos de computação via uma rede global como um conceito surgiu na década de sessenta. Algumas dessas ideias tiveram a participação de Licklinder, este que foi responsável pelo desenvolvimento da ARPANET (*Advanced Research Projects Agency*) em 1969. A visão de Licklinder seria de uma rede intergaláctica que todos poderiam ter acesso a dados ou programas de onde quer que estivessem. (MOHAMED, 2011).

Desde então, computação em nuvem (*Cloud Computer*) passou por várias mudanças em sua definição ao longo dos anos quando vários autores tentaram solidificar o que realmente a mesma significava. Em uma busca pôde-se encontrar cerca de 20 diferentes tipos de definições para o que exatamente é a computação em nuvem.

O termo nuvem (*cloud*) vem de uma metáfora adota na telefonia que visava descrever a internet nos diagramas de rede, e esta, significava algo intangível e indicava que todas as linhas que passavam pelas nuvens eram fluxos de dados que cruzavam a internet (TAURION, 2009).

Segundo Taurion (2009, p. 2) atualmente a nuvem tem uma representação bem sólida e apresenta a mesma como “[...] outra coisa. Aplicações podem usar recursos computacionais da nuvem ou elas mesmas podem executar de lá. A nuvem não é mais algo intangível, mas o cerne da computação. “

O NIST (National Institute os Standards and Technology) define computação em nuvem como:

> Modelo para habilitar acesso via rede, de forma ubíqua, conveniente e sob demanda, a um conjunto compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser provisionados e liberados rapidamente com

> mínimo de esforço de gerenciamento ou interação com o provedor de serviço.

Ainda Taurion (2009, p.25) destaca que:

> Ainda existe muito desconhecimento, desinformação e até mesmo mitos são criados em torno do assunto. Mas é inegável que a computação em nuvem vai transformar a maneira de como as empresas operam sua TI, bem como vai transformar a maneira como os provedores irão oferecer seus serviços de TI.

Pode-se entender então, que de forma resumida a computação em nuvem consiste em um armazenamento dos dados feito em serviços que disponibilizam o acesso para os mesmos de qualquer lugar do mundo, sem necessidade de usar qualquer software instalável de forma intermediaria ou de qualquer banco de dados. O acesso é realizado utilizando uma conexão via internet e navegadores como, por exemplo: Google Chrome, Mozilla Firefox, Internet Explorer.

4.1 CARACTERÍSTICAS ESSENCIAIS

Foram definidas pelo NIST algumas características que descrevem o que exatamente o modelo de computação como sendo de fato uma computação em nuvem. Características estas que melhor identifica, representa as vantagens da mesma e também serve para distinguir a computação em nuvem de outros paradigmas.

A figura a seguir resume as características:

Figura 9 - Características da computação em nuvem

FONTE: Adaptado pelo autor (VERAS, 2015, p. 75)

4.1.1 Virtualização de recursos

Há muito existem tecnologias que são capazes de virtualizar recursos importantes usados em maquinas e dentre elas é importante citar as maquinas virtuais, virtualização de rede, de memória e de armazenamento de dados.

Sendo assim nasce o que se pode ser tratado como uma nova camada, a camada inferior as camadas convencionais, isso graças a possibilidade da separação dos serviços de infraestrutura dos recursos físicos como hardwares e rede.

A esse ponto de abstração tem-se os recursos sendo disponibilizados e podendo ser utilizados como serviços utilitários, sem necessidade de ter uma manipulação do hardware ou rede.

4.1.2 Serviços sob demanda

O cliente tem a possibilidade de a qualquer momento adequar o uso de recursos computacionais de acordo com a sua necessidade momentânea ou não. Estes recursos são, por exemplo: Tempo de processamento, armazenamento e até

mesmo largura de banda. As requisições de aumento ou não de recursos são feitas de forma automática, descartando assim a necessidade de uma interação humana por conta do provedor do serviço.

De forma direta o NIST (2014) caracteriza como “a capacidade de o provedor da nuvem agrupar e mover recursos (físicos e virtuais) para acomodar as necessidades de expansão e demanda do cliente. ”

Os recursos computacionais, através de um provedor, de forma ideal, devem atender os consumidores através de um modelo multicliente, se utilizando de diferentes recursos físicos e virtuais, sendo a atribuídos e podendo ser retribuídos de forma dinâmica de acordo com a necessidade, demanda, dos consumidores. (Borges et al., 2014)

4.1.3 Elasticidade e Escalabilidade

A preocupação por parte de todo gerenciamento de infraestrutura de TI é ter um potencial de expansão da mesma, ou o potencial de possíveis mudanças, ou até mesmo necessárias mudanças, sem danificar o negócio que se está se apoiando nesta infraestrutura.

A computação em nuvem tem esta característica, a elasticidade, que faz dela uma grande inovação para o negócio de TI. De acordo com Borges et al. (2014) escalabilidade é “a capacidade de disponibilizar e remover recursos computacionais em tempo de execução, independentemente da quantidade solicitada. ”

A escalabilidade é parte do contexto e se define sendo “aumento da capacidade de trabalho através da adição proporcional de recursos. ” (Borges et al., 2014).

O prestador de serviços não tem a possibilidade de prever com antecedência se a utilização do serviço disponibilizado para o cliente será feita todos os dias ou se será feita de forma esporádica e em situações de pico. Sendo assim, o provedor tem o dever de disponibilizar o serviço contratado os sete dias da semana durante as 24 horas por dia, além de ter o reconhecimento automático de quando escalar para mais ou para menos, e sendo acionado de forma que não haja intervenção humana.

4.1.4 Medição dos Serviços

Grandes recursos que utilizamos no dia a dia têm de estarem disponíveis todos os dias devido a sua grande importância para todos, porém o pagamento deste uso não é perante o uso e sim a quantia de uso do mesmo. A computação em nuvem elevou o uso de recursos computacionais a um novo nível, conseguindo controlar e aperfeiçoar o uso da mesma por meio de medições inteligentes.

De acordo com Borges et al. (2014) a monitoração empregada gera uma transparência muito grande ao provedor quanto ao cliente, isto por meio de contratos diferentes de acordo com o serviço (SLA – *Service Level Agreement*) que especifica as características dos serviços, parâmetros de qualidade (QoS – *Quality of services*) e assim determinar qual o valor será cobrado.

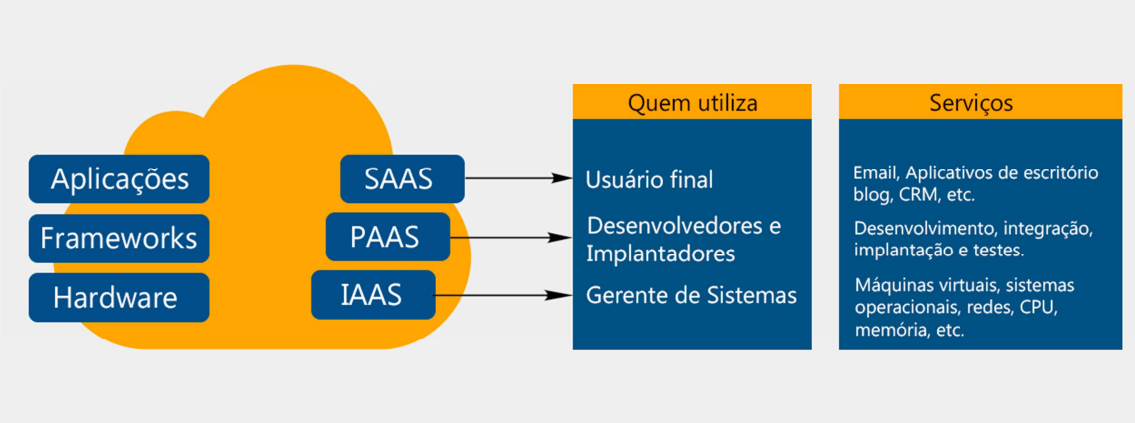
4.2 PRINCIPAIS MODELOS DE SERVIÇOS

De acordo com Elsenpeter et al. (2011), o conceito de serviços se tratando de computação em nuvem, se diz a utilização de componentes de forma a possibilitar a reutilização do mesmo assim que o necessitar. Esta utilização é conhecida como “as a service” (como serviço).

Ainda Elsenpeter et al. (2011) descreve algumas características, sendo elas:

- Possibilidade de adoção por parte de empresas de pequeno porte;
- Sua escalabilidade;
- A multilocação, permitindo assim que os recursos sejam compartilhados entre muitos usuários;
- A possibilidade de acesso por parte dos usuários independente dos dispositivos e dos hardwares destes dispositivos em uso.

Figura 10 - Principais modelos de serviço em nuvem



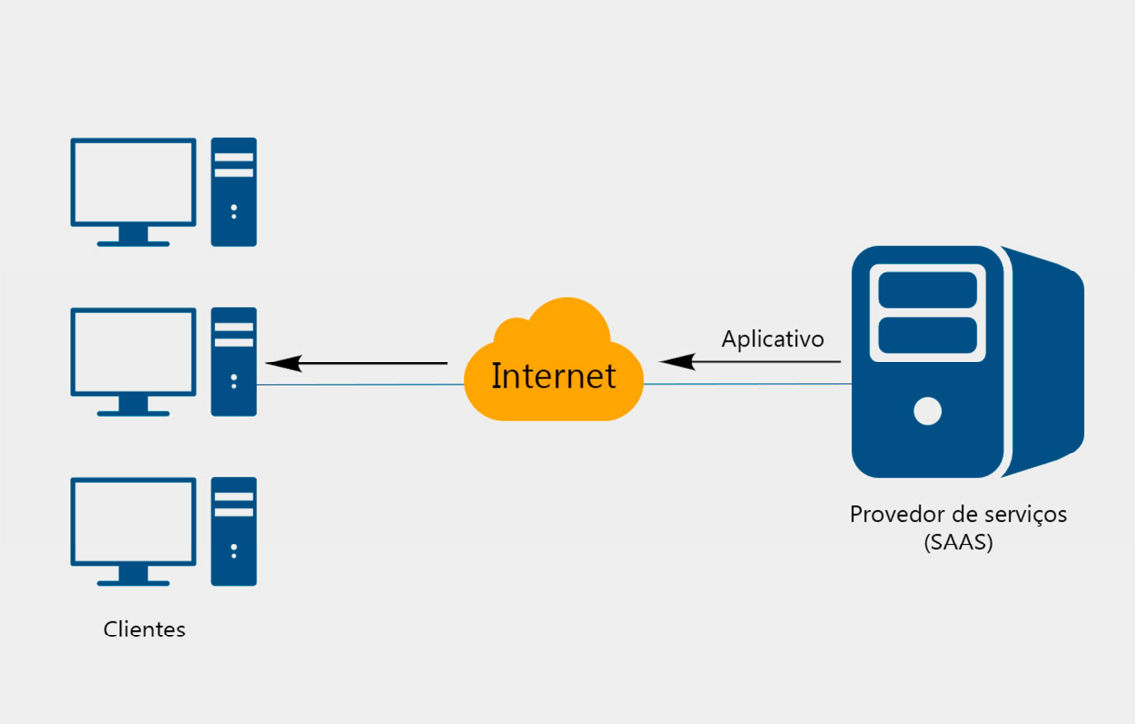
Fonte: Adaptado pelo autor (BORGES ET AL, 2014 p.8)

4.2.1 Software como Serviço (SaaS)

O modelo de Software como um serviço (SAAS) é um aplicativo que desempenha algumas funcionalidades especificas, este que será acessado via conexão de internet pelo cliente que o contratou. O cliente não necessita de preocupar-se com licenciamento do mesmo ou suporte, como quando algum software comum é instalado ema estação de trabalho.

