UNIVERSIDADE FEDERAL DO CEARÁ-CAMPUS QUIXADÁ
CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES

MARIA PATRÍCIA HOLANDA DA SILVA

UMA METODOLOGIA PARA MELHORAR A SEGURANÇA EM AMBIENTES DE COMPUTAÇÃO EM NUVEM - ESTUDO DE CASO

QUIXADÁ
2019

MARIA PATRÍCIA HOLANDA DA SILVA

UMA METODOLOGIA PARA MELHORAR A SEGURANÇA EM AMBIENTES DE COMPUTAÇÃO EM NUVEM - ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnóloga em Redes de Computadores.

Orientador: Prof. Dr. Alberto Sampaio Lima

QUIXADÁ

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S581m Silva, Maria Patrícia Holanda da.
Uma metodologia para melhorar a segurança em ambientes de computação em nuvem : Estudo de caso / Maria Patrícia Holanda da Silva. – 2019.
41 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Redes de Computadores, Quixadá, 2019.
Orientação: Prof. Dr. Alberto Sampaio Lima.

1. Computação em Nuvem. 2. Gerenciamento de Serviços de TI. 3. Segurança da Informação. I. Título.

CDD 004.6

MARIA PATRÍCIA HOLANDA DA SILVA

UMA METODOLOGIA PARA MELHORAR A SEGURANÇA EM AMBIENTES DE COMPUTAÇÃO EM NUVEM - ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnóloga em Redes de Computadores.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

Prof. Dr. Alberto Sampaio Lima (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Wladimir Araújo Tavares
Universidade Federal do Ceará (UFC)

Prof. Me. Francisco Erivelton Fernandes de Aragão
Universidade Federal do Ceará (UFC)

À minha família, por sua capacidade de acreditar em mim. Ao meu namorado, minhas amigas e amigos por me incentivarem a continuar e concluir esse trabalho.

AGRADECIMENTOS

Agradeço, primeiramente, à Deus que me deu o apoio para concluir esse trabalho. Agradeço aos meus pais que me incentivaram todos esses anos. Aos meus colegas de sala, especialmente aqueles nos quais encontrei bons amigos. Aos colegas de trabalho por me motivarem. Ao meu namorado por me ouvir e apoiar. Agradeço aos professores, coordenadores do curso e demais servidores da universidade. E em especial agradeço ao meu orientador por sua empatia e por me ajudar a cumprir essa etapa.

“A persistência é o caminho do êxito.”

(Charles Chaplin)

RESUMO

A convergência e o aperfeiçoamento de tecnologias resultou no paradigma de computação em nuvem. Esse novo modelo de entrega de serviços de T.I. simultaneamente trouxe melhorias e redução de custos para as empresas mas também lançou novos desafios de segurança da informação. Esse trabalho teve como objetivo estabelecer uma metodologia organizada em uma abordagem de processos de melhoria continuada, visando identificar passos que possam ser adotados por gestores de T.I. para melhoria da segurança em uma nuvem privada. O trabalho foi estruturado como um estudo de caso, no qual a metodologia foi aplicada parcialmente. A partir desse estudo evidenciou-se a necessidade de investimento na estrutura para atender a princípios essenciais da computação em nuvem como a disponibilidade e o amplo acesso.

Palavras-chave: 1. Computação em nuvem. 2. Gerenciamento de Serviços de TI. 3. Segurança da informação.

ABSTRACT

Convergence and enhancement of technologies has resulted in the cloud computing paradigm. This new I.T. service delivery model has simultaneously brought improvements and cost savings to enterprises, but has also introduced new information security challenges. This paper aimed to establish a methodology organized in a continuous improvement process approach, aiming to identify steps that can be adopted by managers of I.T. to improve security in a private cloud. The work was structured as a case study, in which the methodology was partially applied. From this study the need to invest in the structure to meet key principles of cloud computing such as availability and broad access was evidenced.

Keywords: 1. Cloud Computing. 2. IT Service Management. 3. Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

À medida que as redes globais expandem a interconexão dos sistemas de informação, o funcionamento satisfatório das soluções de comunicação e computação torna-se vital. Contudo, eventos recorrentes como vírus e *worms* e o sucesso dos criminosos ilustram as deficiências das atuais tecnologias da informação e a necessidade de Segurança desses sistemas (WHITMAN, 2011).

A convergência e o aperfeiçoamento de tecnologias como virtualização de servidores, *Grid Computing, Utility Computing* contribuíram para o desenvolvimento da Computação em Nuvem. Que atualmente tem ganhado mais espaço no mercado que busca por eficiência. Com o aumento da demanda dessas tecnologias, cresce também os riscos inerentes à esse paradigma. Portanto pode-se afirmar necessária a implantação de mecanismos de segurança que possam prover controles condizentes com a complexidade de gerenciamento dessa infraestrutura.

A computação em nuvem tem se tornado a palavra da moda na indústria de TI (WANG et al., 2010; VOUK, 2008) com o objetivo de proporcionar serviços sob demanda com pagamento baseado no uso (*pay-per-use*). Tendências anteriores à computação em nuvem foram limitadas a uma determinada classe de usuários ou focadas em tornar disponível uma demanda específica de recursos de TI (BUYYA *et al.*, 2009). De acordo com Fenner (2019), a computação em nuvem é uma tendência recente de tecnologia muito utilizada por empresas que buscam reduzir seus custos, alugando capacidade de processamento e armazenamento. Usuários de serviços tecnologia da informação (TI) e várias empresas consolidadas no mercado tem optado pela adoção de soluções na nuvem em substituição ao paradigma *on premise*.

Provedores de serviços em nuvem oferecem a entrega de serviços sob medida, de acordo com a demanda dos seus clientes. A responsabilidade pela gestão dos serviços deixa de ser do cliente passando a ser do provedor. Entre os principais pontos que necessitam ser muito bem gerenciados pelo provedor de serviços de nuvem, destaca-se a gestão de segurança da informação. O provedor necessita de políticas eficazes, bem como de processos que possam ser efetivamente utilizados na gestão de segurança. A avaliação periódica do contexto de segurança é uma necessidade dos gestores dos provedores de serviços em nuvem.

Em ambientes de segurança em TI, muitas vezes os requisitos técnicos de segurança são subjugados aos requisitos funcionais, deixando informações sensíveis ao negócio expostas às ameaças.

Faz-se necessária uma adequada gestão da segurança da informação, no sentido

de que, através da padronização dos procedimentos, processos e das respostas a incidentes, seja possível reduzir os riscos e mitigar os danos causados por incidentes. Ainda com relação a gestão dos riscos, a questão ganha maior notoriedade quando se trata de dados de clientes. Há a necessidade de ações que resultem em uma nuvem que atenda aos requisitos técnicos de segurança, estejam alinhadas aos objetivos de negócio e sejam gerenciáveis.

A presente pesquisa apresenta uma metodologia para melhorar o processo de gerenciamento de segurança em ambientes de computação em nuvem. Através de um estudo de caso realizado em uma nuvem privada do campus da UFC em Quixadá resultados iniciais indicaram sua utilidade na identificação de pontos para melhoria na gestão de segurança da nuvem, como por exemplo a necessidade de redundância e garantia da disponibilidade em caso de oscilações na rede. Dessa forma, a proposta se mostrou efetiva, contribuindo para a atuação dos gestores na área de segurança da informação em ambientes de nuvem.

2 TRABALHOS RELACIONADOS

Os trabalhos relacionados selecionados tratam dos desafios da segurança e governança de T.I na Computação em Nuvem.

