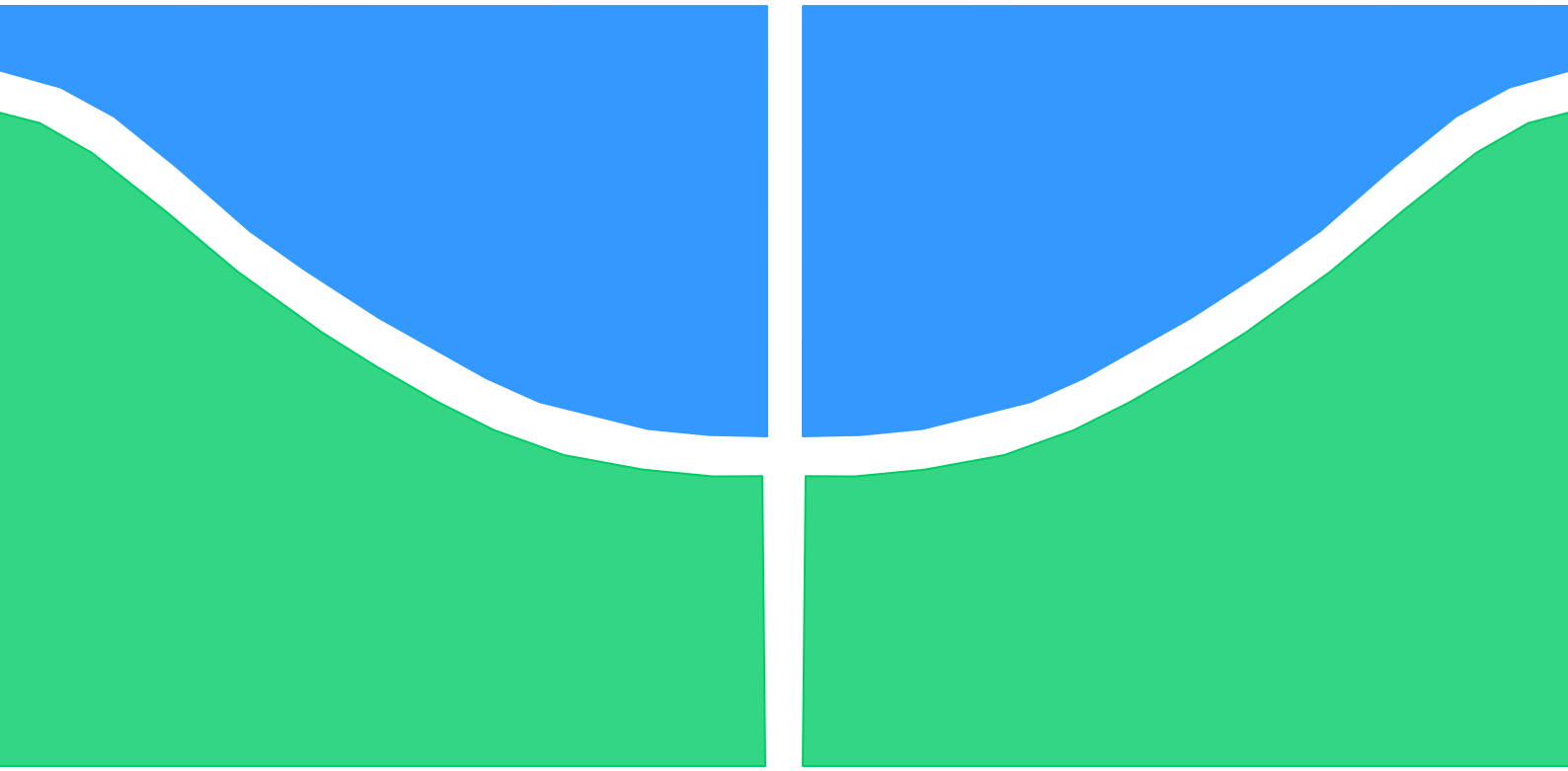

TRABALHO DE GRADUAÇÃO

RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO PARA SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO BASEADAS EM COMPUTAÇÃO EM NUVEM

Paulo Matheus Nicolau Silva

Brasília, abril de 2013

UNIVERSIDADE DE BRASILIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA

Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO PARA SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO BASEADAS EM COMPUTAÇÃO EM NUVEM

Paulo Matheus Nicolau Silva

Relatório submetido como requisito parcial para obtenção
do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Edgard Costa, UnB/ FGA (Orientador) _____

Prof. José Edil, UnB/ENE _____

Eng. Pedro Paulo Mendes, UnB _____

Dedicatória

Dedico esse trabalho aos meu pais, pois sem eles, nada seria possível.

Paulo Matheus Nicolau Silva

Agradecimentos

Agradeço a todos os amigos e familiares que me auxiliaram nessa aventura que é a graduação na Universidade de Brasília. Agradeço também a Deus por ter colocado bons amigos no caminho para me apoiarem nessa boa jornada que foi a graduação em Engenharia de Redes da UnB.