Elsenpeter et al. (2011, p.12) explica que “a ideia é que você usa o software fora da caixa e que não precisa fazer muitas mudanças ou solicitar a integração a outros sistemas. O provedor faz todo o processo e atualizações assim como mantém a infraestrutura funcionando”.

Figura 11 - Software como Serviço (SaaS)



Fonte: Adaptado pelo autor (ELSENPETER ET AL, 2011 p.12)

As aplicações são acessadas pelo cliente via browser e estas são disponibilizadas através de um provedor. Todo o controle e gerenciamento de rede, sistema operacional, armazenamento ou servidores é feito pelo provedor de serviço (Veras, 2015).

Existem vários softwares que poderiam se tornar um SaaS, e são eles softwares que executam tarefas simples e sem necessidade de interação com outros sistemas. Há algumas aplicações que mesmo potentes operam como SaaS. De acordo com Elsenpeter et al. (2011) estas aplicações incluem:

- Gerenciamento de recurso do cliente (CRM);
- Videoconferência;
- Gerenciamento de serviços de TI;
- Contabilidade;
- Analise de web;
- Gerencia do conteúdo web.

Segundo Elsenpeter et al. (2011) o SaaS traz muitos benefícios, e de forma clara se aponta o fato de não haver o custo da compra da aplicação de forma direta, bem como sua licença de operação. Existem ainda outros benefícios.

- A familiaridade com a World Wide Web: por conta da facilidade de acesso a World Wide Web, a aprendizagem para utilização das aplicações é menor.
- Equipe reduzida: há cortes de gastos por parte do RH, visto que a necessidade de um espaço físico, salários, benefícios e seguro não é necessário por conta da habilidade de produção desses aplicativos fora deste ambiente.
- Personalização: Facilidade de entregar uma maior personalização para cliente de uma forma mais organizada.
- Marketing eficiente: O SaaS proporciona um mundo inteiro aberto aos fornecedores, diferente de uma aplicação criada somente a um pequeno mercado especifico.
- Confiabilidade na web: Existe uma confiabilidade muito grande em relação a World Wide Web, consolidada ao longo dos anos.
- Segurança: A utilização do SSL como padrão faz com que o cliente não precise utilizar recursos como redes privadas virtuais (VPN's).
- Conexão mais veloz: Com a melhora da velocidade de conexão as empresas conseguem acesso com baixas latências.

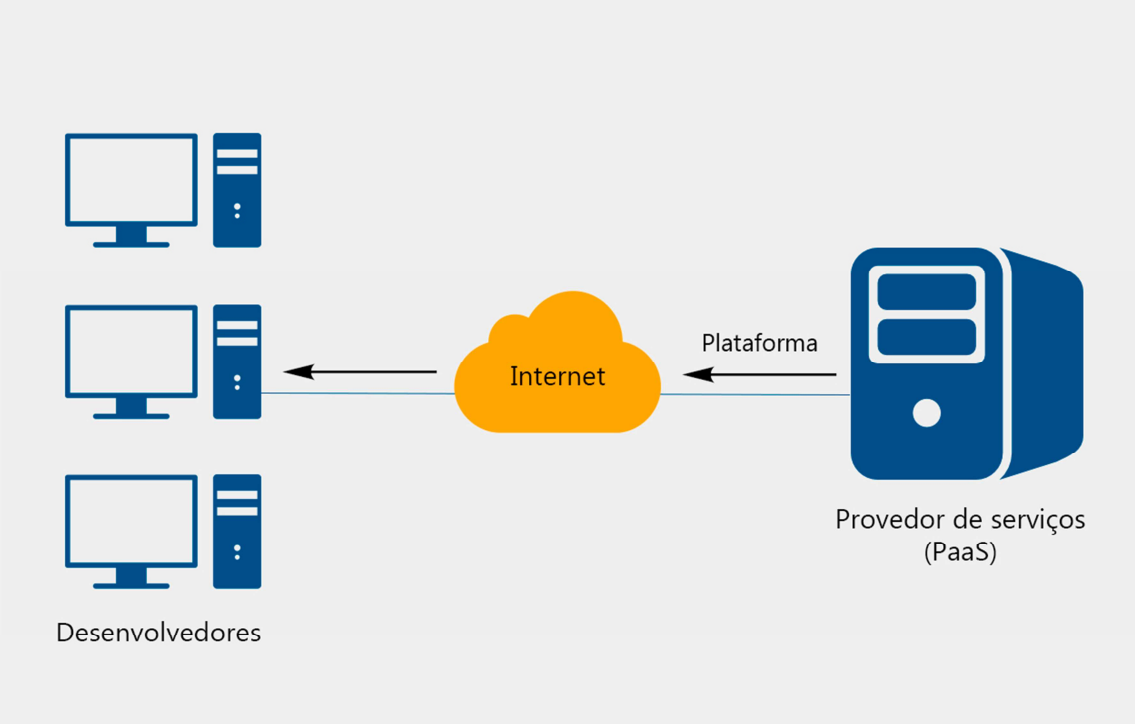
4.2.2 Plataforma como Serviço (PaaS)

A plataforma como serviço (PaaS) segue os passos do SaaS, e é outro modelo de aplicação. De acordo com Elsenpeter et al. (2011) o PaaS oferece todos os recursos necessários para que possa ser utilizado para a construção de aplicativos e outros serviços diretamente da internet, isso sem baixar ou instalar qualquer tipo de software.

Para Veras (2016), além de oferecer a capacidade para o desenvolvimento de aplicativos, estes que serão executados e disponibilizados na nuvem, o PaaS oferece também um armazenamento e comunicação entre estes aplicativos.

Ainda de acordo com Veras (2013), o PaaS "[...] está vinculado ao uso de ferramentas de desenvolvimento de software gratuitas, oferecidas por provedores de serviços, onde desenvolvedores criam as aplicações utilizando tecnologias de internet".

Figura 12 - Plataforma como Serviço (PaaS)



FONTE: Adaptado pelo autor (Elsenpeter et al., 2011 p.14)

O serviço PaaS inclui ainda design de aplicações, desenvolvimentos, implantações, testes e hospedagens, como de sites por exemplo. Há ainda outros serviços, como colaborações em equipe, integração de serviços web, integração de banco de dados, segurança, escalabilidade, gerenciamento de armazenamento, de estado e de versões. (Elsenpeter et al., 2011)

O PaaS ainda possui o recurso de utilização de muitos usuários de forma simultânea, ele de fato foi desenvolvido para este fim, de forma geral, o mesmo dispõe de instalações automáticas de simultaneidade, gerenciamento, escalabilidade, *failover* (redundância) e segurança. (Elsenpeter et al., 2011)

Borges et al. (2014) cita uma funcionalidade interessante do PaaS:

> [...] PaaS contribui com a disseminação de princípios da Service Oriented Architecture (SOA) que permitem a integração de dados e funcionalidades de aplicativos que residem na plataforma de nuvem com outros sistemas e aplicações on-premise ou on-demand.

O PaaS também tem seu grau de apoio destinado ao desenvolvimento de interfaces web, como *Simple Object Access Control* (SOAP) e *Representational*

State Transfer (REST), ambos que permitem construção de serviços de forma múltipla a web, também chamadas de Mashups. Estas interfaces são capazes de acessar base de dados e serviços de reutilização mesmo estas estando dentro de uma rede privada. (Elsenpeter et al. 2011)

De acordo com Elsenpeter et al. (2011) o PaaS pode ser encontrado de três diferentes tipos de sistemas. São eles:

- Add-on de desenvolvimento: Eles permitem que o usuário tenha seus aplicativos em SaaS personalizados. Necessitam, em sua maioria, de compra de licença.
- Ambientes autônomos: São ambientes sem necessidade de licença, sem dependências técnicas ou financeiras em aplicações SaaS. Este é utilizado para desenvolvimento de forma geral.
- Ambientes de entrega somente de aplicativos: Estes ambientes suportam serviços como por exemplo de hospedagens, segurança e a escalabilidade por encomenda. Este que não inclui suporte a desenvolvimento, eliminações de erros, como também capacidades de testes.

Como todo serviço, o PaaS também possui e entrega benefícios quanto a sua utilização, sua adoção como serviço em uma organização. Borges et al. (2014) cita alguns:

- O investimento inicial é baixo, isto representa um menor risco ao negócio, não tendo a necessidade de investimentos com infraestruturas, softwares básicos, sistemas operacionais e softwares adicionais necessários para execução das aplicações necessárias do ambiente de desenvolvimento. Tendo isso em vista, é inegável que ocorra uma redução em gastos.
- Novas funcionalidades, bem como atualizações de segurança ou não, são recebidas de forma imediata não tendo a necessidade de programar estas e disponibilizar profissionais para tal tarefa.
- Soluções para problemas encontrados são rapidamente implementadas sem ocasionar o retardo do mesmo tratando-o de forma individual. Todo o tratamento e sua solução é feita de forma transparente ao usuário.
- A segurança dos dados e o aumento da disponibilidade, isto muito importante, tendo em vista que a maioria das empresas são deficitárias quando se tratam

de realização de backups de dados importantes, restauração e planos de contingencia.