No artigo (CASTRO; SOUSA, 2017) pontuam que os processos negociais e de segurança devem estar harmonizados, de forma que os riscos possam ser gerenciados ao mesmo tempo em que as necessidades do negócio são atendidas. O artigo fala ainda que o modelo de nuvem privada é o que apresenta os menores riscos, quando comparado aos demais modelos. Em contrapartida possui dificuldade de gerenciamento por estar atrelado aos processos corporativos. Diferentemente da nuvem pública, a nuvem privada não possui restrições para a aplicação de técnicas de autorização, autenticação e gerenciamento de redes. A publicação aponta a precedência dos requisitos funcionais sobre os requisitos de segurança, o que segundo este, contribui para o desenvolvimento de sistemas e ambientes extremamente vulneráveis a ataques externos. Em se tratando dos riscos associados à Computação em Nuvem, as questões situam-se no âmbito da privacidade e da segurança das informações residentes na nuvem. Os autores questionam como podem exigir garantias de que as informações residentes na Nuvem estão realmente seguras. O artigo ressalta ainda que entre os objetivos de Gestão de Riscos estão a proteção da informação baseada em ativos, planos de mitigação de riscos, proteção baseada no risco ou ameaça sofrida por determinado ativo, e na utilização de uma metodologia de gestão de risco que abranja toda a organização. A principal contribuição do artigo para este trabalho, encontra-se na seção 5.4 que trata dos Requisitos para Gestão de Risco na Nuvem, requisitos estes que serão utilizados nesse trabalho a fim complementar a metodologia de segurança proposta.

O segundo artigo apresenta a implantação de uma nuvem privada como solução aos riscos de segurança enfrentados pela nuvem pública. No qual (RISTOV SASKO, 2013) analisa as vulnerabilidades de nuvens públicas e privadas em instâncias de máquinas virtuais com o OpenStack. E procura evidenciar por meio da verificação de uma de suas hipótese, que a solução de computação em nuvem é mais vulnerável internamente do que externamente. E que portanto os sistemas são mais vulneráveis se o atacante estiver na mesma LAN.

Em (MARTINS; SANTOS, 2005) o autor estabelece uma metodologia para a implantação de um SGSI, baseada em normas e padrões internacionais, como a ISO/IEC TR 13335-2 e BS 7799. O trabalho em questão possui proximidade porque também procura estabelecer uma metodologia de segurança alicerçada em por padrões de segurança vigentes e nos moldes da técnica PDCA. Este trabalho diferencia-se de (MARTINS; SANTOS, 2005) por tratar-se de uma

metodologia para melhoria da segurança em uma nuvem privada independente de organização possuir um SGSI implantado.

A dissertação de (FERREIRA, 2013), foi relevante para este trabalho ao elencar riscos encontrados no paradigma da computação em nuvem. Entre eles a possobilidade de a utilização dos serviços em nuvem poder impactar na observância de padrões, ocasionado uma dificuldade nos processos de auditoria. O risco à disponibilidade dos dados, autenticação e autorização, backup de dados ou a própria exclusão acidental de máquinas virtuais, ataques entre outros. Além disso, (FERREIRA, 2013) divide os riscos em organizacional e políticas legal e técnico que será também utilizada por esse trabalho.

Em (FERREIRA, 2017), se realiza a implantação de uma nuvem privada confiável baseada no OpenStack.

A migração de um ambiente de servidor de TI convencional para um paradigma de nuvem coloca novos desafios e riscos e oferece oportunidades de redução de custos (KRUTZ RONALD L, 2010). Segundo Sousa et al.(2010). a computação em nuvem tem por objetivo proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso. Na adoção do modelo de Computação em Nuvem os processos de negócios e procedimentos precisam levar em conta a segurança e privacidade das informações que ficarão na nuvem (Castro et. al).

3 OBJETIVOS

3.1 Objetivo Geral

Elaborar uma metodologia conceitual que contribua para melhorar a segurança em ambiente de computação em nuvem privada baseada no modelo IaaS.

3.2 Objetivos Específicos

- Identificar as vulneralidades inerentes ao paradigma da computação em nuvem, mais especificamente, relacionados ao modelo de nuvem privada;
- Levantar e selecionar os controles para o adequado gerenciamento vulnerabilidades identificadas.
- Prover uma metodologia que auxilie profissionais de T.I. na elaboração de políticas de segurança para nuvens privadas.

4 FUNDAMENTAÇÃO TEÓRICA

4.1 Governança de Tecnologia da Informação

De acordo com (HAES; GREMBERGEN, 2004), a governança de TI é um conceito em que não é possível precisamente afirmar quando surgiu, e que já em 2004 havia tornado-se rapidamente uma importante questão no campo da tecnologia da informação.

> A governança de TI é responsabilidade do Conselho de Diretores e gerência executiva. É parte integrante da governança corporativa e consiste na liderança e organização de estruturas e processos que asseguram que a TI sustenta e amplia a estratégia e os objetivos da organização.

[1]

Uma das questões levantadas no artigo IT Governance and Its Mechanisms acerca de como proceder a implantação da governança de TI em uma organização, leva a conclusão de que pode ser realizada por meio de estruturas, processos e mecanismos relacionais. Além de que o que funciona para uma organização não necessariamente funcionará para outra. O que isso quer realmente dizer? Isso implica que as estruturas estão relacionadas a existência de funções responsáveis, os processos referem-se ao monitoramento e a tomada de decisão (SLA's, COBIT e ITIL dentre outros) e, os mecanismos relacionais incluem o compartilhamento de aprendizagem e diálogo entre TI/negócios (sendo estes últimos entendidos como os objetivos da organização, seja ela comercial ou não).

A TI é uma ferramenta fundamental para as organizações, requer alto grau de investimento e com frequência não gera totalmente o retorno esperado.

De acordo com (FENNER, 2019), nos últimos anos, o termo governança vem ganhando a atenção das organizações devido à necessidade em adotar uma abordagem para responder as exigências e desafios dos negócios globais. O autor afirma que para o IT Governance Institute (ITGI), o termo governança de tecnologia da informação (TI) envolve um conjunto de estruturas e processos que visa garantir que a TI suporte e maximize adequadamente os objetivos e estratégias de negócio da organização, adicionando valores aos serviços entregues, balanceando os riscos e obtendo o retorno sobre os investimentos em TI. Diversas áreas estão tendo algum tipo de intervenção para gerar melhorias. São intervenções que vão desde a criação

[1] IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives

e estabelecimento de padrões, modelos de processos, documentações, alternativas para criação de indicadores de desempenho. A governança de TI é responsabilidade dos executivos e da alta direção da empresa, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. É responsabilidade da governança de TI integrar e institucionalizar boas práticas para garantir que os objetivos de negócios sejam suportados. Por meio de uma boa gestão de governança de TI, torna-se possível obter vantagens da informação, maximizando os benefícios, aumentando as oportunidades e ganhando em poder competitivo. A governança de TI deve envolver os executivos, a alta direção, nas tomadas de decisões relacionados ao uso da TI no negócio. É fundamental que gestores de TI participem da tomada de decisão.

4.2 COBIT: O guia de melhores práticas

De acordo com (FENNER, 2019), o guia COBIT (*Control Objectives for Information and Related Technologies*) foi a primeira iniciativa desenvolvida para a criação de um padrão que possibilita aos profissionais da TI, terem orientações sobre o que fazer para desenvolver e aplicar a Governança de TI dentro das organizações. Atualmente se encontra em sua quinta versão, utilizada como referência na presente pesquisa. Desenvolvido pela Information System Auditand Control (ISACA), ele é um guia, estruturado como framework, que possui uma série de componentes que podem ser usados como modelo de referência para gestão da TI. O COBIT pode ser utilizado como alternativa visando à otimização dos investimentos de TI como, por exemplo: melhorar o retorno de investimento (ROI) com a utilização de indicadores de desempenho para avaliação de performance e dos resultados. O guia COBIT também pode ser usado para avaliar o nível de maturidade da empresa. A utilização do COBIT independe do tipo da plataforma de TI, do tipo de negócio e da participação que a TI tem na empresa. (FENNER, 2019) afirma que o guia COBIT, em sua quinta versão, ajuda as organizações a criar valor para TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos. Os objetivos do COBIT incluem:

- Oferecer um framework abrangente que auxilia as organizações a otimizar o valor gerado pela TI;
- Permitir que a TI seja governada e gerenciada de forma holística para toda a organização;
- Criar uma linguagem comum entre TI e negócios para a governança e gestão de TI corporativa.