Paulo Matheus Nicolau Silva

RESUMO

A computação em nuvem é um modelo de oferta de serviços de TIC que permite a organizações redução de custos com recursos computacionais e maior disponibilidade de suas aplicações. Apesar da computação em nuvem trazer diversos benefícios, muitas organizações permanecem receosas quanto a sua adoção, pois, estas têm dúvidas quanto à segurança da informação em um ambiente de nuvem. O presente trabalho apresenta a computação em nuvem, suas motivações e principais características, os principais problemas quanto à segurança da informação e preocupação das organizações em relação a adoção da computação, e um compilado de recomendações de segurança de diversos profissionais e especialistas em computação em nuvem. Dessa forma, este trabalho oferece as organizações um compilado de informações sobre a computação em nuvem, os principais riscos e preocupações envolvidos em sua adoção e recomendações de como reduzir os riscos inerentes da nuvem.

Palavras-chave: computação em nuvem, segurança da informação, tecnologia da informação e comunicação

ABSTRACT

The cloud computing is a computing model that allows organizations to reduce spent with computational resources and bigger availability of applications. Although cloud computing brings several benefits, many organizations stay afraid in it adoption. Therefore, this present work presents the cloud computing it motivations and main features, the major information security concerns related to the cloud computing are raised and a compiled of security recommendations from several cloud computing professionals and specialists is presented. Thereby, this work provides to organizations a source of information about cloud computing, the major concerns involved in it adoption, and security recommendations about how to reduce inherent risks of the cloud.

Keywords: cloud computing, information security, information technology and communication.

SUMÁRIO

1 INTRODUÇÃO 12

1.1 OBJETIVOS 12

1.2 METODOLOGIA 13

1.3 JUSTIFICATIVA 13

2 REVISÃO BIBLIOGRÁFICA 13

2.1 COMPUTAÇÃO EM NUVEM 13

2.2 CARACTERÍSTICAS ESSENCIAS DA NUVEM 14

2.3 MODELOS DE SERVIÇOS 15

2.4 MODELOS DE IMPLANTAÇÃO 16

2.5 MODELOS DE REFERENCIA DE NUVEM 17

2.6 CLOUD SECURITY ALLIANCE 18

2.7 ÁREAS CRÍTICAS DE SEGURANÇA DA COMPUTAÇÃO EM NUVEM 18

3 PROBLEMAS DE SEGURANÇA DA INFORMAÇÃO NA COMPUTAÇÃO EM NUVEM . 19

3.1 GOVERNANÇA CORPORATIVA E GESTÃO DE RISCOS 20

3.2 ASPECTOS LEGAIS E *ELETRONIC DISCOVERY* 22

3.3 CONFORMIDADE E AUDITORIA 23

3.4 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DOS DADOS 24

3.5 PORTABILIDADE E INTEROPERABILIDADE 24

3.6 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES... 25

3.7 OPERAÇÕES E *DATACENTER* 26

3.8 RESPOSTA A INCIDENTES 26

3.9 SEGURANÇA DE APLICAÇÕES 27

3.10 CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES 28

3.11 GERENCIAMENTO DE IDENTIDADE 29

3.12 VIRTUALIZAÇÃO 29

4 RECOMENDAÇÕES 32

4.1 GOVERNANÇA CORPORATIVA 32

4.2 ASPECTOS LEGAIS E *ELETRONIC DISCOVERY* 34

4.3 CONFORMIDADE E AUDITORIA 35

4.4 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DE DADOS 36

4.5 PORTABILIDADE E INTEROPERABILIDADE 38

4.6 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES 41

4.7 OPERAÇÕES E *DATACENTER* 42

4.8 RESPOSTA A INICIDENTE, NOTIFICAÇÃO E REMEDIAÇÃO 43

4.9 SEGURANÇA DE APLICAÇÕES 44

4.10 CRIPTOGRAFIA E GERÊNCIA DE CHAVES 45

4.11 GERENCIAMENTO DE IDENTIDADE E ACESSO 45

4.12 VIRTUALIZAÇÃO 47

5 SEGURANÇA COMO UM SERVIÇO 49
6 CONCLUSÕES..... 52
REFERÊCIAS BIBLIOGRÁFICAS..... 53

LISTA DE FIGURAS

1 Modelos de serviço de nuvem.....155
2 Modelos de implementação de nuvem.....166
3 Modelo de referência de nuvem 188

LISTA DE SIMBOLOS

Siglas

ABNT	Associação Brasileira de Normas Técnicas
CSA	Cloud Security Alliance
TIC	Tecnologia da Informação e comunicação
NIST	National Institute of Stands and Technology
DoS	Denial of Service
VM	Virtual Machine
SIEM	Security Information and Event Management
DMZ	DeMilitarized Zone
SOA	Service-Oriented Architecture
URL	Uniform Resource Locator
ISO	International Standardization Organization
DAM	Database Activity Monitoring
SPML	Service Provisioning Mark-up Language
PId	Provedor de identidade
VPN	Virtual Private Network
SSO	Single Sign-On
LDAP	Lightweight Directory Access Protocol
SSL	Secure Sockets Layer
DLP	Data Loss Prevention
C.P.F.	Cadastro de Pessoas Físicas
FAM	File Activity Monitoring
CSA	Cloud Security Alliance
CSABR	Cloud Security Alliance – Brazilian Chapter

1 INTRODUÇÃO

Organizações, independentemente do porte, demandam cada vez mais recursos tecnológicos e esses recursos precisam possuir grande flexibilidade para que possam se ajustar às demandas do mercado (CSABR, 2012). Nesse cenário, a computação em nuvem vem ganhando espaço, pois permite atender sob medida as necessidades de recursos de tecnologia da informação e comunicação das organizações.