4.2.3 Infraestrutura como Serviço (IaaS)

O modelo IaaS consiste de variados conceitos e composto por componentes que foram ao longo dos anos sendo desenvolvidos e melhorados, e ainda sim se é um desafio à segurança e a privacidade.

Veras (2016) o define como:

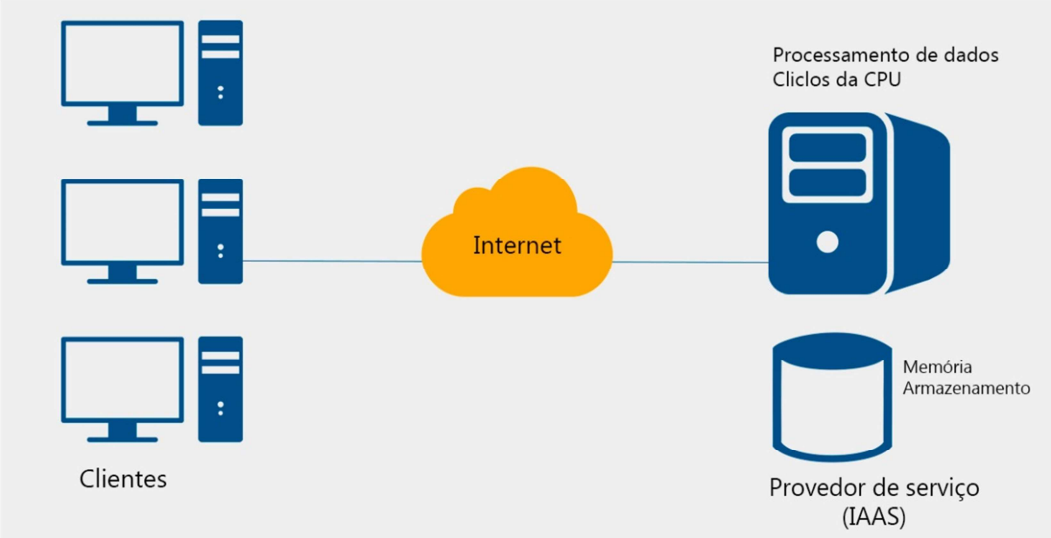
> Neste cenário, o usuário não tem o controle da infraestrutura física, mas, através de mecanismos de virtualização, possui controle sobre sistemas operacionais, armazenamento, aplicações instaladas e possivelmente um controle limitado dos recursos de rede.

Este modelo de serviço descarta a necessidade da compra de periféricos físicos como servidores, *racks*, *softwares*, até mesmo ter que arcar com gastos de um espaço físico para alocar o data center.

De acordo com Elsenpeter et al. (2011) o IaaS “aluga” recursos como:

- Espaço de alocação física do servidor;
- Rede e seus equipamentos;
- Memoria;
- CPU;
- Armazenamento e seu espaço.

Figura 13 - Infraestrutura como Serviço (IaaS)



Fonte: Adaptado pelo autor (Elsenpeter et al., 2011 p.15)

O IaaS pode ser dinamicamente ajustado para cima, com uma grande necessidade de uso, ou para baixo, com uma baixa necessidade de recurso de uso. Além disso a infraestrutura pode ser usada por múltiplos locatários ao mesmo tempo.

O serviço de IaaS também é pago conforme a sua utilização e a necessidade de negócio da empresa.

De acordo com Elsenpeter et al. (2011) o IaaS possui diversas partes:

- Acordos de nível de serviço: É acordado entre o cliente e o provedor o mínimo de desempenho aceitável do sistema.
- Hardware: Estes são alugados e os prestadores os possuem em grade possibilitando uma futura escalabilidade.
- Network: Inclui periféricos físicos para routers, balanceamento de cargas, firewalls, entre outros.
- Conectividade da internet: possibilita o acesso aos hardwares contratados de modo remoto.
- Ambiente de virtualização da plataforma: o cliente pode utilizar a máquina virtual que desejar.
- Faturamento de suprimentos de informática: utilizados para realizar a cobrança do uso dos recursos do sistema que fora utilizado.

O modelo de serviço em nuvem IaaS possui diversos benefícios quando empregado de forma correta em uma empresa. Borges et al. (2014) cita alguns deles sendo:

- Possibilidade de a gestão do negócio não ter a preocupação com a gestão de infraestrutura de TI da organização.
- Não há necessidade de investimentos em infraestrutura, sendo somente necessária a preocupação com a contratação do serviço, cujo o provedor será responsável por arcar com manutenções entre outras questões.
- Possibilita enxergar quando, o quanto e como investir no futuro.
- Possibilidade de escalabilidade tecnológica de equipamentos e sistemas de rede que são de vital importância para o crescimento do negócio da organização.
- Redução de gargalos e de *downtime* em equipamentos de rede.
- Aumento na produtividade da equipe, por não haver necessidade de alocar profissionais para reparos ou manutenções na infraestrutura.
- Custo operacional fixo.

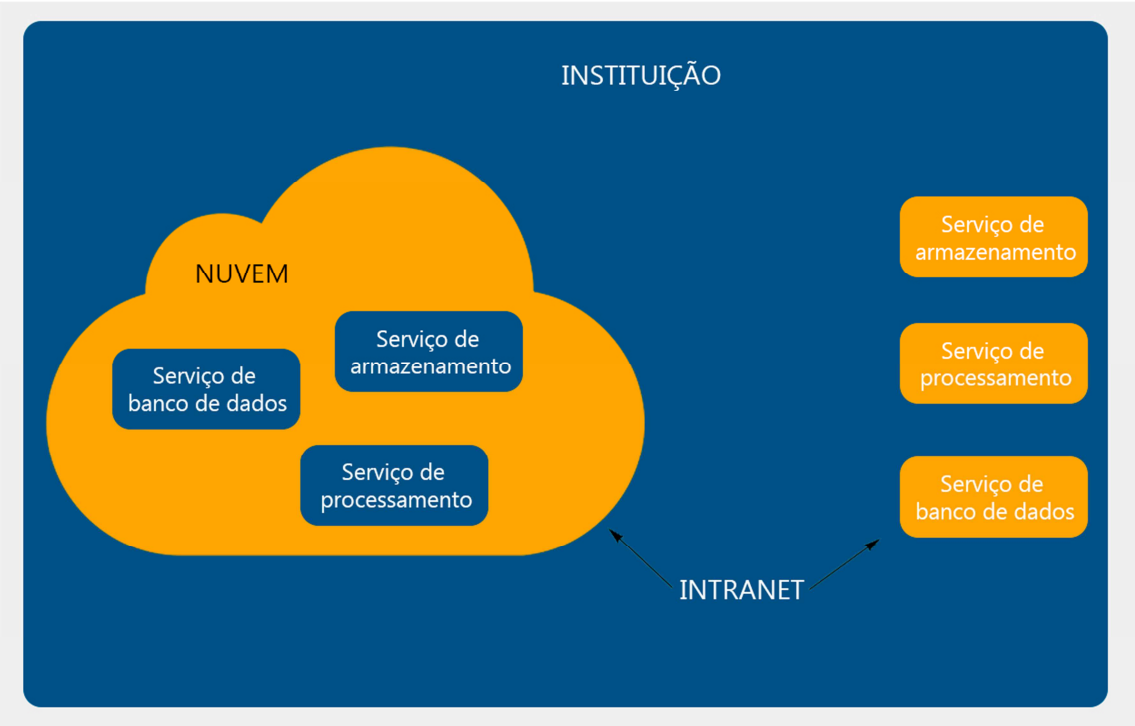
4.3 MODELOS DE IMPLANTAÇÃO

A necessidade de adequação a necessidade da organização quanto a implantação de fato da nuvem levou a uma variedade de modelos. De acordo com Veras (2015) existem quatro principais modelos que serão descritos a baixo.

4.3.1 Nuvem Privada (Private Cloud)

Uma infraestrutura de computação em nuvem que tem seu gerenciamento feito quase sempre pela organização cliente. Os serviços oferecidos são somente usados pela organização contratante, isso quer dizer que o mesmo não está disponível para uso geral, ou de demais organizações clientes. (Veras, 2015).

Figura 14 - Nuvem Privada (Private Cloud)



Fonte: Adaptador pelo autor (Borges et al., 2014 p.11)

Ainda Veras (2015) sugere que existe dois tipos de nuvem privada: a nuvem privada hospedada pela empresa e a hospedada de fato em um provedor de serviço.

De acordo com Borges et al. (2014) está nuvem privada pode ser de fato local ou remota, porém é empregada políticas de acesso aos serviços que estão nesta nuvem.

As nuvens privadas são munidas de restrições de acesso, geralmente com um *firewall* a frente para realizar esta devida proteção trazendo benefícios tecnológicos para empresa e mantendo o nível de serviço interligada a segurança estipulada da instituição. (Taurion, 2009)