De acordo com a (BUYYA *et al.*, 2013), as organizações e seus executivos se esforçam para:

- Manter informações de alta qualidade para apoiar decisões corporativas;
- Agregar valor ao negócio a partir dos investimentos em TI, ou seja, atingir os objetivos estratégicos e obter benefícios para a organização através da utilização eficiente e inovadora de TI;
- Alcançar excelência operacional por meio da aplicação confiável e eficiente da tecnologia;
- Manter o risco de TI em um nível aceitável;
- Otimizar o custo da tecnologia e dos serviços de TI;
- Cumprir as leis, regulamentos, acordos contratuais e políticas pertinentes cada vez mais presentes.

Organizações bem-sucedidas reconhecem que a diretoria e os executivos devem aceitar que a TI é tão significativa para os negócios como qualquer outra parte da organização. Diretores e gestores - Seja em funções de TI ou de negócios - devem colaborar e trabalhar em conjunto a fim de garantir que a TI esteja inclusa na abordagem de governança e gestão. Além disso, cada vez mais leis e regulamentos estão sendo aprovados e estabelecidos para atender a essa necessidade. As partes interessadas, também referenciadas pelo termo *stakeholder*, podem ser os clientes internos de uma organização, os usuários que necessitam dos serviços de TI para realizar as suas ações. No cenário de IaaS, são os clientes que através da nuvem, acessam aos serviços (rede, processamento, armazenamento) ofertados pelo provedor, organização, empresa que utiliza este modelo de negócio. Organizações existem para criar valor para suas partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos.

4.3 ITIL

ITIL (*Information Technology Infrastructure Library*) fornece uma descrição detalhada de várias práticas importantes de TI, com compreensivas listas de verificação, tarefas, procedimentos e responsabilidades que podem ser sob medida para qualquer para qualquer organização. Onde possível, essas práticas devem ser definidas como processos, cobrindo as principais atividades dos serviços de T.I. (BON, 2007)

De acordo com (BON, 2007) no livro *Foundations of IT Service Management, based on* ITIL, os processos de gerenciamento de serviços de TI são melhor compreendidos no contexto

dos conceitos de organização, qualidade e serviços.

Serviços e qualidade: os serviços são providos através da interação com o cliente/usuário. As organizações são frequentemente dependentes de seus serviços de T.I., não apenas para suporte, mas também para apresentar novas opções para implementar os objetivos da organização. Nesse contexto descrito pelo autor e traçando um paralelo com o trabalho proposto a elaboração de uma metodologia de segurança encontra o desafio de prover um método capaz de predizer o comportamento eficaz da Unversidade Federal do Ceará frente a exploração de uma vulnerabilidade na nuvem do campus.

4.4 Norma Brasileira ISO/IEC 27002

Esta norma é parte da família de normas 27000 a qual refere-se a implantação de um Sistema de Gestão de Segurança da Informação (SGSI). Trata-se de um código de prática para a gestão da segurança da informação. Ainda de acordo com texto da referida norma, esta é idêntica a norma ISO/IEC 17799:2005 que em 2007 por meio de publicação de errata passou a nomenclatura de ISO/IEC 27002:2005.

4.5 Segurança da Informação

De acordo com a norma (ABNT, 2005), Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades. A Segurança da informação protege a confidencialidade, integridade e disponibilidade, armazenagem, processamento ou transmissão. É obtida através do Aplicação de políticas, educação, treinamento e conscientização, e tecnologia (WHITMAN, 2011). Ainda segundo o Committee on National Security Systems (CNSS):

> O Comitê de Sistemas de Segurança Nacional (CNSS) define a segurança da informação como a proteção da informação e seus elementos críticos, incluindo os sistemas e hardware que usam, armazenam e transmitem essas informações. A segurança da informação inclui as áreas abrangentes de gerenciamento de segurança de informações, segurança de computadores e dados e segurança de rede.(WHITMAN, 2011).

Política de Segurança No contexto abordado convém definir política de segurança, segundo a conceituação proposta por (MARTINS; SANTOS, 2005) embasada na RFC's 2196 e 2828, é um documento que deve descrever as recomendações, as regras, as responsabilidades e

as práticas de segurança. O autor destaca também a impossibilidade de conceber uma política de segurança que possa ser implementada em qualquer organização. Uma vez que, esta deverá ser moldada à especificidade de cada caso.

1. **Identificação e Autenticação** : Em *cloud computing*, dependendo do tipo de nuvem, bem como o modelo de entrega, os usuários especificados devem ter prioridades de acesso estabelecidas, suplementares e permissões podem ser concedidas em conformidade. Este processo consiste em verificar e validar usuários individuais da nuvem por meio da utilização de proteções de nomes de usuários e senhas para seus Perfis de nuvem.
2. **Autorização**: é uma importante ferramenta de exigência na computação em nuvem para garantir a integridade referencial é mantido. Segue em exercer controle e privilégios sobre fluxos de processos dentro da computação em nuvem. As autorizações são mantidas pelo administrador do sistema em ambientes de nuvem privada.
3. **Confidencialidade**: Na computação em nuvem, a confidencialidade desempenha um papel importante, especialmente em manter o controle sobre os dados das organizações. Situado em vários bancos de dados distribuídos. É uma obrigação quando se emprega uma nuvem pública devido as nuvens públicas de natureza da acessibilidade. Confirmar a confidencialidade dos perfis dos usuários e protegendo seus dados, é praticamente acessado, permite protocolos de segurança da informação a serem cumpridos em diferentes camadas de aplicações em nuvem.
4. **Integridade**: A exigência de integridade reside na aplicação de Diligência no domínio da nuvem, principalmente ao acessar os dados. Portanto ACID (atomicidade, consistência, isolamento e durabilidade) dos dados da nuvem devem ser a dúvida seja fortemente imposta em todos os modelos de *cloud computing*.
5. **Não repúdio**: o não repúdio da computação em nuvem pode ser obtido por aplicações dos protocolos tradicionais de segurança do comércio Provisionamento de *token*para transmissão dos dados dentro da nuvem Como assinaturas digitais, carimbos de data e hora e Serviços de Confirmação de recibos (Recibo digital confirmando dados enviados/recebidos).
6. **Disponibilidade**: A disponibilidade é um dos mais críticos requisitos da computação em nuvem é um fator chave ao decidir entre fornecedores de nuvens privadas, públicas ou híbridas, bem como nos modelos de entrega. O nível de acordo de serviço é o documento mais importante que destaca a apreensão da disponibilidade em serviços e recursos da

nuvem entre o provedor de nuvem e o cliente.

Portanto, explorando os requisitos de segurança da informação em cada uma das várias plataformas de implantação e modelos de entrega definidos pela ISO, fornecedores e organizações podem tornar-se confiantes na promoção de uma estrutura de nuvem altamente protegida e segura.