Apesar da demanda cada vez maior por recursos, existe uma grande quantidade de recursos de TIC subutilizados, pois muitas organizações, adquirem grandes quantidades de recursos computacionais para atenderem a demanda de momentos de pico e uma vez que a demanda diminui uma parte dos recursos passam a ficar ociosos. Apesar dos esforços em atender a demanda mesmo em momentos de pico, podem ocorrer altas de demanda tão grandes que a infraestrutura da organização pode não suportar. Dessa forma organizações geralmente investem bastante capital para manter uma infraestrutura de TIC que muitas vezes não atendem com qualidade às suas necessidades. Portanto, é prudente afirmar que utilizando soluções baseadas em nuvem a organização pode, além de economizar, atender com maior qualidade a demanda por recursos computacionais (SILVA, 2012).

De forma simplificada a computação em nuvem consiste na oferta de recursos de TIC sob demanda, de forma mensurável e rápida. E os clientes de nuvem podem, unilateralmente, escalar para cima ou para baixo a quantidade de recursos contratados de forma automática. Dessa forma, os clientes de nuvem não precisam adquirir mais recursos do que necessitem em um dado momento.

A computação em nuvem hoje é para muitas empresas, principalmente startups e empresas de pequeno porte, um fator crítico de sucesso da organização (CSABR, 2012). Uma vez que a nuvem permite a empresas pequenas, sem muitos recursos financeiros, ter acesso a recursos de TIC que suportem e agilizem os processos.

Da mesma forma que a computação em nuvem pode abrir novos horizontes para as organizações ela também introduz novos riscos. Com isso apesar das organizações estarem interessas na adoção da computação em nuvem, elas também encontram-se preocupadas com os riscos inerentes da computação em nuvem.

Os problemas de segurança em um ambiente de computação em nuvem são muitos, e existem poucos documentos que os endereçam. Portanto nesse trabalho será feito um compilado dos principais problemas e preocupações relacionadas a adoção da computação em nuvem. Treze áreas críticas de preocupação foram levantadas pela Cloud Security Alliance, um dos principais grupos engajados em fazer a computação em nuvem mais segura. Nesse trabalho serão compilados os problemas, no que tange a computação em de cada uma dessas treze áreas críticas, assim como recomendações para que esses problemas possam ser resolvidos.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

O propósito deste trabalho é oferecer um compilado de informações acerca da computação em nuvem, seus principais problemas de segurança, e recomendações para reduzir os riscos envolvidos na sua utilização.

1.1.2 OBJETIVOS ESPECÍFICOS

- Pesquisar e apresentar a computação em nuvem, suas principais características e motivações;
- Identificar e caracterizar os principais problemas de segurança da computação em nuvem;
- Fazer um compilado de recomendações de segurança da informação, explicitadas pelos autores descobertos na pesquisa bibliográfica exploratória.

1.2 METODOLOGIA

O desenvolvimento do projeto se deu em três partes. Primeiramente o levantamento e pesquisa bibliográfica exploratória, em seguida a análise dos problemas relacionados à segurança na computação em nuvem e por último foi feito um compilado de recomendação de se segurança da informação para a computação em nuvem encontradas na literatura.

Para atingir o primeiro o objetivo foi feita uma pesquisa bibliográfica exploratória por meio de livros e artigos sobre o assunto os quais foram consultados a fim de apresentar a computação em nuvem, suas principais características e motivações. O critério utilizado para levantar os livros e artigos mais relevantes foi a quantidade de citações e referências que esses artigos e livros recebem. Nessa fase foram identificadas diversas fontes confiáveis de conteúdo e a Cloud Security Alliance é um grupo que se destacou devido à grande quantidade de citações de seus guias e artigos em outros artigos e livros encontrados.

Para atingir o segundo objetivo, foi realizada uma minuciosa exploração, dos livros e artigos encontrados na primeira etapa do trabalho, afim de encontrar as principais ameaças que os clientes de computação em nuvem estão sujeitos, e as principais preocupações das organizações que ainda permanecem receosas quando a adoção nuvem.

Para atingir o terceiro objetivo, uma nova análise minuciosa dos livros e artigos foi feita agora com o objetivo de encontrar e compilar as recomendações de segurança da informação apresentadas nesses documentos. Um trabalho de filtragem por recomendações mais relevantes também feito, o critério usado nesse filtro foi o de quais recomendações mais se relacionavam com os problemas encontrados na segunda etapa do trabalho.