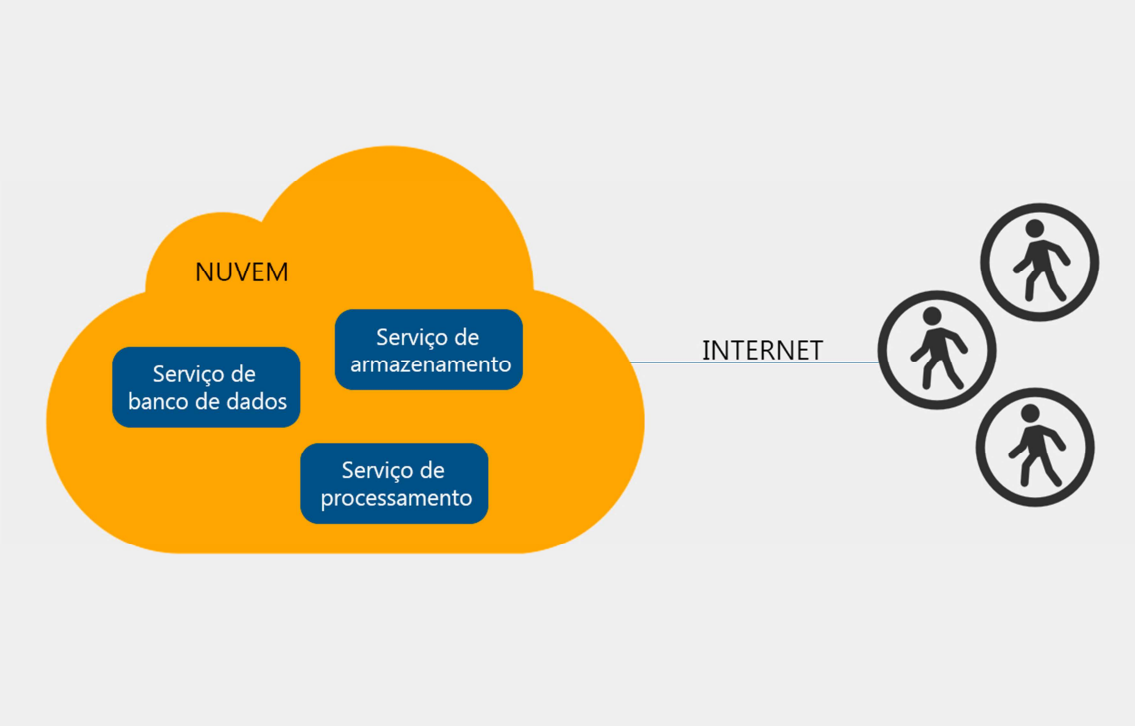
De acordo com Borges et al. (2014) a nuvem privada tem sua adoção por parte das organizações clientes dificultadas por conta de seu custo de operação continua e isso pode fazer com o que a contratação da nuvem privada exceda muito a contratação da nuvem pública. Porém Borges et al. (2014) destaca que a nuvem privada possui vantagens muito superiores a nuvem publica mesmo seu valor muito superior, como por exemplo um controle maior aos recursos da nuvem.

4.3.2 Nuvem Pública (Public Cloud)

De acordo com Borges et al. (2014) em uma nuvem publica a sua infraestrutura é pertencente a uma organização que vende o serviço e este pode ser acessado por todos que saibam onde o mesmo se localiza. A possibilidade de todos poderem ter acesso é a não possibilidade de utilização de restrição do mesmo ou o uso de qualquer mecanismo de autenticação.

Veras (2015) destaca que a nuvem pública é disponibilizada através do modelo “pague-por-isso”. O modelo é em sua maioria oferecido a grandes empresas que necessitam de grande poder de processamento e armazenamento.

Figura 15 - Nuvem Pública (Public Cloud)



Fonte: Adaptado pelo autor (Borges et al., p.12)

Estas nuvens assumem responsabilidades quanto a instalação, gerenciamento, disponibilização e manutenção, tentando assim descomplicar o cliente, deixando-o longe de toda a complexidade maior de TI. (Borges et. al., 2014)

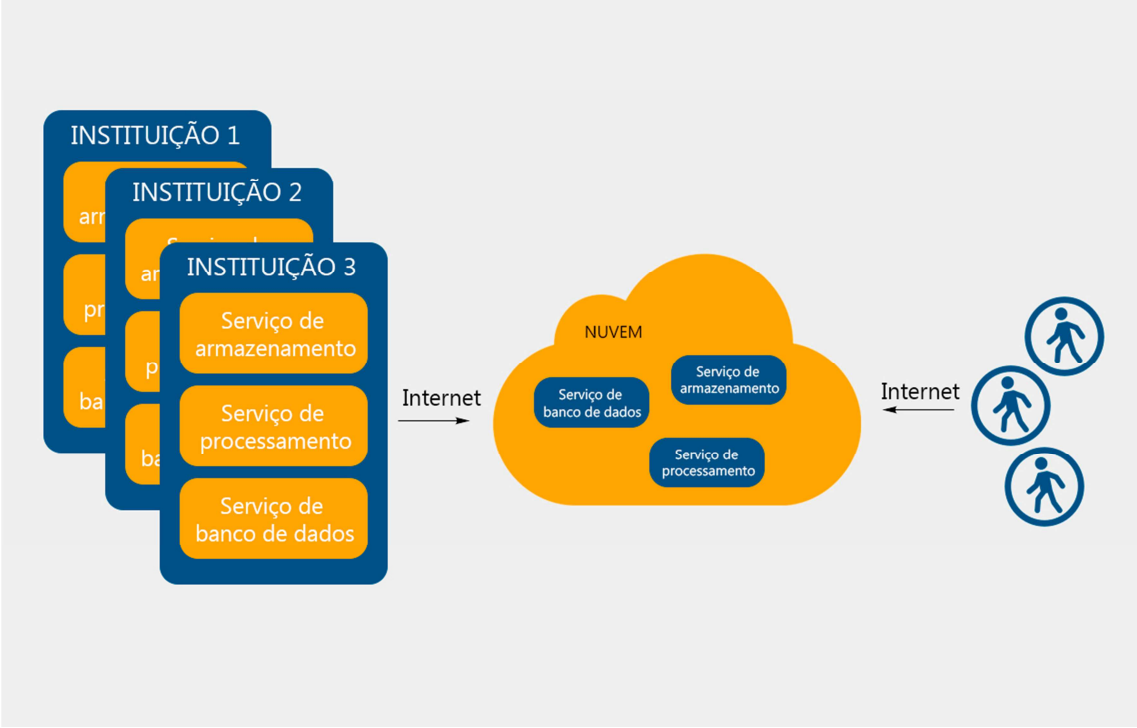
Ainda Borges et al. (2014) destaca que uma organização cliente que possui politicas fortes e elevadas quanto ao aspecto de flexibilidade ou compatibilidade, não se enquadra tornando-se uma opção não viável.

4.3.3 Nuvem comunitária (Community Cloud)

Veras (2015) define a nuvem comunitária como uma infraestrutura de computação em nuvem que é compartilhada entre várias organizações, mantendo-a por intermédio de interesses comuns. A sua administração pode ser feita através de terceiros ou até mesmo pode ser feita pelas organizações que fazem parte da comunidade.

Para Oliveira et al. (2015), a arquitetura de segurança da nuvem comunitária se encontra em um nível intermediário quando se comparada a nuvem privada e pública. As organizações clientes deste tipo de nuvem tem suas políticas de uso e a segurança muito bem acordadas.

Figura 16 - Nuvem Comunitária (Community Cloud)



Fonte: Adaptado pelo autor (Borges et al., p.12)

4.3.4 Nuvem Hibrida (Hybrid Cloud)

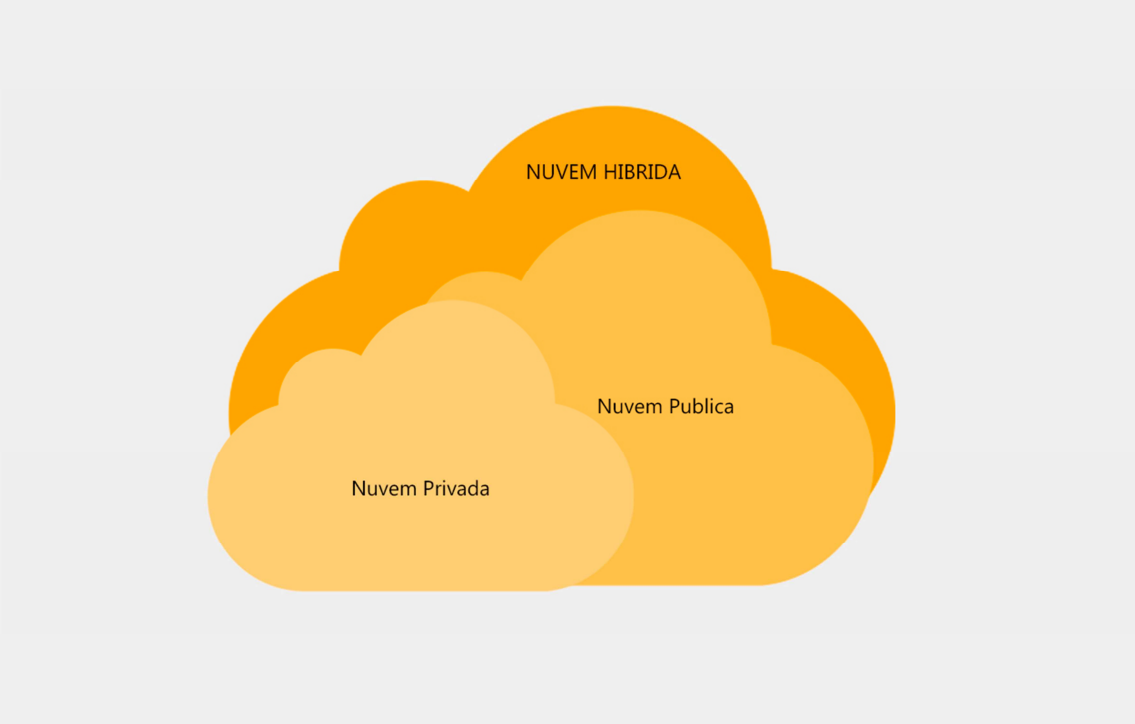
O modelo de nuvem hibrida se resume a uma junção dos modelos anteriormente apresentados. De acordo com Veras (2015) é uma infraestrutura

formada pela junção de duas ou mais nuvens (privadas, públicas e comunitárias) que são únicas, estas conectadas através de tecnologias desenvolvidas por elas próprias ou padronizadas para que possa haver uma portabilidade entre dados e aplicações.

Borges et al. (2014) afirma que:

> Uma nuvem híbrida bem construída poderia atender processos seguros e críticos, tais como recebimento de pagamentos de clientes, assim como aqueles que são secundários para o negócio, tais como processamento de folha de pagamento de funcionários.

Figura 17- Nuvem Hibrida (Hybrid cloud)



Fonte: Adaptado pelo autor (Borges et al., p.12)

Ainda de acordo Borges et al. (2014), a principal limitação da nuvem é fazer com que diversas aplicações e serviços, vindos de diferentes fontes, conversem entre si e que tenham um suporte e uma administração eficaz.

Oliveira et al. (2015) destaca que com uma mescla de nuvens de diferentes fontes, o controle e organização da segurança se torna uma tarefa complicada a se realizar, e que de fato isso é um ponto fraco no modelo hibrido. A necessidade de uma definição refinada quanto aos objetivos e necessidade do uso da nuvem em

questão se torna essencial para que haja uma minimização dos riscos que a utilização da mesma envolve.