4.6 Computação em Nuvem

A computação em nuvem refere-se a entrega de recursos de T.I. como um serviço, disponibilizados sob demanda através da Internet e a infraestrutura de datacenters que provê o suporte a tais serviços. A monetização é feita em função do tempo e da quantidade de recursos alocados. Os serviços entregues podem ser: armazenamento, servidores(processamento), softwares, plataformas, rede e etc). Algumas de suas características essenciais são:

4.7 Modelos de Serviços

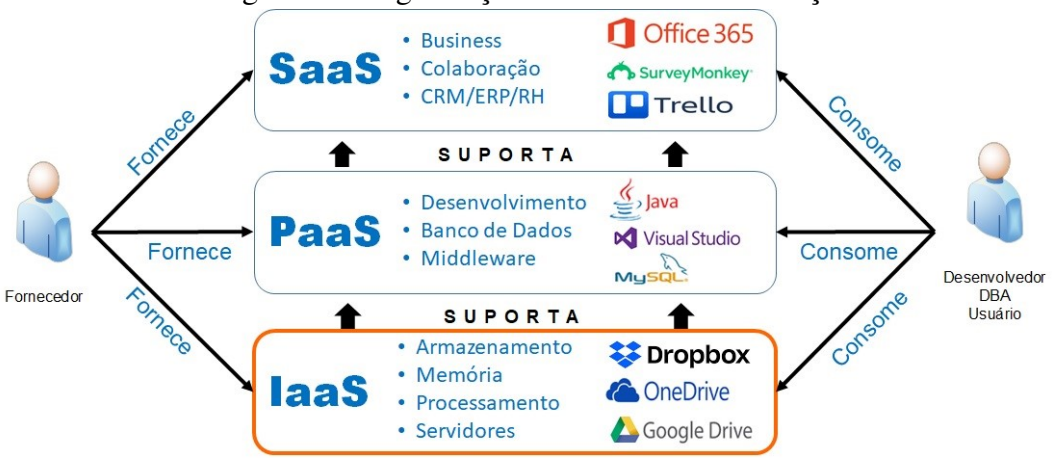
O ambiente de computação em nuvem é composto de três modelos de serviços (VAQUERO et al., 2008; RIMAL; CHOI; LUMB, 2009), apresentados e descritos na sequência. Esses modelos são importantes, pois definem um padrão arquitetural para soluções de computação em nuvem.

O modelo de computação em nuvem permite às empresas uma nova opção em seu planejamento de disponibilização de novos serviços de TI, internos ou externos. Não é mais necessário adquirir a infraestrutura física de computadores, redes, armazenamento de dados para hospedar o seu serviço. Os modelos de serviços são acessados por usuários com papéis distintos. Os papéis são importantes para definir responsabilidades, acesso e perfil para os diferentes usuários que fazem parte e estão envolvidos em uma solução de computação em nuvem. Para entender melhor a computação em nuvem, pode-se classificar os atores dos modelos de acordo com os papéis desempenhados (COUTINHO E. F.AND OUSA *et al.*, 2013). A Figura 1 apresenta os modelos/tipos de serviço e os papéis.

Considerando a visão do NIST, os modelos referem-se aos tipos de recursos e a forma de entrega desses recursos ao usuário. Está intrinsecamente relacionado aos papéis que desempenham os provedores da nuvem, desenvolvedores e os usuários.

- Software como um serviço (SaaS): Esse modelo ilustra a capacidade de execução de softwares ou aplicativos em uma infraestrutura de nuvem. As aplicações são acessíveis a

Figura 1 – Organização dos Modelos de Serviços

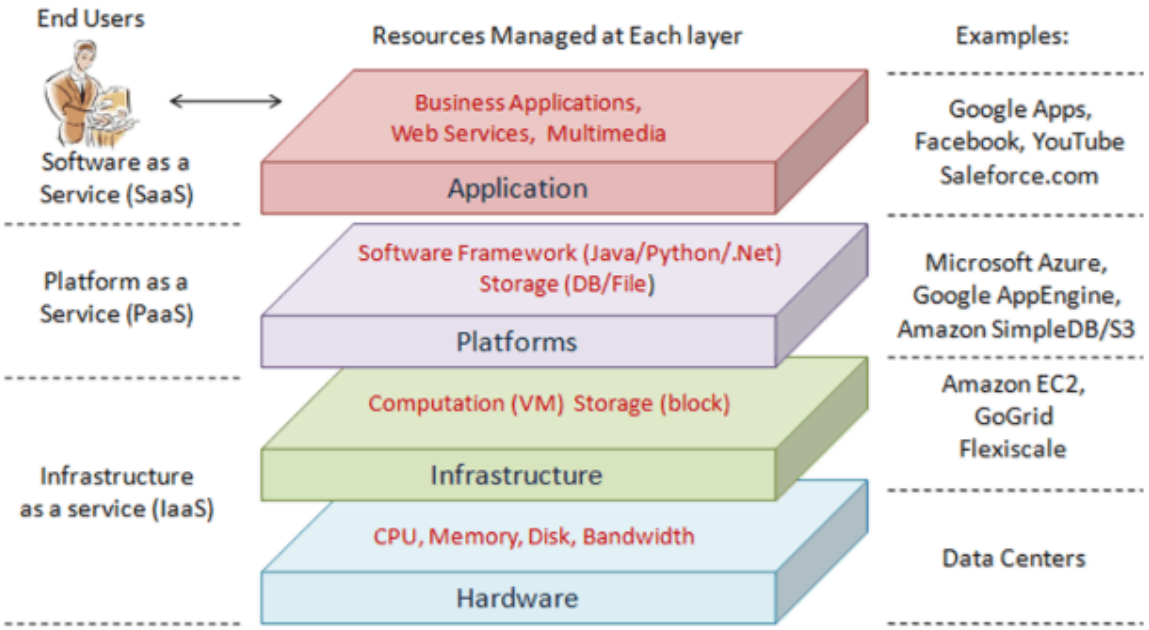


Fonte – (FENNER, 2019)

partir de vários dispositivos cliente através de uma interface como um navegador Web ou um programa.

- Plataforma como um serviço (PaaS): A capacidade oferecida ao usuário/desenvolvedor para implementar na infraestrutura da nuvem aplicações criadas pelo desenvolver ou adquiridas usando linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor da nuvem. O desenvolvedor não gerencia ou controla a infraestrutura de nuvem subjacente, incluindo rede, servidores, sistemas operacionais ou de armazenamento, mas tem controle sobre os aplicativos implantados e definições de configuração para o ambiente de hospedagem de aplicativos.
- Infraestrutura como um serviço (IaaS): Contém os componentes básicos da T.I. acessíveis na nuvem. O cliente utiliza recursos computacionais como processamento, armazenamento e rede de maneira virtualizada ou com hardware dedicado. Pode ter controle sobre os sistemas operacionais, softwares, armazenamento. E possivelmente controle limitado de componentes de rede, como *firewalls* de *host*. De acordo com a arquitetura descrita por (ZHANG QI, 2010), pode-se ainda considerar a camada de hardware, responsável pelo gerenciamento dos recursos físicos da nuvem, incluindo servidores físicos, roteadores, *switches*, sistemas de energia e refrigeração. Na prática, a camada de hardware é tipicamente implementada em *data centers*. Um centro de dados geralmente contém milhares de servidores que são organizados em *racks*, interconectados através de interruptores, roteadores entre outros. Questões típicas na camada de hardware incluem configuração de hardware, tolerância, gestão do tráfego, recursos de energia e resfriamento gestão.

Figura 2 – Arquitetura da Computação em Nuvem



Fonte – (ZHANG QI, 2010)

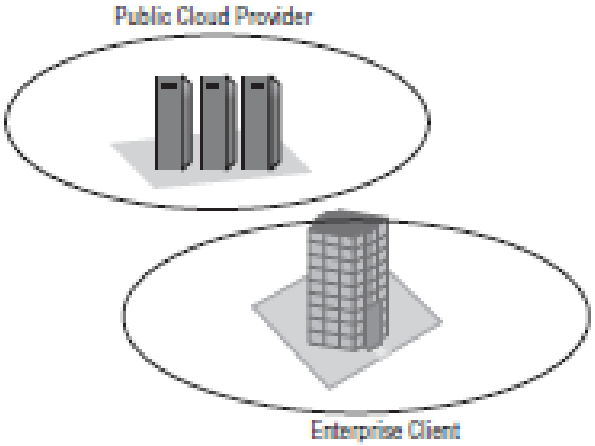
4.8 Modelos de Implantação

Novamente utilizando a visão do NIST para a descrição existem quatro modelos de implantação, são eles:

- Nuvem Privada: A infraestrutura de nuvem é provisionada para uso exclusivo por uma única organização. Ela pode ser de propriedade, gerenciada e operada pela organização, por terceiros ou por alguma combinação deles, e pode existir dentro ou fora das instalações da organização.
- Nuvem Comunidade: Nesse modelo a infraestrutura de nuvem é provisionada para uso exclusivo por uma comunidade específica de usuários/clientes de organizações que compartilham preocupações (por exemplo, missão, requisitos de segurança, políticas e considerações de conformidade). A nuvem pode ser de propriedade, gerenciada e operada por uma ou mais das organizações da comunidade, por um terceiro ou uma combinação deles, e pode existir dentro ou foras das instalações das organizações.
- Nuvem Pública: A infraestrutura de nuvem é provisionada para uso aberto pelo público em geral. A nuvem pode ser de propriedade, gerenciada e operada por uma organização comercial, acadêmica ou governamental ou por alguma combinação deles. Existe nas instalações do provedor de nuvem. Segundo definiu (WHITMAN, 2011) nuvem pública

é um esquema de implementação de computação em nuvem que geralmente é aberto para uso pelo público em geral. O público em geral é definido neste caso como usuários individuais ou corporações. A infraestrutura de nuvem pública usada é propriedade de uma organização de fornecedores de serviços em nuvem; exemplos de implantação de nuvem pública incluem Amazon Web Services, Google App Engine e Salesforce.com e Microsoft Windows Azure e a solução opensource OpenStack.