1.3 JUSTIFICATIVA

Apesar das vantagens oferecidas pela computação em nuvem ainda existem organizações receosas em aderi-la por não confiarem que suas informações estarão seguras em um ambiente de nuvem. A perda de controle físico dos dados é o que mais impulsiona essa desconfiança. Contudo muitas vezes as informações dessas organizações estariam mais seguras com um provedor de nuvem do que na própria organização, pois o foco dos provedores é na oferta de recursos de TIC de forma segura, elástica e rápida.de nuvem já o *core* do negócio da maioria das organizações não é esse. Dessa forma este trabalho visa oferecer a base de informações necessárias para que organizações possam melhor julgar quando ou não aderir à computação em nuvem, e também oferecer um compilado de informações à organizações que já fazem o uso da a computação em nuvem possam conhecer as ameaças a que estão sujeitas e como se proteger.

2 REVISÃO BIBLIOGRÁFICA

2.1 COMPUTAÇÃO EM NUVEM

Computação em nuvem é um modelo, ubíquo e sob demanda, de acesso um conjunto de recursos computacionais configuráveis que podem ser rapidamente providos com um esforço mínimo de gerência ou interação com o provedor do serviço (NIST, 2011).

De forma simplificada a computação em nuvem consiste na oferta de recursos de TIC sob demanda, de forma mensurável e rápida. E os clientes de nuvem podem, unilateralmente, escalar para cima ou para baixo a quantidade de recursos contratados de forma automática. Dessa forma, os clientes de nuvem não precisam adquirir mais recursos do que necessitem em um dado momento. A computação em nuvem pode ser entendida como a entrega de recursos de TIC de forma análoga a entrega de energia elétrica, dessa forma clientes que utilizam mais recursos pagam mais e clientes que utilizam menos recursos pagam menos.

A computação em nuvem é resultado da combinação e evolução de diversos conceitos. Segundo CSABR (2012), os principais conceitos e modelos pré-existentes englobados em computação em nuvem

são os seguintes: terceirização, *utility computing*, *grid computing* (Computação em grade), *Autonomic Computing* e virtualização

Terceirização - O conceito de terceirização refere-se à contratação de serviços de terceiros para realizar determinada atividade dentro da organização. Um dos maiores benefícios deste modelo é permitir que uma organização consiga concentrar seus recursos e esforços em torno de sua atividade fim, transferindo algumas de suas atividades de apoio para terceiros especializados naquele ramo de atividade. Nos casos da adoção de serviços que são implementados vem nuvens públicas ou comunitárias o cliente estará terceirizando serviços de TIC. No entanto adotar a computação em nuvem não significa terceirizar serviços uma vez que modelos de nuvem privadas podem ser implementados.

Utility Computing - *Utility Computing* consiste em serviços e produtos TIC disponibilizados para consumo sob demanda de consumo como serviços utilitários. Provedores de *Utility Computing* oferecem componentes básicos (armazenamento, processamento e largura de banda) para seus clientes que pagam por unidade utilizada sem preocupações com limitações, escalabilidade, integridade ou disponibilidade de recursos.

Grid Computing - No cenário atual muitas vezes grandes capacidades computacionais são necessárias para atingir objetivos ou até mesmo requisitos de negócios. O *Grid Computing* é um modelo capaz de lidar com uma alta taxa de processamento que é dividido em várias maquinas, que encontram-se em estado ocioso, formando uma única máquina virtual. Dessa forma evitando o desperdício de processamento (INTEL, 2011). O núcleo do conceito de Grid Computing, é que por meio da formação de grandes redes de computadores que compartilham recursos, maquinas virtuais com grande poder de processamento são formadas, dessa forma atendendo as grandes necessidades computacionais exigidas pelas organizações hoje.

Autonomic Computing - *Autonomic Computing* ou computação autônoma consiste em um ambiente computacional que se autogere e se autocorrige. Essa iniciativa foi lançada pela IBM em 2001, que vislumbra que as características de auto-gerência e autocorreção sejam implementadas para recursos computacionais que estão também ligados em rede.

Virtualização - Virtualização é um conceito que surgiu no ambiente de computação de grande porte, que a partir do final dos anos 1990 também foi trazido para os microcomputadores. A virtualização consiste na abstração de características físicas de *hardware* e do sistema operacional do hospedeiro por intermédio de *hypervisors*[1]. Ou seja em uma única máquina física podem rodar diversas maquinas virtuais com sistemas operacionais próprios e configurações de *hardware* diferentes. Esse conceito de vários usuários compartilhando um mesma infraestrutura física é chamado de sistema multilocatário. Embora a virtualização não seja um característica essencial da computação em nuvem para o NIST no escopo desse trabalho ela será considerada como tal. Isso será pelo fato de que a virtualização é utilizada pela grande maioria dos provedores de nuvem hoje (VMWARE, 2009).

2.2 CARACTERÍSTICAS ESSENCIAS DA NUVEM

Segundo o NIST (National Institute of Standards and Technology) (2011) os serviços oferecidos precisam possuir cinco características essenciais para serem considerados serviços de nuvem: amplo acesso à rede, rápida elasticidade, serviços mensuráveis, autosserviço sob demanda e agrupamento de recursos.