5 DESENVOLVIMENTO DO MÉTODO

A partir da apresentação e análise do conteúdo abordado até aqui, destacou-se uma necessidade de melhor agregar os conhecimentos extraídos do mesmo para que fosse elaborado um método, que de forma clara, possibilitasse a migração ou não de uma organização para um serviço de nuvem. Embasando-se nos conceitos de nuvem apresentados até aqui, como seus modelos de serviços SaaS, PaaS e IaaS, foram levantados requisitos mínimos que uma organização deve possuir para que possa de fato migrar para qualquer um desses serviços.

5.1 MÉTODO E SEUS REQUISITOS PARA MIGRAÇÃO

O método consolida os conceitos principais da computação em nuvem e seus serviços que foram abordados anteriormente quando conceituados. Foram formuladas questões fundamentadas nos serviços em nuvem com base em requisitos levantados, cada um possuindo um nível de importância, para que dependendo do resultado da avaliação final, possa responder à questão: Minha organização está apta a realizar uma migração para o modelo de serviço de nuvem SaaS, PaaS ou IaaS?

Os requisitos levantados são de uma importância fundamental para que de fato o método atinja sua efetividade alcançada em seu máximo. Estudando os modelos de serviços de nuvem, os requisitos levantados abordam desde a conectividade e a disponibilidade de internet que a organização deve possuir à até a segurança física e lógica que organização possui ou não. Todos os requisitos que foram levantados e reconhecidos como necessários integrar o método, tem em principio um embasamento forte na segurança da informação e o que a nuvem de fato requer, para que possa se concretizar de fato sua adoção por parte da organização.

Abaixo pode-se observar a tabela com os requisitos formulados para composição do método:

Tabela 1- Requisitos do método de migração

Conexão com Internet	Velocidade
	Disponibilidade
Licenciamento e suporte (Atualizações)	Licenciamentos
	Suporte especializado
Sistemas Integrados	Sistemas de negócios
Treinamento de uso da WEB	Usuários com capacitação de uso WEB
Equipe de T.I.	Certificações
	Custo de funcionários
Redundância de dados	Rotinas de Backup
	Disponibilidade dos dados
	Integridade dos dados
Escalabilidade	Adoção de novas tecnologias
	T.I. e competitividade de mercado
Infraestrutura física defasada	Capacidade de armazenamento limitado
	Processamento limitado
Segurança física	Acesso físico
	Acesso de terceiros
Segurança lógica	Criptografia
	Complexidade de senhas
	Senhas padrão em equipamentos
Disponibilidade	Disponibilidade do sistema administrativo
	Usabilidade dos equipamentos de T.I

Riscos	Mapeamento constante dos riscos
	Tratamento dos riscos
Política de segurança	Negócio e T.I.
	Definição da política de segurança

Fonte: Elaborado pelo próprio autor, 2016

Todos estes requisitos mostrados na tabela acima têm seu valor de impacto na hora de empregar o método. Mediante ao resultado, após a aplicação do método, sabemos se a organização está apta ou não para realizar a migração para o serviço em nuvem.

Alguns dos requisitos mais importantes, como a conectividade com a internet por exemplo, possui um peso maior em relação ao demais requisitos, porém é importante ressaltar que os demais requisitos também são de extrema valia, assim como os requisitos de maior relevância no método.

Requisitos como escalabilidade, disponibilidade e riscos são também de fato muito relevantes. Os mesmos possuem um valor muito grande em relação a governança de T.I. e a organização. A capacidade de escalabilidade do T.I. de uma organização a põe em patamares muito altos e dá a possibilidade para a mesma conseguir se destacar em meio outras organizações concorrentes no mercado.

5.2 CONTROLES DO COBIT 4.1 E ISO 27001 USADOS NO MÉTODO

Com base nos conceitos levantados e expostos anteriormente sobre o Cobit 4.1 e a ISO 27001 e suas importâncias quando tratamos de governar uma T.I. em conjunto com o negócio da organização, fora separados dois controles do framework Cobit juntamente com os controles da ISO 27001 equivalentes, para que a efetividade de entrega de resposta do método fosse maior. São eles: O processo de controle PO9 e DS5.

5.2.1 Processo de controle DS5 – Assegurar segurança dos serviços

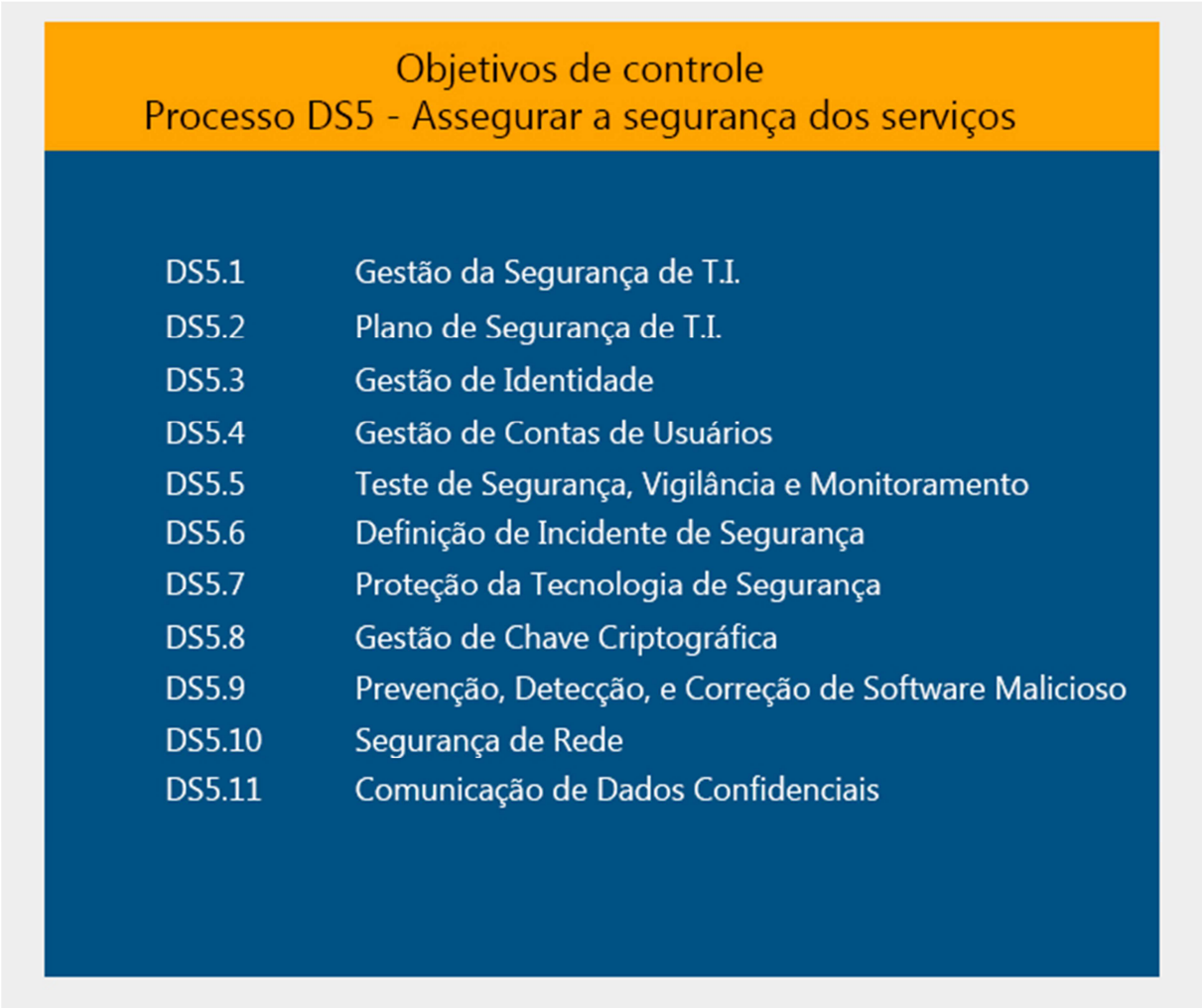
O processo de controle DS5 – Assegurar segurança dos serviços, tem como principal objetivo analisar o processo de gestão da segurança, através do estabelecimento e manutenção de papeis, responsabilidades, politicas, padrões e procedimentos de segurança de T.I. O processo de controle se preocupa em manter a integridade da informação que a organização possui, assim como, proteger os ativos que a mesma possui.

O DS5 também tem seu foco voltado a resposta aos riscos que a organização já conhece e os trata, bem como, os testes periódicos e o monitoramento dos mesmos. Em suma, o processo trata de fazer com que a organização se preocupe com a gestão da segurança e a faça do modo mais eficaz possível, protegendo-se assim de qualquer grande impacto que possa abalar seus negócios.

O processo DS5 possui 11 objetivos de controles, cada um deles tratando de um ponto distinto de acordo com o propósito principal do processo, que é assegurar a segurança dos serviços da organização.