Figura 3 – Nuvem Pública



Fonte – (ZHANG QI, 2010)

- Nuvem Híbrida: Essa infraestrutura é uma composição de duas ou mais infraestruturas de nuvem distintas (privada, comunitária ou pública) que permanecem como entidades exclusivas, mas unidas por tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicativos. Como por exemplo, o *cloud bursting* para balanceamento de carga entre nuvens. Que consiste na execução de um aplicativo em uma nuvem privada ou data center e direcionamento para uma nuvem pública quando a demanda por capacidade de computação aumentar.

4.9 OpenStack

Para (RISTOV SASKO, 2013) a maioria das discussões e artigos relacionados concluem que o principal obstáculo para as soluções de nuvem pública é a segurança. Confidencialidade, integridade e disponibilidade são as maiores preocupações de segurança enfrentadas por clientes em soluções de nuvem pública. Portanto, utilizar uma nuvem privada é uma abordagem que deve solucionar a maioria dos desafios, uma vez que mitiga os riscos de segurança.

O OpenStack é um sistema *opensource* que provê uma infraestrutura como um serviço na qual é possível oferecer uma solução completa de computação (*compute*), rede (*networking*) e armazenamento (*storage*). O software OpenStack controla grandes conjuntos de recursos de computação, armazenamento e rede em todo o datacenter, gerenciados por meio de um painel ou por meio da API do OpenStack (ISACA; MEADOWS-USA, 2019).

> O sistema OpenStack consiste em vários serviços principais que são instalados separadamente. Esse serviços funcionam juntos dependendo de suas necessidades de nuvem e incluem serviços de computação, identidade, rede, imagem, armazenamento, armazenamento em bloco, armazenamento de objetos, telemetria, orquestração e banco de dados. Qualquer um desses projetos podem ser instalados e configurados separadamente ou ainda como entidades conectadas.(ISACA; MEADOWS-USA, 2019)

Com relação à segurança os serviços do OpenStack suportam vários métodos, incluindo o servidor de banco de dados e o intermediário de mensagens, dão suporte à segurança de senha. Trata-se de um sistema com uma infinidades de serviços que podem ser adicionados independentemente. Os principais são:

- Keystone: *Identity Service*(Serviço de identidade);
- Glance: *Image Service*(Serviço de Imagem);
- Nova: *Compute Service*(Serviço de Computação);
- Neutron *Networking Service*(Serviço de Rede).
- Horizon: *Dashboard* (Interface Web);
- Cinder: *Block Storage service*(Serviço de Armazenamento em Bloco).

Figura 4 – Senhas no OpenStack

Nome da senha	**Descrição**
Senha do banco de dados (nenhuma variável usada)	Senha de root para o banco de dados
`ADMIN_PASS`	Senha do usuário **`admin`**
`CINDER_DBPASS`	Senha do banco de dados para o serviço Block Storage
`CINDER_PASS`	Senha do usuário do serviço de armazenamento em block **`cinder`**
`DASH_DBPASS`	Senha do banco de dados para o painel
`DEMO_PASS`	Senha do usuário **`demo`**
`GLANCE_DBPASS`	Senha do banco de dados para o serviço de imagem
`GLANCE_PASS`	Senha do usuário do serviço de imagem **`glance`**
`KEYSTONE_DBPASS`	Senha do banco de dados do serviço de identidade
`METADATA_SECRET`	Segredo para o proxy de metadados
`NEUTRON_DBPASS`	Senha do banco de dados para o serviço de rede
`NEUTRON_PASS`	Senha do usuário do serviço de rede **`neutron`**
`NOVA_DBPASS`	Senha do banco de dados para o serviço de computação
`NOVA_PASS`	Senha do usuário do serviço Compute **`nova`**
`PLACEMENT_PASS`	Senha do usuário do serviço de veiculação **`placement`**
`RABBIT_PASS`	Senha do usuário do RabbitMQ **`openstack`**

Fonte – (ISACA; MEADOWS-USA, 2019)