Amplo acesso à rede - O amplo acesso à rede consiste na capacidade de estar disponível na rede e que possa ser acessados através de qualquer dispositivo com acesso à internet.

Rápida elasticidade - A rápida elasticidade está associada a capacidade de prover recursos, de forma que os estes possam ser aumentados ou diminuídos de forma bem ágil e sem interrupção do serviço. Para o cliente de nuvem, os recursos disponíveis para provisionamento geralmente parecem ser ilimitados e podem ser contratadas em qualquer quantidade e a qualquer hora.

---

[1] *Hypervisor* – Também conhecido como monitor de máquina virtual, é a camada de *software* entre o *hardware* e o sistema operacional. O *hypervisor* é responsável por fornecer ao sistema operacional hospedeiro a abstração da máquina virtual (MATTOS, 2008).

Serviços mensuráveis - Os serviços oferecidos por provedores de computação em nuvem devem ser mensuráveis. Isso significa que o provedor deverá ser capaz de medir e informar a seus clientes quanto de recursos estes estão consumindo em quanto serão cobrados por isso. A forma de mensurar o serviço varia de acordo com o serviço contratado pelo cliente.

Autosserviço sob demanda - A característica de autosserviço sob demanda consiste na capacidade do cliente de nuvem unilateralmente aumentar ou diminuir os recursos utilizados sem a necessidade de interação humana com o provedor de serviços.

Agrupamento de recursos - Na computação em nuvem, os recursos de computação do provedor estão reunidos para atender vários usuários utilizando um modelo de multilocação. Exemplos de recursos são: armazenamento, processamento, memória e largura de banda. Implementações de nuvens privadas também tendem a reunir recursos e distribui-los as diferentes partes da organização (CSABR, 2012).

2.3 MODELOS DE SERVIÇOS

Além das cinco características essenciais da computação em nuvem ela também é dividida em três grandes classes, de acordo com os recursos oferecidos, também conhecidas como modelos de serviço, exibidas na Figura 1.

Estes três níveis de abstração (SaaS, PaaS e IaaS) podem também ser vistos como uma arquitetura em camadas, onde os serviços de uma camada superior podem ser compostos de serviços da camada imediatamente inferior, onde o SaaS se encontra na camada mais elevada e o IaaS na camada mais baixa (CSABR, 2012). Veja Figura 3.

Figura 1 - Modelos de serviço de nuvem (CSABR, 2012).

***Software* como serviço (SaaS – *Software as a Service*)** - Os aplicativos constituem o topo da pilha da nuvem. Serviços prestados por esta camada podem ser acessados por usuários finais através de navegadores da web. Aplicações tradicionais de desktops, tais como processamento de texto e planilhas eletrônicas, já podem ser acessados como serviços na web. Este modelo de entrega de aplicativos, conhecida como Software como Serviço (SaaS), diminui a preocupação com manutenção do software para os clientes finais e simplifica o desenvolvimento e testes para os fornecedores (CSABR, 2012). O SaaS é o modelo de serviço de computação em nuvem menos flexível, uma vez que só permite configurações específicas do usuário na aplicação. Contudo não exige quase nenhum esforço de configuração e manutenção por parte do usuário. Os provedores deste tipo de serviço se encarregam de tarefas como atualização da aplicação, monitoramento e disponibilidade, *backups*, balanceamento de carga, etc.

Plataforma como serviço (PaaS – *Platform as a Service*) - No PaaS o recurso de TIC fornecido ao cliente é um ambiente no qual os desenvolvedores podem criar e implantar aplicações. O cliente não gerencia nem controla a infraestrutura na nuvem incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente configurações do ambiente de hospedagem de aplicações (NIST, 2011). É um modelo de nuvem menos flexível que IaaS – Infraestrutura como Serviço (do inglês *Infrastructure as a Service*), porém não tão fechado quando o SaaS.

Infraestrutura como serviço (IaaS – *Infrastructure as a Service*) - O IaaS consiste na oferta de recursos, geralmente virtualizados, de processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais nos quais o consumidor pode instalar e executar *softwares* em geral, incluindo sistemas operacionais e aplicativos (NIST, 2011). Os serviços de IaaS são considerados a camada mais inferior dos sistemas de computação em nuvem. A configuração do ambiente, incluindo a instalação das aplicações e bibliotecas necessárias, é feita pelo usuário do serviço, isso faz com que e

o IaaS seja o modelo de serviço mais flexível de computação em nuvem, pois, permite ao usuário configurar exatamente o que precisa.

2.4 MODELOS DE IMPLANTAÇÃO

Independente do sistema modelo de serviço utilizado, IaaS, PaaS ou SaaS, existem quatro modelos de implementação de nuvem: público, privado, hibrido e comunitário (Fig. 2). Embora a computação em nuvem tenha surgido principalmente a partir da oferta de serviços públicos de computação, outros modelos de implantação, com variações na localização física e na distribuição, foram adotados. E os principais são: o público, o privado, o comunitário e o híbrido.