A imagem a seguir ilustra os objetivos de controle do processo DS5:

Figura 18 - Objetivos de controle do processo DS5



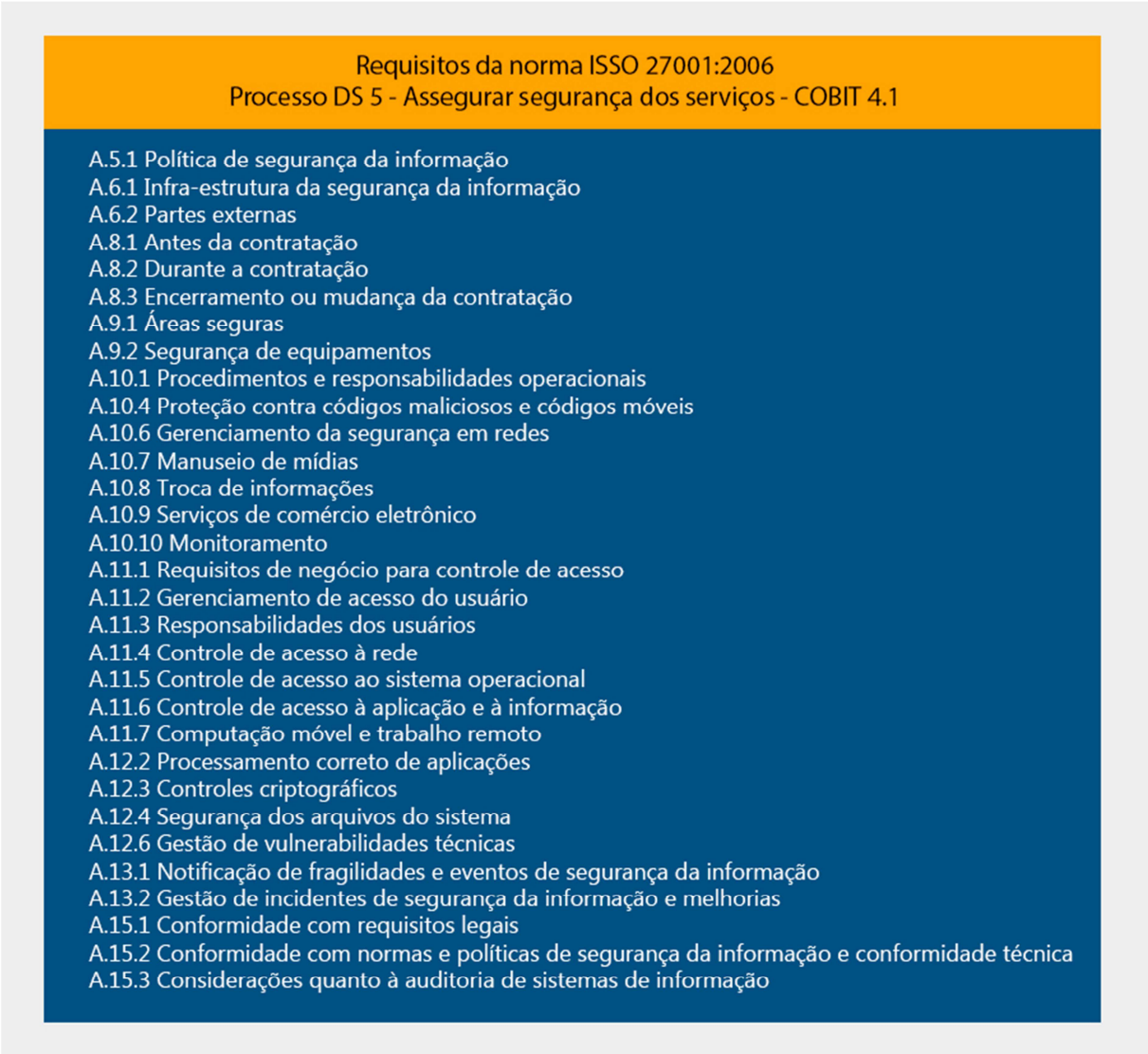
Fonte: Adaptado pelo autor (Cobit 4.1)

De acordo com os objetivos de controle do processo, foram desenvolvidas duas questões para cada, que visa a verificação do estado atual da T.I. da organização. Esta prática visa melhorar a taxa de precisão do método e empregar os conceitos anteriormente apresentados.

Os controles da ISO 27001:2006 equivalentes ao processo DS5, foram usados também para dar um melhor embasamento que se julgou necessário para a formulação das questões desenvolvidas e empregadas no método.

A figura a seguir exibe os controles da ISO 27001:2006 equivalentes ao processo DS5 do COBIT 4.1 que foram escolhidos:

Figura 19 - Requisitos da norma ISO 27001:2006 referente ao processo DS5 do Cobit 4.1



Fonte: Elaborado pelo autor, 2016

5.2.2 Processo de controle PO9 – Avaliar e Gerenciar os Riscos de T.I.

O processo PO9 – Avaliar e gerenciar os Riscos de T.I., tem como objetivo criar e manter uma estrutura de gestão do risco, visando ter uma documentação dos riscos, possíveis estratégias de mitigação dos riscos, tendo em vista que estes riscos mapeados ou possíveis riscos não mapeados, podem impactar de forma severa o negócio da organização.

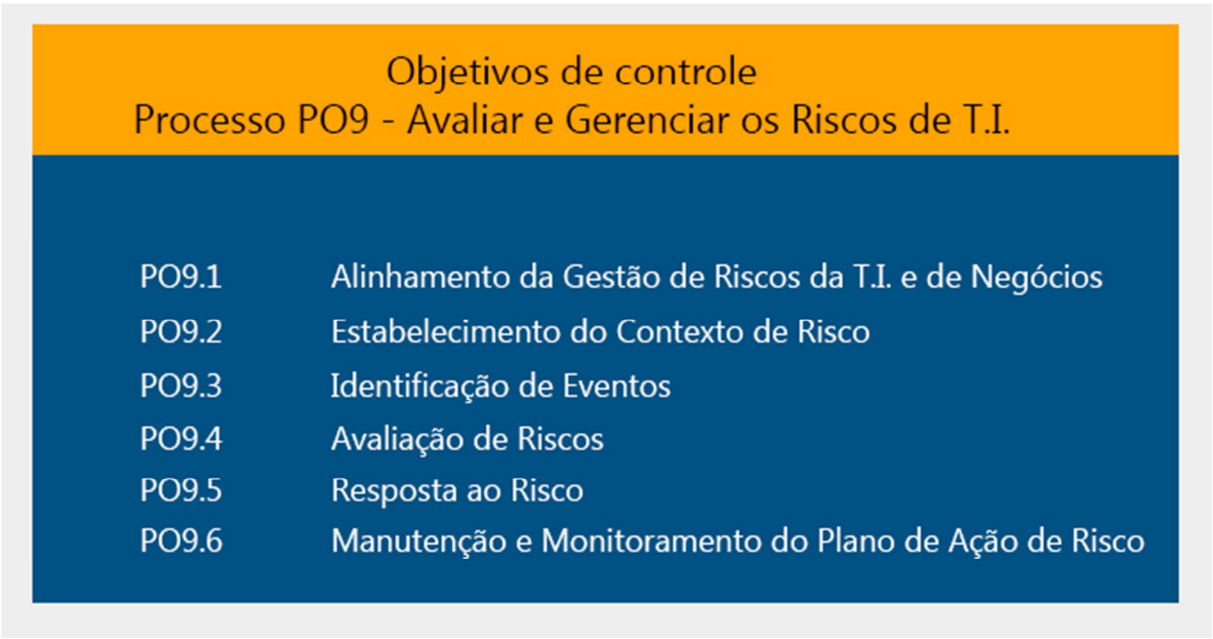
O processo também se preocupa em gerir os riscos residuais, riscos esses que a empresa os aceita e que precisam ser tratados de forma adequada, caso

contrário, poderá se tornar um problema maior para a organização e causará sem dúvidas, um impacto maior que o anteriormente esperado.

O PO9 também possui objetivos de controle, ao todo são 6 objetivos, que vão tratar pontos distintos, porém dentro do proposito principal do processo, que é avaliar e gerenciar o risco da T.I.

Os objetivos de controle estão ilustrados na figura abaixo:

Figura 20 - Objetivos de controle do processo PO9

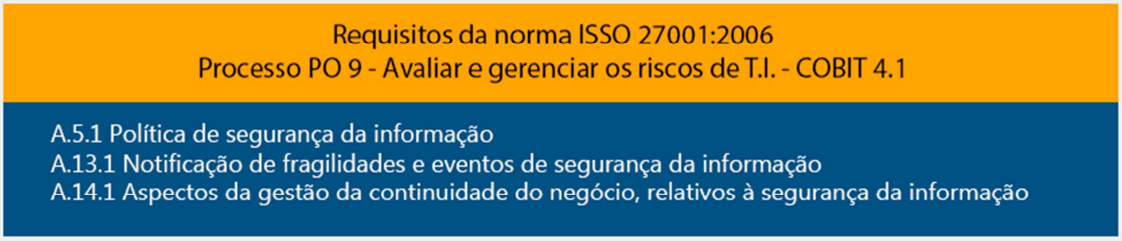


Fonte: Adaptado pelo autor (Cobit 4.1)

Para integrar o método, também foram formuladas 2 questões de cada objetivo de controle do processo PO9, visando dar uma melhor visão de como a T.I. da organização se encontra. Para a formulação das questões também foram utilizados os controles da ISO 27001:2006 equivalentes ao processo em questão. A partir deles pode-se obter melhor profundidade nas questões que foram desenvolvidas e que integram o método.

A figura a seguir ilustra os controles da ISO 27001:2006 equivalentes ao processo PO9:

Figura 21 - Requisitos da norma ISO 27001:2006 referente ao processo PO9 do Cobit 4.1



Fonte: Elaborado pelo autor, 2016.

6 ESTUDO DE CASO: APLICAÇÃO DO MÉTODO

Conforme anteriormente citado, o método que foi desenvolvido com base nos conceitos da computação em nuvem e seus serviços, ISO 27001 e Cobit 4.1, tem como objetivo avaliar uma organização e definir se de fato a mesma está pronta ou não para que possa de fato migrar para o serviço desejado pela direção e T.I. da organização.

Portanto, a aplicação em forma de um estudo de caso, visa a solidificação dos conceitos, bem como a prática e o resultado da efetividade do mesmo quando empregado em uma organização, seja ela pública ou privada.

A aplicação na organização foi feita através do método principal e a aplicação dos dois processos do Cobit que compõe o método por completo. Ambos anteriormente citados.

6.1 A ORGANIZAÇÃO E SUA T.I.

Para solidificação do método e do trabalho fora realizada a aplicação do método e esta foi feita em uma instituição de ensino superior pública.

A instituição possui alguns sistemas internos e também alguns de uso externo. Ela também já utiliza um sistema em nuvem, quando a mesma utiliza uma hospedagem externa para seu site próprio. A T.I. da organização possui alguns serviços como: servidores de arquivos, balanceador de cargas, proxy e outros diversos. Muitos destes serviços são rodados em servidores virtuais, o que diminui seu tempo de resposta e que demanda uma necessidade precisa de atenção quando se trata de backup de configurações e estados da virtualização. Por conta de sua limitação de equipamentos, e em alguns casos limitações de mão de obra especializada com domínio pleno de ferramentas, algumas aplicações tem seu gerenciamento feito de forma não apropriada e a aplicação não funciona da melhor forma.

Todo o processo de entrevista e avaliação foram realizadas com a equipe de T.I. local da organização em seu próprio setor e todo o material colhido da entrevista se encontra em tabelas que serão expostas a seguir no próximo capítulo.