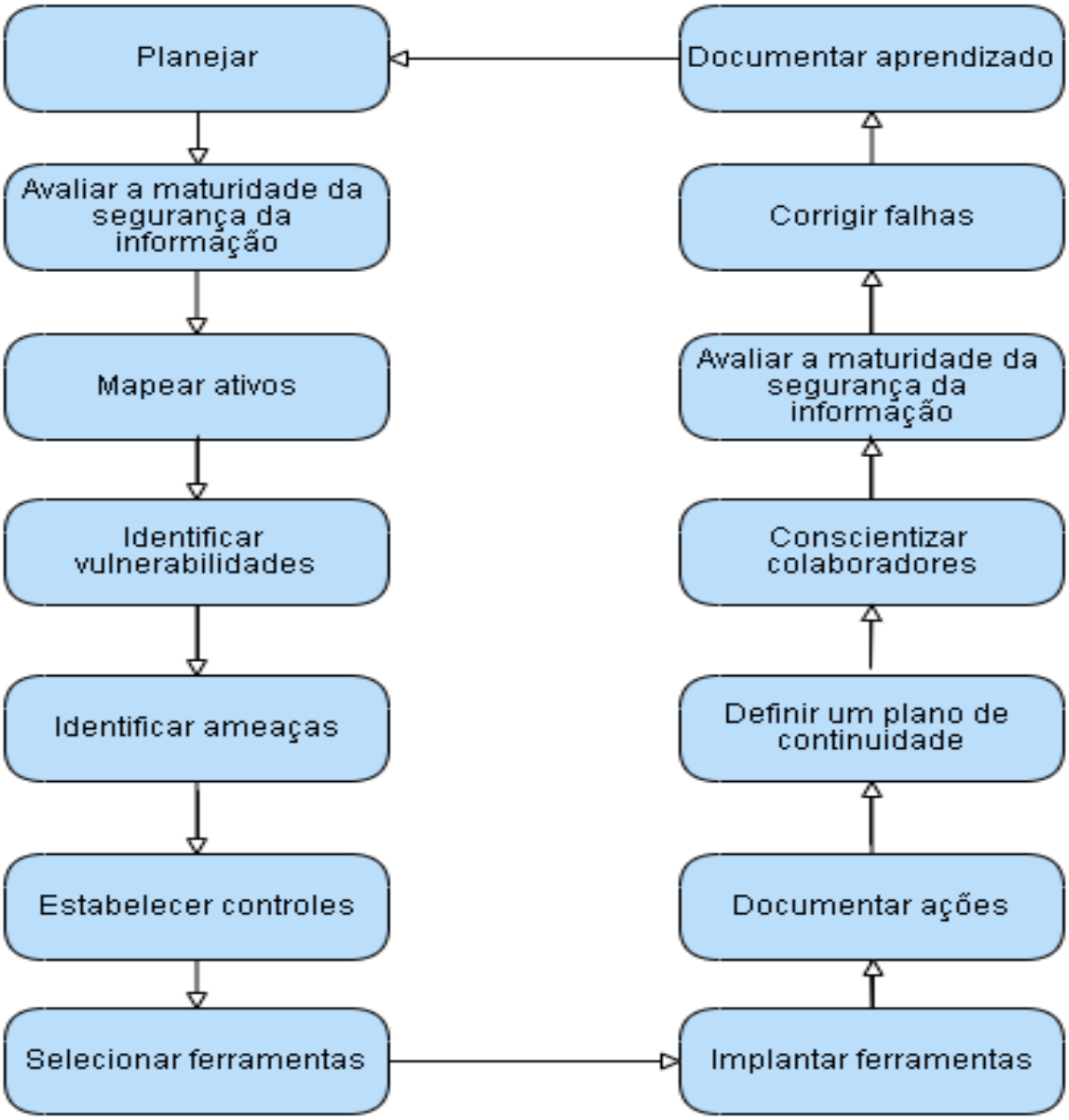
5 SOLUÇÃO PROPOSTA

A metodologia propõe-se a prover melhoria contínua para a segurança da computação em nuvem. Por essa razão será utilizado o modelo PDCA. Este trabalho baseou-se ainda na metodologia descrita em BARBOSA et al. Tendo em vista a complexidade de estabelecer uma metodologia conceitual e de implantação abrangente este trabalho limita-se a fornecer uma metodologia conceitual. A metodologia em questão, foi elaborada considerando cada etapa como um processo. De forma que, a partir do mapeamento dos ativos possa-se identificar as ameaças a que esses ativos estão sujeitos. Identificando-se as ameças parte-se para a verificação do nível de risco resultante de cada uma dessas ameaças. De posse do nível de risco imposto pela ameaça é possível determinar os controles necessários para mitigar o risco de incidência, resposta a danos causados e o plano de continuidade de negócios. Os ativos existentes e os não existentes antecipam os tipos de ameaças aos quais a organização estará exposta . Além disso a metodologia sugere um questionário para avaliar o cenário atual de segurança da nuvem. Procurando verficar se a infraestrutura atende aos princípios de segurança da informação. Será utilizada uma abordagem de processos, justificada pelo descrito na norma (ABNT, 2006)

> Uma organização precisa identificar e gerenciar muitas atividades para funcionar efetivamente. Qualquer atividade que faz uso de recursos e os gerencia para habilitar a transformação de entradas em saídas pode ser considerada um processo. Frequentemente a saída de um processo forma diretamente a entrada do processo seguinte. A aplicação de um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos, e a sua gestão podem ser consideradas como abordagem de processos.

Nessa perspectiva da abordagem de processos cada etapa descrita na metodologia consiste em um processo, que composto de uma entrada, realiza uma ação e entrega uma saída para o processo/etapa seguinte. Os macro processos estão descritos na Figura 5.

Figura 5 – Processos da metodologia proposta



Fonte – Elaborada pela autora

Conforme mostrado na Figura 5, a partir dos passos indicados abaixo, a metodologia proposta segue um ciclo iterativo, de melhoria continuada, que pode ser comparada a um ciclo do tipo PDCA (*Plan-Do-Check-Act*).

- **Planejar** - O primeiro processo refere-se ao planejamento, nessa etapa é necessário identificar quem serão os responsáveis e os colaboradores envolvidos na aplicação da metodologia. Nesse etapa deve-se ainda estabelecer o(s) colaborador(es) que responderão a avaliação de maturidade presente no processo seguinte. Bem como, elaborar o questionário de avaliação que será utilizado. Além disso durante esse processo deve-se definir quais são os serviços críticos executados na nuvem. Essa informação será necessária em um dos

processos subsequentes para definição do plano de continuidade de negócios.

- **Avaliar a maturidade da segurança da informação** - Essa etapa consiste na aplicação do questionário de avaliação da maturidade de segurança da informação, análise e documentação dos resultados obtidos. Esses dados serão importantes para o gestor de T.I. decidir que estratégias de segurança são prioritárias e verificar quais requisitos de segurança não estão sendo atendidos pela organização atualmente.
- **Mapear ativos** - O mapeamento de ativos deverá ser realizado nessa etapa com a finalidade de identificar tudo aquilo que compõe a infraestrutura que será gerenciada, colaboradores da empresa e demais partes que fazem uso da nuvem. Esses etapa é importante pois define os objetos de interesse da segurança da informação. De acordo com a norma brasileira ISO/IEC 27002 define como ativo tudo aquilo que possui valor para organização e precise ser protegido.
- **Identificar as vulnerabilidades** - Consiste em associar para cada um dos ativos fragilidades que podem ser exploradas por ameaças e resultar em um incidente de segurança.
- **Identificar as ameaças** - deve-se detectar quais ameças podem explorar as vulnerabilidades e comprometer a integridade de cada um dos ativos.
- **Estabelecer controles** - Nessa etapa é importante que ressaltar que as ameaças não podem ser controladas, no entanto pode-se agir para reduzir o risco de que uma ameaça explore determinada vulnerabilidade de um ativo. Esse processo consiste portanto em associar a cada uma das ameaças identificadas ao menos um mecanismo de segurança que neutralize ou mitigue o risco associado a respectiva ameaça. Ex: Dados armazenados (ativo) podem ser excluídos(ameaça), e a exclusão foi realizada por alguém sem credenciais para acessá-los, o controle, nessa situação, poderia ser implantar um controle de acesso com senha ou outro tipo de autenticação.
- **Selecionar ferramentas** - Uma vez que os controles tenham sido estabelecidos, é necessário nesta etapa identificar se o controlador da nuvem utilizado possui essas funcionalidades implementadas. Caso contrário, será necessário pesquisar ferramentas ou criar a própria ferramenta por meio de sua API. Podem haver situações para quais ainda não existam controles viáveis, nesse caso a organização terá que aceitar os riscos.
- **Implantar ferramentas** - Durante a execução desse processo serão realizadas as configurações nos sistemas/serviços existentes, instalação de softwares, hardwares, treinamento de usuários ou a implantação de qualquer outro mecanismo que tenha sido definido como

ferramenta/controle nos processos anteriores.

- **Documentar ações** - A metodologia sugere a documentação detalhada de implantação das ferramentas realizada no processo anterior. Essa prática será útil no futuro para que o gestor e profissionais de T.I. lidem com eventuais incidentes de segurança, caso necessitem refazer a implantação, ou para dar celeridade a resolução de problemas. A documentação das ações é importante ainda porque não limita a manutenção da segurança da nuvem a permanência de determinado colaborador na organização.
- **Definir um plano de continuidade de negócios** - Nesse estágio o gestor de T.I. deverá definir uma estratégia para manter em execução na nuvem os serviços definidos como críticos durante o primeiro processo. Uma vez que, a paralisação destes pode afetar atividades sensíveis da organização trazendo prejuízos.
- **Conscientizar colaboradores** - Nessa fase o gestor de T.I. deve produzir material e treinamento visando que os usuários ou colaboradores da empresa, que utilizam a nuvem, conheçam a conduta adequada para promover e manter a segurança da informação. Por exemplo: cibersegurança, criação de senhas fortes, principais ameaças e boas práticas de uso da infraestrutura.
- **Avaliar maturidade da segurança da informação** - A partir desse processo é possível verificar a eficácia da estratégia adotada pelo gestor T.I. para a segurança da nuvem. Se as ações, treinamentos, controles, ferramentas, configurações foram suficientes para garantir os principios de segurança e o provimeno dos serviços da nuvem.
- **Corrigir falhas** - Após a realização do passo anterior, a avaliação, o gestor de T.I. obterá dados sobre os aspectos que precisem ser corrigidos. Essa etapa consiste portanto em um realinhamento de estratégias para a segurança na nuvem. Isso sugere a busca de novas ferramentas e controles, mapeamento de novas ameaças e aplicação do respectivo contole entre outras.
- **Documentar aprendizado** - O último processo requer a documentação das falhas identificadas, maneiras de contorná-las e dificuldades encontradas.