Figura 2 - Modelos de implementação de nuvem (CSABR, 2012).

Nuvem pública - Esse tipo de implementação de nuvem consiste na oferta de serviços ao público em geral toda a infraestrutura física é provisionada e mantida pelo provedor de nuvem. As organizações ou pessoas clientes não tem controle sobre essa infraestrutura. As nuvens públicas são as que conferem maior economia às organizações clientes, porém é a que oferece os maiores riscos de segurança uma vez que esta é compartilhada por diversos clientes.

Nuvem privada - É uma infraestrutura de nuvem que é provisionada para uso exclusivo de uma única organização é construída em um *datacenter* interno de uma organização ou em um *datacenter* de um terceiro e não disponibilizado ao público em geral (CSABR, 2012). Na maioria dos casos, a adoção de uma nuvem privada corresponde uma reestruturação da infraestrutura existente, adicionando virtualização e interfaces de nuvem. Isso permite aos usuários interagir com o centro de dados local, enquanto experimenta as mesmas vantagens de nuvens públicas como autoatendimento, acesso a servidores virtuais sob demanda e medição e contabilidade baseados no uso (CSABR, 2012). A nuvem, privada é o modelo de implementação de nuvem que oferece o menor risco, por causa de sua natureza privada. No entanto é a que exige maior trabalho com gerenciamento por parte da organização usuária de nuvem, pois, a menos que ele contrate uma nuvem privada de um terceiro, a organização em questão é cliente e provedora ao mesmo tempo.

Nuvem comunitária - A infraestrutura de nuvem comunitária, é provisionada para uso exclusivo de uma comunidade específica de usuários, que têm preocupações comuns (por exemplo, considerações referentes a missão, requisitos de segurança e política). Ela pode ser controlada, gerenciada e operada por uma ou mais das organizações na comunidade ou por um terceiro (NIST, 2011). Um fator que merece destaque nesse modelo de implementação de nuvem é que concorrentes podem ter seus dados armazenados juntos (CASTRO e SOUSA, 2010). O que necessita de um cuidado especial no que tange a compartimentalização e a confidencialidade dos dados utilizados na nuvem.

Nuvem híbrida - A infraestrutura da nuvem híbrida é uma composição de duas ou mais infraestruturas de nuvem distintas (privada, comunitária ou pública) que permanecem como entidades únicas, mas são unidas por tecnologia padronizada ou proprietária que permita a portabilidade de dados e aplicativos entre elas (NIST, 2011).

Ainda existem alguns modelos derivados desses quatro fundamentais surgindo no mercado. Um exemplo de modelo emergente são as Virtual Private Clouds, que consiste em uma maneira de se utilizar infraestrutura de nuvem pública de uma forma privada, ou pelo menos semiprivada e conectando esses recursos via VPN (Virtual Private Network) aos datacenters internos dos clientes (CSA, 2011).

2.5 MODELOS DE REFERENCIA DE NUVEM

Entender as relações e dependências entre os modelos de computação em nuvem é fundamental para compreender os riscos de segurança. IaaS é o fundamento de todos os serviços de nuvem, com o PaaS sendo construído com base na IaaS, e SaaS por sua vez, sendo construído baseado no PaaS, como descrito no diagrama do Modelo de Referência de Nuvem, Fig. (3). Desta forma, assim como as capacidades são herdadas, também são herdadas as questões de segurança da informação e o risco. É importante notar que provedores comerciais de nuvem podem não se encaixar perfeitamente nos modelos de serviços em camadas. No entanto, o modelo de referência é importante para estabelecer uma relação entre os serviços do mundo real e o framework arquitetônico, bem como a compreensão dos recursos e serviços que exigem análise de segurança (CSABR, 2010).

A IaaS inclui todos os recursos da pilha de infraestrutura desde as instalações até as plataformas de hardware que nela residem. Ela incorpora a capacidade de abstrair os recursos (ou não), bem como oferecer conectividade física e lógica a esses recursos. Finalmente, a IaaS fornece um conjunto de APIs que permitem aos clientes de nuvem a interação e gestão da infraestrutura (CSABR, 2010).

A PaaS trabalha em cima da IaaS e acrescenta uma camada adicional de integração com frameworks de desenvolvimento de aplicativos, recursos de *middleware* e funções como banco de dados, mensagens e filas, o que permite aos desenvolvedores criarem aplicativos para a plataforma cujas linguagens de programação e ferramentas são suportadas pela pilha (CSABR, 2010).

O SaaS por sua vez, é construído sobre as pilhas IaaS e PaaS logo abaixo, e fornece um ambiente operacional autocontido usado para entregar todos os recursos do usuário, incluindo o conteúdo, a sua apresentação, as aplicações e as capacidades de gestão (CSABR, 2010).

Uma conclusão importante sobre a arquitetura de segurança é que quanto mais baixo na pilha estiver o serviço contratado, mais controles de segurança são de responsabilidade do cliente (CSABR, 2010).