6.2 APLICAÇÃO DO MÉTODO PRINCIPAL

A primeira aplicação feita foi do método principal, no qual colheu as informações com base nos requisitos que os serviços de nuvem requerem, para que possa haver de fato a migração e o funcionamento não possa ser comprometido e frustrante para a organização.

Abaixo pode-se observar nas tabelas o resultado extraído através da aplicação do método.

Tabela 2 - Resultado da aplicação do método principal

Conexão com Internet	Velocidade	A organização possui 3 links não dedicados de 20Mb de velocidade e um link dedicado de 10MB.
	Disponibilidade	O link tem quedas ou perdas de conexão em intervalos de 2 a 6 meses.
Licenciamento e suporte (Atualizações)	Licenciamentos	Totalmente licenciado
	Suporte especializado	É coberto pelo licenciamento
Sistemas Integrados	Sistemas de negócios	Todo sistema é provido pela central e não possui interferência de sistemas de terceiro.
Treinamento de uso da WEB	Usuários com capacitação de uso WEB	Todos os usuários possuem a mínima noção de uso.
Equipe de T.I.	Certificações	A organização não possui funcionários de T.I. certificados.
	Custo de funcionários	O custo não é calculado, tendo em vista que nenhum dos funcionários são de fato certificados.
Redundância de dados	Rotinas de Backup	Existe uma rotina empregada e a mesma é seguida de forma rígida.
	Disponibilidade dos dados	Os dados, quando necessários, são disponibilizados sem maiores problemas.

	Integridade dos dados	Todo backup é realizado em uma fita e um HD externo, mantendo uma redundância maior, diminuindo o risco de corrupção dos dados e diminuindo também sua integridade.
Escalabilidade	Adoção de novas tecnologias	A organização possui uma infraestrutura limitada dificultando a implementação de aplicações ou recursos que requerem maior poder computacional.
	T.I. e competitividade de mercado	Apesar da limitação de infraestrutura, a organização mantem um nível acima se comparada às organizações de ensino superior de sua região.
Infraestrutura física defasada	Capacidade de armazenamento limitado	A organização enfrenta um problema com a falta de falta de armazenamento.
	Processamento limitado	Há gargalos e muitas das vezes a T.I. não consegue entregar o que precisa de fato.
Segurança física	Acesso físico	Não possui medidas ou políticas que visam a proteção física.
	Acesso de terceiros	Não possui medidas ou políticas que visam a proteção física.
Segurança lógica	Criptografia	Há aplicações que possuem criptografia empregada, outras não.
	Complexidade de senhas	Não possui medidas ou políticas quanto a isso.
	Senhas padrão em equipamentos	Não possui medidas ou políticas quanto a isso.
Disponibilidade	Disponibilidade do sistema administrativo	O sistema administrativo não tem quedas ou paralização dos serviços necessários.
	Usabilidade dos equipamentos de T.I	Todos dentro da organização possuem equipamentos para realização do trabalho.
Riscos	Mapeamento	Não possui medidas ou políticas quanto a isso.

	constante dos riscos	
	Tratamento dos riscos	Não possui medidas ou políticas quanto a isso.
Política de segurança	Negócio e T.I.	Há um documento que de fato visa a divisão de serviços, mas não é seguida como deveria.
	Definição da política de segurança	Não possui medidas ou políticas quanto a isso.

Fonte: Elaborado pelo autor, 2016.

6.3 APLICAÇÃO DOS PROCESSOS DO COBIT

Após realizada a aplicação do método principal e ter-se obtido muitas informações relevantes e prioritárias que irá impactar diretamente no resultado, houve a aplicação dos processos do Cobit.

Ambos os processos de controle, DS5 e PO9, foram descritos anteriormente e tem seu papel de importância e impacto no resultado.

6.3.1 Aplicação do Processo de controle DS5

Nesta aplicação o objetivo era identificar como eram feitos os controles na organização que deveriam assegurar a segurança dos serviços que a mesma deveria prover.

A avaliação se embasava em todos os 11 controles que o processo DS5 possuía e de acordo com eles obter o resultado do nível de maturidade do mesmo.

Abaixo pode se observar o resultado da aplicação, bem como o nível de maturidade atingido pela organização no processo de controle.

Tabela 3 - Resultados obtidos através da aplicação do processo de controle DS5

Abordagem	Nota preliminar	Maturidade Preliminar
DS5.1 Gestão da Segurança de TI Q1 - As decisões de negócio e TI são tomadas em conjuntos? Q2 - Todas as decisões antes mesmo de tomadas são comunicadas de um para o outro?	0	0
DS5.2 Plano de Segurança de TI Q1 - Existem políticas de segurança implementadas na organização? Q2 - A organização possui treinamentos e simulações quanto as políticas de segurança empregadas?	0	0
DS5.3 Gestão de Identidade Q1 - Todos os acessos dentro da organização são realizados através de logins únicos? Q2 - Os níveis de acessos de cada usuário condizem com sua necessidade de acesso dentro da organização?	1	1
DS5.4 Gestão de Contas de Usuário Q1 - Existe uma gestão de privilégio de cada usuário dentro da organização? Q2 - Há uma rotina de revisões de privilégios de acesso dos usuários?	0	0
DS5.5 Teste de Segurança, Vigilância e Monitoramento Q1 - A organização possui rotinas de testes de segurança que garanta uma melhoria continua da mesma? Q2 - Existe uma preocupação em avaliação de logs de segurança?	0	0
DS5.6 Definição de Incidente de Segurança Q1 - Incidentes de segurança são definidos e comunicados? Q2 - Existem tratamentos definidos de forma diferente entre os diversos tipos de segurança?	0	0
DS5.7 Proteção da Tecnologia de Segurança Q1 - Os acessos a tecnologias de segurança empregadas na empresa são devidamente assegurados? Q2 - Documentos de segurança são devidamente mostrados somente quando necessário e por funcionários que devem ter acesso?	0	0
DS5.8 Gestão de Chave Criptográfica Q1 - Existe implementado na organização criptografia em sistemas e acessos? Q2 - Há uma gestão das chaves da criptografia empregada, garantindo mudança, revogação ou até mesmo a destruição da mesma?	0	0
DS5.9 Prevenção, Detecção e Correção de Software Malicioso Q1 - Existe uma rotina de medidas preventivas logica e física através de	1	1

aplicações de patches e service packs? Q2 - Há um sistema de antivírus prevenindo a organização de vírus, malware, spans, entre outros?		
DS5.10 Segurança de Rede Q1 - A organização possui mecanismos de segurança de rede como firewall, sistema de detecção de intrusão, segmentação de rede, entre outros? Q2 - Como é feita a gestão da segurança de rede?	1	1
DS5.11 Comunicação de Dados Confidenciais Q1 - O TI possui formas de autenticações rígidas que garanta segurança nas comunicações confidenciais na organização? Q2 - Todas autenticações realizadas em redes de maior confidencialidade geram comprovantes de entrega e recebimento?	0	0

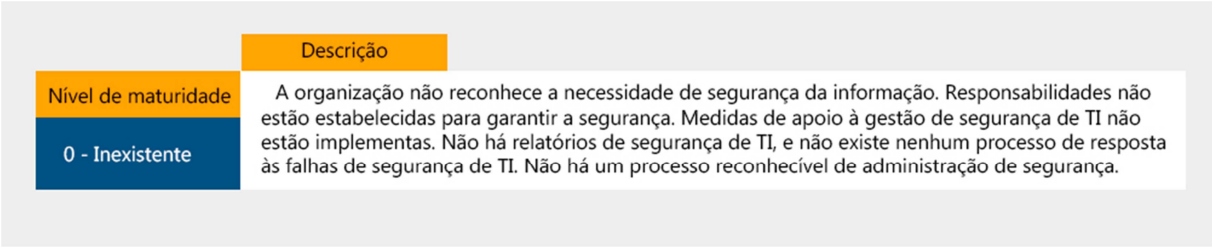
Fonte: Elaborada pelo autor, 2016.

A partir da tabela acima pôde-se concluir de que o nível de maturidade atual da organização, quando se diz respeito ao processo de controle DS5, é de 0.

De acordo com o Cobit 4.1 o nível de maturidade 0 significa que o processo em questão é inexistente dentro da organização.

Abaixo, através da figura, podemos observar o que o Cobit 4.1 diz a respeito do nível 0 quando alcançado no processo de controle DS5.

Figura 22 - Definição do nível de maturidade 0 no processo de controle DS5 pelo Cobit 4.1



Fonte: Adaptado pelo autor (Cobit 4.1)

6.3.2 Aplicação do Processo de controle PO9

Nesta aplicação o objetivo era identificar como eram feitos os controles na organização que deveriam avaliar e gerenciar os riscos de T.I. que a organização possui.

A avaliação se embasava em todos os 6 objetivos de controles que o processo de controle PO9 possuía e de acordo com eles obter o resultado do nível de maturidade do mesmo.

Abaixo pode se observar o resultado da aplicação, bem como o nível de maturidade atingido pela organização no processo de controle.

Tabela 4 - Resultados obtidos através da aplicação do processo de controle PO9

Abordagem	Nota preliminar	Maturidade Preliminar
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios Q1 - É realizado o gerenciamento de riscos pela organização? Q2 - O gerenciamento dos riscos de TI é alinhado aos riscos da organização?	0	0
PO9.2 Estabelecimento do Contexto de Risco Q1 - Há uma contextualização dos riscos quando o mesmo é interno ou externo? Q2 - A organização toma um cuidado quanto a definir o objetivo da avaliação?	0	0
PO9.3 Identificação de Eventos Q1 - Há mecanismos para identificação de eventos que são danosos a organização? Q2 - Existe uma preocupação em registrar e manter o histórico de riscos mais relevantes?	0	0
PO9.4 Avaliação de Risco Q1 - Assim que identificado os riscos, é avaliada regularmente a probabilidade de impacto de todos através de métodos qualitativos e quantitativos? Q2 - Todos os riscos estão devidamente categorizados de acordo com a organização?	0	0
PO9.5 Resposta ao Risco Q1 - Existem respostas previamente separadas para cada risco anteriormente catalogado? Q2 - O processo de resposta ao risco é rigorosamente seguido?	0	0
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco Q1 - Existe uma preocupação em planejar e monitorar os planos de ações destinados aos riscos que a organização possui? Q2 - Os controles das atividades são devidamente implementados em todos os níveis da organização?	0	0

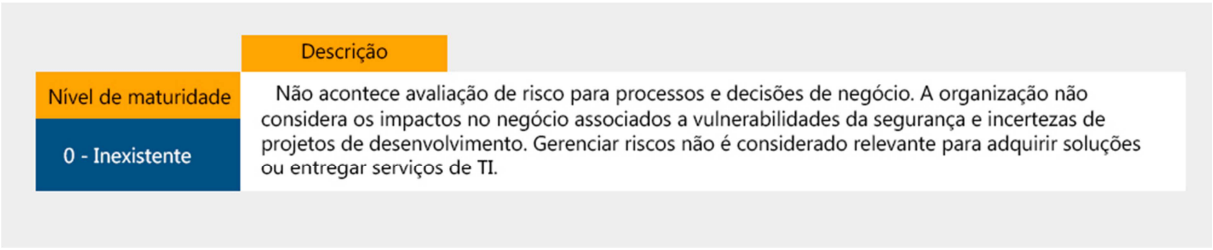
Fonte: Elaborada pelo autor, 2016.