6 ESTUDO DE CASO

O estudo inclui as seguintes etapas: revisão de literatura, definição escopo, estudo de caso, levantamento dos ativos e riscos, elaboração do questionário para avaliar a maturidade da segurança da informação, aplicação do questionário, análise das respostas, estabelecimento dos controles, elaboração da metodologia.

6.1 Descrição

A pesquisa foi desenvolvida como um estudo de caso de carácter qualitativo com objetivo exploratório. De acordo com (GIL, 2002), os estudos de caso caracterizam-se como exploratórios quando o acesso a múltiplos casos é difícil e o pesquisador tem possibilidade de investigar um deles.

Esse estudo ocorreu em torno do funcionamento da infraestrutura de nuvem privada da UFC Campus Quixadá. No estudo inicialmente foi identificada a infraestrutura atual que compõe a nuvem. Essa etapa foi realizada por meio de consulta ao técnico de TI.

A partir dos dados foi constatado que as máquinas atendem e excedem as configurações mínimas para a utilização do OpenStack.

De acordo com o guia de instalação presente no site da ferramenta (ISACA; MEADOWS-USA, 2019), na criação de ambientes, recomenda-se que estes atendam ou excedam os seguintes requisitos de *hardware*:

- *Controller Node*: 1 processador, 4GB de memória RAM e 5GB de armazenamento.
- *Compute Node*: 1 processador, 2GB de memória RAM e 10 GB de armazenamento.

A *cloud* do estudo de caso é composta por 5 Máquinas do tipo desktop e 1 servidor de Rack:

Tabela 1 – Máquinas da nuvem

Tipo	**Fabricante**	**Processador**	**RAM**	**HD**	**Sistema Operacional**
Desktop	Dell	Core i7-2600 3.40GHz x86_64	4 GB	500 GB	Ubuntu 16.04 LTS
Servidor	Dell	Core i7-2600 3.40GHz x86_64	4 GB	500 GB	Ubuntu 16.04 LTS

Fonte: Elaborada pela autora

Com o intuito de avaliar a metodologia proposta, foi realizado a aplicação parcial da solução na nuvem privada do campus da UFC em Quixadá. O experimento seguiu os passos descritos na sequência.

6.1.1 Identifcação dos ativos

Para prover a segurança da informação em uma organização é necessário previamente identificar os ativos que são suscetíveis a erros e danos. De acordo com a estrutura e utilização da nuvem de estudo os ativos foram classificados em humanos, informação, software e infraestrutura descritos a seguir na Tabela 2.

Tabela 2 – Matriz de Ativos

CATEGORIA DO ATIVO	**ATIVO**
Humanos	Usuários Funcionários
Informação	Informações dos projetos na nuvem Serviços fornecidos Armazenamento de dados Credenciais dos usuários Documentação
Software	Máquinas virtuais Softwares aplicativos Sistemas Operacionais das máquinas virtuais Controlador de nuvem (OpenStack)
Hardware	Servidores Acesso à Internet Switches Roteadores

Fonte: Elaborada pela autora

6.1.2 Identificação das vulnerabilidades e ameaças

Uma vez identificados os ativos, procurou-se mapear as ameaças e vulnerabilidades de cada. Seguindo o que foi adotado por (AMARAL *et al.*, 2011), relacionou-se um ativo as suas vulnerabilidade e inerentes ameaças que possam explorá-las. Conforme descrito na tabela 3.

Tabela 3 – Ativos x Vulnerabilidades X Ameaças

ATIVO	VULNERABILIDADE	AMEAÇA
Usuários	Falta de treinamento	Erro na utilização da infraestrutura
Funcionários	Insatisfação e doença Falta de capacitação	Baixa produtividade Erros nos processos de trabalho
Informações dos projetos na nuvem	Rede inacessível	Indisponibilidade das informações Perda das informações
Serviços fornecidos	Rede inacessível	Indisponibilidade dos serviços
Armazenamento de dados	Falta de treinamento do usuário Invasão da máquina	Exclusão acidental Alterações maliciosas (perda de integridade)
Credenciais dos usuários	Perda das credenciais	Indisponibilizar acesso aos projetos existentes
Documentação	Incompleta Inexistente	Torna-se ininteligível Atraso na solução de problemas
Máquinas virtuais	Desconhecimento da ferramenta	Exclusão de máquinas de virtuais
Softwares aplicativos	Configuração	Mau funcionamento
SO's das máquinas virtuais	Imagem corrompida Exclusão da .iso	Erro na criação das máquinas Falha a criação das VM's
Controlador (OpenStack)	Sobrecarga Desligamento	Acesso lento aos serviços Indisponibilidade dos serviços
Acesso à Internet	Conexão lenta	Baixa produtividade
Switches	Desligamento	Erro de acesso a rede local
Roteadores	Perda de acesso a Internet	Perda de amplo acesso

Fonte: Elaborada pela autora

6.1.3 Elaboração e aplicação do questionário

Para a continuidade do estudo ocorreu através da coleta de informações funcionais da nuvem. Através de questionário, o qual de acordo com (LAKATOS; MARCONI, 2003), consiste em uma técnica de observação extensiva, constituída por perguntas escritas e que devem ser respondidas sem a presença daquele que realiza o trabalho. A elaboração do questionário, que consta no APÊNDICE A, foi baseada na leitura de artigos e nos requisitos de segurança, principalmente, confidencialidade, integridade, disponibilidade e autenticidade. O questionário propôs-se avaliar a maturidade da segurança da informação na infraestrutura estudada. O entrevistado foi o Professor Doutor Paulo Rego Lima, que acompanhou a implantação da nuvem e o seu funcionamento até 2018. A entrevista foi respondida pelo professor através de formulário eletrônico.

6.1.4 Controles para o gerenciamento de riscos em uma nuvem privada

Para (KRUTZ RONALD L, 2010) a postura da segurança da informação em uma organização é definida por três princípios fundamentais, são eles: confidencialidade, integridade e disponibilidade. Aos quais todos os controles, as ameaças e vulnerabilidades e os processos estão sujeitos.

Integridade: Cenário de Risco: Invasões por hackers aos ambientes da nuvem

Controle: Restrição de acesso, utilização de Firewall, autenticação de usuários;

Confidencialidade: Cenário de Risco: Aplicações de diversos usuários coabitam nos mesmos locais/sistemas de armazenamento. Controle: Isolamento de projetos/ Autenticação;

Disponibilidade: Cenário de Risco: Recuperação de dados armazenados dos projetos Controle: /Redundância de mídias de armazenamento e backups;

Autenticação: Cenário de Risco: Verificação de autenticidade dos usuários/aplicações Controle: Política de senhas;

Não-repúdio: Cenário de Risco: Auditabilidade das ações executadas por usuários no sistema Controle: Monitoramento e análise de arquivos de logs.

Tabela 4 – Princípio x Cenário de risco x Controle

Princípio de Segurança	**Cenário de Risco**	**Controle**
Integridade	Invasões de hackers ao ambiente de nuvem	Restrição de acesso
Confidencialidade	Compartilhamento de ambientes	Isolamento de ambientes
Disponibilidade	Recuperação dos dados	Redundância
Autenticidade	Verificação de autenticidade dos usuários/aplicações	Política de senhas
Não repúdio	Auditabilidade das ações executadas por usuários no sistema	Análise de logs

Fonte: Elaborada pela autora

7 ANÁLISE DE RESULTADOS

A análise das respostas do questionário permitiu inferir que a nuvem necessita de investimento em *hardware* para atender a princípios de segurança como a disponibilidade. Fator observado nas respostas 1), 5), 10) e 15) que evidenciaram a ausência de SLA e tolerância a falhas em caso de oscilações na rede elétrica, por exemplo. Sendo a disponibilidade um dos mais críticos requisitos da computação em nuvem seria interessante um plano de contingência de T.I. que visasse a continuidade dos serviços em caso de falhas.