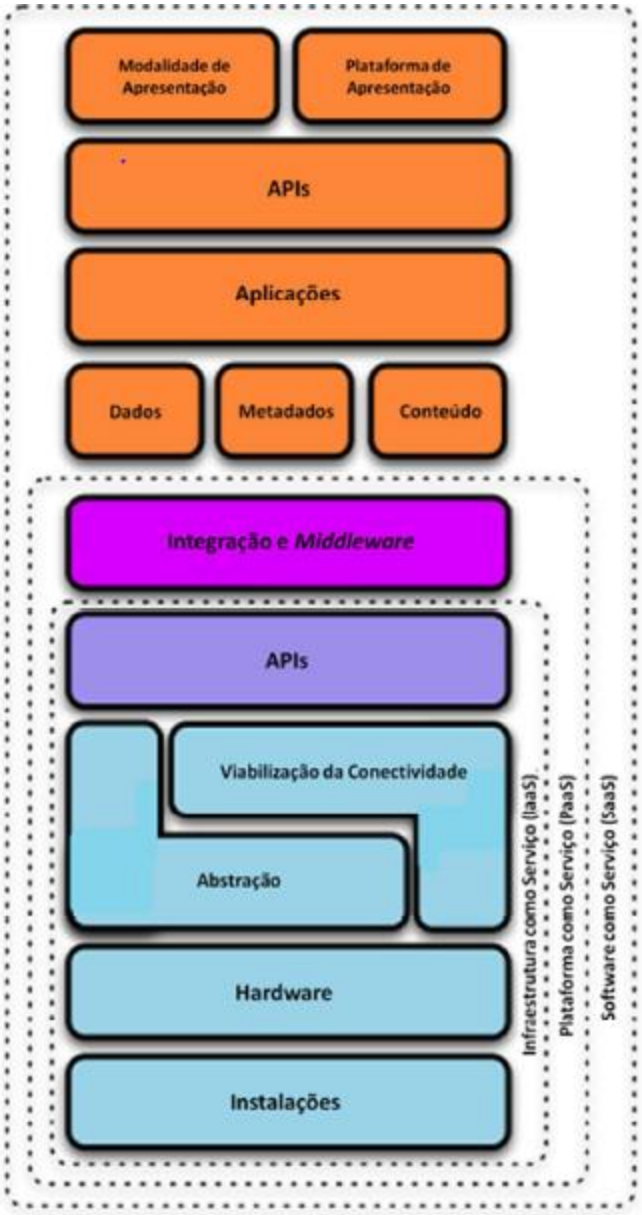

Figura 3 - Modelo de referência de nuvem (CSABR, 2010).

2.6 CLOUD SECURITY ALLIANCE

A Cloud Security Alliance é uma organização sem fins lucrativos que tem como missão promover o uso de melhores práticas de segurança na computação em nuvem. A Cloud Security Alliance é constituída por uma grande quantidade de profissionais das área de computação em nuvem e segurança, assim como empresas e associações interessadas em fazer da nuvem um ambiente mais seguro.

Os guias da Cloud Security Alliance são as referências mais citadas em livros e artigos sobre segurança em computação em nuvem. Portanto tanto pela falta de referência renomadas e pela qualidade dos guias apresentados pela Cloud Security Alliance esse trabalho tem seus guias como base.

2.7 ÁREAS CRÍTICAS DE SEGURANÇA DA COMPUTAÇÃO EM NUVEM

Treze áreas críticas de preocupação foram levantadas pela Cloud Security Alliance (2011). Nesse trabalho serão compilados os problemas, no que tange à computação em nuvem de cada uma dessas treze áreas críticas, assim como as recomendações para que esses problemas possam ser resolvidos. Essas áreas críticas de segurança são divididas em dois domínios: domínio de governança e domínio operacional.

Domínio de governança - As áreas que constituem esse domínio são amplas e tratam de questões estratégicas e políticas da organização que estão associadas com a computação em nuvem. As áreas que constituem esse grupo são: governança e gestão de riscos corporativos; aspectos legais e *Eletronic Discovery*; Conformidade e auditoria; gerenciamento do ciclo de vida da informação; portabilidade e interoperabilidade. Os problemas e preocupações de cada uma dessas área serão apresentados no capítulo três. E as recomendações de segurança serão apresentadas no capitulo 4.

Domínio operacional - As áreas que constituem esse domínio estão associadas as questões táticas de segurança e sua implementação. As áreas constituintes desse grupo são: segurança tradicional, continuação de negócios e recuperação de desastres; operações e *datacenter*; resposta a incidentes; segurança de aplicações; criptografia e gerenciamento de chaves; gerenciamento de identidade; virtualização. Os problemas e preocupações de cada uma dessas área serão apresentados no capítulo três. E as recomendações de segurança serão apresentadas no capitulo 4.

3 PROBLEMAS DE SEGURANÇA DA INFORMAÇÃO NA COMPUTAÇÃO EM NUVEM

A adoção da computação em nuvem pode trazer diversos benefícios para organização. Contudo a adoção de serviços de nuvem não pode se dar de forma não programada pois a mesma introduz novos riscos a organização. Portanto antes de se começar a utilizar serviços de computação em nuvem é importante que as organizações conheçam os riscos associados à adoção desse tipo de oferta de recursos de TIC.