A partir da tabela acima pode-se concluir de que o nível de maturidade atual da organização, quando se diz respeito ao processo de controle PO9, é de 0.

De acordo com o Cobit 4.1 o nível de maturidade 0 significa que o processo em questão é inexistente dentro da organização.

Abaixo, através da figura, podemos observar o que o Cobit 4.1 diz a respeito do nível 0 quando alcançado no processo de controle PO9.

Figura 23 - Definição do nível de maturidade 0 no processo de controle PO9 pelo Cobit 4.1



Fonte: Adaptado pelo autor (Cobit 4.1)

6.4 RESULTADO DA APLICAÇÃO

Com base na auditoria dos processos do Cobit, fica evidenciado que não existe segurança necessária para garantir um adequado funcionamento das aplicações quando houver um incidente de segurança. Sendo assim, a organização deveria migrar para um serviço de nuvem. O serviço mais indicado mediante a tabela a seguir, é o IaaS, entregando assim para a organização a infraestrutura de T.I. necessária para que seu poderio de entrega e suporte seja nivelada com as necessidades da organização.

Tabela 5 - Indicativas para migração para o modelo de serviço em nuvem: Infraestrutura como serviço (IaaS)

Equipe de T.I.	Certificações	A organização não possui funcionários de T.I. certificados.
Escalabilidade	Adoção de novas tecnologias	A organização possui uma infraestrutura limitada dificultando a implementação de aplicações ou recursos que requerem maior poder computacional.

Infraestrutura física defasada	Capacidade de armazenamento limitado	A organização enfrenta um problema com a falta de falta de armazenamento.
	Processamento limitado	Há gargalos e muitas das vezes a T.I. não consegue entregar o que precisa de fato.
Segurança física	Acesso físico	Não possui medidas ou políticas que visam a proteção física.
	Acesso de terceiros	Não possui medidas ou políticas que visam a proteção física.
Segurança lógica	Criptografia	Há aplicações que possuem criptografia empregada, outras não.
	Complexidade de senhas	Não possui medidas ou políticas quanto a isso.
	Senhas padrão em equipamentos	Não possui medidas ou políticas quanto a isso.
Riscos	Mapeamento constante dos riscos	Não possui medidas ou políticas quanto a isso.
	Tratamento dos riscos	Não possui medidas ou políticas quanto a isso.
Política de segurança	Negócio e T.I.	Há um documento que de fato visa a divisão de serviços, mas não é seguida como deveria.
	Definição da política de segurança	Não possui medidas ou políticas quanto a isso.

Fonte: Elaborada pelo autor, 2016.

Porém, por outro lado, a tabela a seguir evidência que a organização deveria primeiro realizar a migração ou contratação de link de maior velocidade e disponibilidade, pois com a configuração do atual link não será possível obter bons resultados transferindo os serviços para nuvem. A migração implicaria em lentidão e até mesmo a não entrega ou resposta quando houvesse requisição à algum serviço.

Tabela 6: Indicativos que impedem a migração para serviço em nuvem

Conexão com Internet	Velocidade	A organização possui 3 links não dedicados de 20Mb de velocidade cada e um link dedicado de 10MB.
	Disponibilidade	O link tem quedas ou perdas de conexão em intervalos de 2 a 6 meses.

Fonte: Elaborada pelo autor, 2016.

7 CONSIDERAÇÕES FINAIS

De fato, a importância que a informação tem para a organização é enorme, e mediante ao volume imenso e a sua importância, é preciso que o tratamento da mesma seja feito de forma condizente.

Entende-se então, que a aplicação de uma boa governança de T.I., apoiando assim, de forma correta o negócio, são de extrema importância, o que leva a consideração de utilização de frameworks como o do Cobit, embasando-se sempre na norma ISO 27001.

Ir para nuvem, levando informações que são de vital importância para uma organização, é preocupante, e conforme mencionado anteriormente não é de fato aconselhável a migração sem que se analise alguns requisitos seja feita e principalmente sem possuir uma gestão sólida.

O método que fora desenvolvido e aplicado proporcionou um aprofundamento em questões que devem ser analisadas para que, de fato, a segurança da informação seja efetiva quando uma organização projeta o desejo de uma mudança de como vai executar ou prover seus serviços. Sendo assim, o método, abordando e possuindo como seu objetivo a preocupação que a organização deve entender e absorver sobre ela mesma antes da mesma migrar para um serviço em nuvem, deve entender o quanto pode-se ganhar realizando a gestão da informações e processos que envolve a T.I. e o negócio.

Este trabalho visou destacar as opções de serviços em nuvem e seus benefícios de uso e também a importância de uma governança de T.I. suprindo as necessidades da organização quanto a segurança da informação. Fica de fato evidenciado o quão interessante pode vir a ser esta possível mudança para uma organização, porém, também é destacado que os perigosos de uma migração sem antes a aplicação de métodos de verificação de compatibilidade, pode frustrar a organização, fazendo com que a mesma possa migrar sem estar de fato preparada. A organização poderia perder informações importantes e acabar tendo mais problemas, do que de fato, tendo as soluções anteriormente previstas e desejadas.

É importante destacar que este método pode ser evoluído mediante a seleção de outros processos do Cobit e do framework PMBOK, alinhados com segurança da informação, bem como requisitos de normas e questões dirigidas, tornando-o mais robusto e adequado ao mercado em que as organizações estão inseridas.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO, Márcio Tadeu; FREITAS FERREIRA, Fernando Nicolau. **Política de Segurança da Informação: Guia prático para elaboração e implementação** – Rio de Janeiro: Editora Ciência Moderna, 2006. 224p.

ARAÚJO, Victor Melo. **Segurança da Informação: Uma abordagem holística com foco na implantação de um SGI**. 2015. 44p.

ABNT – **Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2005.

BARBOSA, Andressa Munhoz. **Governança de TI: COBIT; ITIL**. Revista Cientifica Eletrônica de Administração, Garça - Sp, v., n. 19, p.21-33, fev. 2011.

BORGES, Hélder Pereira; SOUZA, José Neuman de; SCHULZE, Bruno; MURY, Antonio Roberto. **Computação em Nuvem.** 2014. 48 f. TCC (Graduação) - Curso de Ciência da Computação, Instituição Federal de Educação, Ciência e Tecnologia do Maranhão, São Luís.

CAMPOS, André. **Sistema de Segurança da informação: Controlando os Riscos.** 2.ed. Florianópolis: Visual Books, 2007.

Cobit 4.1 - Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>. Acesso em: set. 2016.

DANTAS, Marcus Leal. **Segurança da Informação: Uma Abordagem Focada Gestão de Riscos**. Olinda: Livro Rápido, 2011. 152 p.

ELSENPETER, Robert; VELTE, T. Anthony; VELTE, J. Toby. **Cloud Computing: Uma Abordagem Prática**. Alta Books, 2011. 352p.

FERREIRA, Fernando Nicolau Freitas
ARAÚJO, Márcio Tadeu - **Políticas de segurança da informação - Guia prático para elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008. 224p.

FONTES, Edison Luiz Gonçalves. **Segurança da informação: O Usuário faz a Diferença.** - São Paulo: Saraiva, 2006. 168p.

ISO 27001 - Disponível em: <https://www.27001.pt/>. Acesso em acesso em: 13 set. 2016.

IT GOVERNANCE INSTITUTE (ITGI) - **Governança de TI** - Disponível em: <http://www.geraldoloureiro.com/wiki/index.php?title=P%C3%A1gina_principal> Acesso em: 12 set. 2016.

MOHAMED, Arif. **A History of Cloud Computing**. Computer. Weekly, march 2009. http://www.computerweekly.com/Articles/2009/06/10/235429/A-history-of-cloud-computing.htm. Acesso em: 27 Jul. 2011.

National Institute of Standars and Technology - **The NIST Definition of Cloud Computing.** Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 21 ago. 2016.

OLIVEIRA, Dhiego Alves; LOPES, Kelvin Dias; ROCHA, Mário Carneiro. **Cloud Computing: Definições e análise para Além das Vantagens.** 2015. Canindé. Disponível em: <http://www.infobrasil.inf.br/userfiles/16-S3-2-97220-Cloud%20computing___.pdf>. Acesso em: 17 set. 2016.

Profissionais de TI, **O que é Governança de TI.** Disponível em: <https://www.profissionaisti.com.br/2009/03/o-que-e-governanca-de-ti/>. Acesso em 11 de out de 2016.

RITTINGHOUSE, John W; RANSOME, F. James. **Cloud Computing: Implementation, Management and Security.** CRC PRESS, 2009.

TAURION, Cezar. **Cloud Computing: computação em nuvem: Transformando o Mundo da Tecnologia da Informação**. Rio de Janeiro: Brasport, 2009.

VERAS, Manoel de Sousa Neto. **Arquitetura de Nuvem: Amazon Web Services (AWS)**. São Paulo: Brasport, 2013. 570 p.

VERAS, Manoel de Sousa Neto. **Computação em Nuvem: Nova Arquitetura de TI**. [s.i]: Brasport, 2015. 192 p.

VERAS, Manoel de Sousa Neto**. Virtualização (2ª edição): Tecnologia Central do Datacenter**. 2. ed. São Paulo: Brasport, 2016. 224 p.

WEILL, Peter; ROSS W. Jeanne. **Governança de Tecnologia da Informação**. São Paulo: M.books do Brasil, 2006. 276 p.