Em continuação a questão 08), destacou-se não ser possível garantir a integridade dos dados. O princípio da confidencialidade foi abordado na questão 9), na qual identificou-se que a segregação dos dados é realizada através da criação de um projeto para cada usuário com rede própria e isolada.

A autenticação e controle de acesso dos quais tratam as questões 3) e 11) são realizados, exclusivamente, pela verificação de usuário e senha.

A questão 02) tratou de técnicas de gerenciamento da rede que têm impacto sobre a nuvem, ao que o mesmo informou ser basicamente a política de firewall.

Questão 06) o entrevistado ressaltou que a implantação permite a portabilidade dos dados para outra tecnologia.

Questão 12) Existem logs do sistema que podem ser rastreados para identificar ações do usuário.

Questão 13) Inexiste Plano de Mitigação de Riscos. Questão 14) O entrevistado do pode responder se há uma metodologia de gestão de risco de seguraça da informação.

Questão 07) abordou as garantias para a segurança das informações residentes na nuvem. De acordo com o entrevistado, o escopo da nuvem privada não possibilita exigir garantias, e ressaltou ainda que princialmente na nuvem do campus por possuir poucos recursos de equipamentos.

Tabela 5 – Resumo da avaliação de maturidade da segurança

REQUISITOS	**SIM**	**NÃO**
Tolerante a falhas		x
SLA		x
Recuperação de informações críticas		x
Plano de continuidade		x
Portalibilidade dos dados	x	
Integridade dos dados		x
Segregação dos dados	x	
Garantia da confidencialidade	x	
Autenticação de usuários	x	
Controle de acesso	x	
Política de Firewall		x
Auditoria de logs		x

Fonte: Elaborada pela autora

8 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho teve como objetivo elaborar uma metodologia de segurança para nuvens privadas. O estudo teve a seguinte questão de pesquisa: "Como melhorar a segurança em uma infraestrutura de nuvem privada?". No qual utilizou-se como estudo de caso a nuvem da UFC Campus Quixadá. Para isso, foi avaliada a maturidade da segurança da informação e, a partir dessa análise, identificados tanto os requisitos que já são atendidos, quanto aqueles que ainda devem ser implantados.

Verifica-se que os objetivos do trabalho foram atingidos ao se conseguir, nas seções 5.7 e 5.8, elencar ameaças as quais a infraestrutura está exposta, bem como, sugerir controles que neutralizem essas ameaças.

Ademais, tendo em vista os resultados observados na avaliação, propôs-se uma metodologia conceitual com aspectos de segurança a serem considerados durante a implantação de uma nuvem privada ou mesmo o incremento da segurança em uma estrutura existente. Tais como, o mapeamento dos ativos e das ameaças, e, além disso, a seleção dos controles.

Como trabalho futuro pode-se elaborar uma política de segurança incluindo os controles identificados a partir da metodologia proposta. Sugere-se ainda promover testes de instrusão e atualizar a metodologia para o caso de surgimento de novas ameaças ou vulnerabilidades.

REFERÊNCIAS

AMARAL, M. M. *et al.* **Metodologia Para Análise e Avaliação de Riscos por Composição de Métodos**. [S.l.]: Universidade Federal de Santa Maria, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002**: Código de prática para gestão de segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27001**: Sistema de gestão de segurança da informação - requisitos. Rio de Janeiro, 2006.

BON, J. v. **Foundations of IT Service Management, based on ITIL**. [S.l.]: ITSMF internacional, 2007.

BUYYA, R.; YEO, C.; VENUGOPAL, S.; BROBERG J, B. I. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. **Future Generation Computer Systems**, Elsevier Science, v. 25, 2009.

BUYYA, R.; YEO, C.; VENUGOPAL, S.; BROBERG J, B. I. Cobit 5 - a business framework for the governance and management of enterprise it. **Communications of the ACM**, v. 25, n. 6, p. 599–616, 2013.

CASTRO, R. C. C. de; SOUSA, V. L. Pimentel de. **Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança**. [S.l.: s.n.], 2017.

COUTINHO E. F.AND OUSA, F. R. C.; GOMES, D. G.; SOUZA, J. N. Elasticidade em computação em nuvem: Uma abordagem sistemática. **XXXI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**, 2013.

FENNER, G. **Um modelo orientado ao negócio para suporte à tomada de decisão multicritério no gerenciamento de capacidade em provedores IAAS**. Tese (Doutorado) — Universidade Federal do Ceará, Departamento de Computação, Curso de Doutorado em Computação, Fortaleza, 2019.

FERREIRA, A. S. **Uma arquitetura para monitoramento de segurança baseada em acordos de níveis de serviço para nuvens de infraestrutura**. Tese (Doutorado) — Universidade Estadual de Campinas, Instituto de Computação, Curso de Mestrado em Computação, Campinas, 2013.

FERREIRA, D. M. **Infraestrutura Confiável para Cloud baseada em OpenStack**. Tese (Doutorado) — Universidade do Porto, Departamento de Ciência de Computadores, Curso de Mestrado em Engenharia de Redes e Sistemas Informáticos, Portugal, 2017.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. [S.l.]: Atlas S.A., São Paulo, 2002.

HAES, S.; GREMBERGEN, W. V. **IT Governace and Its Mechanisms**. [S.l.]: Information Systems Audit and Control Association, 2004.

ISACA; MEADOWS-USA, R. **Software de código aberto para criar nuvens privadas e públicas**. 2019. Disponível em: <https://www.openstack.org/>.

KRUTZ RONALD L, V. R. D. **Cloud security: A comprehensive guide to secure cloud computing**. [S.l.]: Wiley Publishing, 2010.

LAKATOS, E. M.; MARCONI, M. de A. **Metodologia científica**. [S.l.]: Atlas São Paulo, 2003.

MARTINS, A. A.-d. B.; SANTOS, C. A. S. Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **JISTEM - Journal of Information Systems and Technology Management**, scielo, v. 2, p. 121 – 136, 00 2005. ISSN 1807-1775.

RISTOV SASKO, M. G. D. A. Openstack cloud security vulnerabilities from inside and outside. **The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization**, 2013.

WHITMAN, M. E. **Principles of information security**. [S.l.]: Cengage Learning, 2011.

ZHANG QI, C. L. B. R. Cloud computing: state-of-the-art and research challenges. **Journal of Internet Services and Applications**, v. 1, n. 1, p. 7–18, 2010.

APÊNDICE A – QUESTIONÁRIO COM PERGUNTAS ABERTAS

1. A estrutura é tolerante a falhas?
2. Quais são as técnicas utilizadas para gerenciamento das redes?
3. Quais são as técnicas de autenticação utilizadas?
4. Quais são as técnicas de autorização utilizadas?
5. A organização possui um plano de contingência?
6. A organização possui SLA?
7. A implantação permite a portabilidade dos dados para outra tecnologia? (No caso de modelos de serviço PaaS as aplicações desenvolvidas ficam presas ao fornecedor do serviço, de acordo o artigo Segurança em Cloud Computing: Governança e Gerenciamento de Riscos).
8. Como exigir garantias de que as informações residentes na Nuvem estão realmente seguras? (questionamento levantado no artigo Segurança em Cloud Computing: Governança e Gerenciamento de Riscos).
9. Quais são as garantias sobre a preservação da integridade dos dados? (Integridade)
10. Como é realizada a segregação de dados? (Confidencialidade)
11. Como é garantida a arquitetura de disponibilidade? A recuperação de informações críticas, está sujeita a atrasos? (Disponibilidade)
12. Que recursos são utilizados na autenticação e controle de acesso dos usuários? (Autenticidade)
13. Os usuários do modelo são capazes de negarem suas ações? (Não repúdio)
14. Existe um Plano de Mitigação de Riscos?
15. A organização possui/utiliza alguma metodologia de gestão de risco de segurança da informação?
16. Há um plano de continuidade de negócios?
17. Existe precedente em matéria de responsabilidade jurídica para a Nuvem?