Existem diversas preocupações quanto a adoção da computação em nuvem que vão desde disponibilidade até questões legais e regulatórias de um determinado segmento de mercado. As principais preocupações levantadas por WINKLER (2011) são:

- Disponibilidade de rede - Pois a computação em nuvem só pode ser utilizada quando sua conectividade e banda atingem limites mínimos. Uma vez que os serviços de nuvem necessitam de alta disponibilidade de rede e banda larga. Se esses dois pontos não estiverem disponíveis os serviços de nuvem não podem ser entregues.

- Viabilidade do provedor de nuvem - A viabilidade de um provedor de nuvem é um ponto importante a se observar, uma vez que os provedores de nuvem são relativamente novos a esse tipo negócio. Ainda existem provedores de nuvem que obrigam os clientes a utilizarem interfaces proprietárias o que no futuro pode levar a ficar preso a esse provedor ou em um cenário onde esse provedor venha a fechar a organização fica em uma situação difícil de troca de provedor pois está utilizando tecnologia proprietária.

- Recuperação de desastres e continuidade de negócio - Os usuários de nuvem precisam se preocupar quanto aos planos de recuperação de desastres e de continuidade de negócio dos provedores que estão contratando. De forma a ter segurança de que mesmo que um desastre ocorra em provedor de nuvem seus serviços e processos não sejam prejudicados e se prejudicados que indenizações sejam pagas pelo provedor.

- Incidentes de segurança - A notificação e respostas a incidentes de segurança também é uma outra grande preocupação que se tem. Pois, os clientes de nuvem precisam ser avisados quando um incidente ocorre e também necessitam de suporte por parte do provedor de nuvem para responder a esses incidentes. Se esses alarmes e suportes não existirem incidentes que poderiam ser rapidamente tratados podem se tornar grandes problemas levando a grandes prejuízos.

- Transparência - A questão da transparência é outra grande preocupação uma vez que as

organizações precisam conhecer as políticas de segurança de seus provedores para que possa fazer uma análise nas mesmas, afim de garantir que as políticas de segurança do provedor se adequam as políticas de segurança da própria organização.

- Perda de controle físico dos dados - A perda do controle físico dos dados também é uma grande preocupação das organizações que pensam em aderir a computação em nuvem. Ao se utilizar modelos de nuvem públicos ou comunitários as organizações perdem o controle físico dos dados e precisam de garantias que esses dados estão sendo tratados de forma adequada. A não observância da forma como os dados são tratados: armazenados, processados, criados e deletados. Pode acarretar processos legais e eventuais prejuízos a organização.

- Aspectos legais e regulatórios também são uma das grandes preocupações envolvidas no uso de computação em nuvem. E esse é um grande desafio para os provedores de nuvem pois obter padrões mínimos regulatórios de determinados segmentos de mercado envolvem requisitos não técnicos associados a maturidade da segurança da informação do provedor como um todo.

Os problemas elencados acima são apenas a ponta do iceberg. Diversos outros problema de segurança da informação serão apresentados seguindo as treze áreas de foco da segurança na nuvem apresentadas pela Cloud Security Alliance (2011). Primeiramente serão apresentados os problemas que afetam as áreas do domínio de governança, que tratam as questões políticas e estratégicas associadas a nuvem. Em seguida serão apresentados os problemas das áreas do domínio operacional, que estão associadas a implementação da nuvem em si e suas questões táticas de segurança da informação.

3.1 GOVERNANÇA CORPORATIVA E GESTÃO DE RISCOS

A computação em nuvem introduz novos desafios a governança corporativa e ao gerenciamento de riscos. Uma vez que a computação em nuvem pode afetar toda a maneira de se tratar de TIC em uma organização, pois, a nuvem possui características muito particulares. Dentre essas características destacam-se a elasticidade, a entrega de serviços sob demanda, serviços mensuráveis e utilizando um agrupamento de recursos computacionais de forma que para o cliente de nuvem os recursos parecem infinitos. Então processos de governança bem definidos para nuvem devem resultar em programas de gerenciamento de segurança da informação que sejam escaláveis com o negócio, aplicáveis em toda a organização, mensuráveis, sustentáveis, defensáveis, continuamente melhorados e com orçamentos justificáveis.

Um outro desafio associado a adoção da computação em nuvem que afeta a governança corporativa é a necessidade de garantir um nível razoável de segurança da informação em toda a cadeia de fornecimento da informação. No caso da adoção de modelos de nuvem públicas ou comunitárias as organizações perdem o controle físico dos dados. Dessa forma mesmo que medidas de segurança estejam sendo tomadas dentro da organização se os mesmos cuidados com segurança não forem tomados no provedor de nuvem, toda a segurança estará comprometida.

O elemento principal de governança corporativa na nuvem é o acordo feito entre cliente e provedor. Esses acordos podem ser extremamente personalizados ou podem ser acordos padrões para todos os clientes de um determinado provedor. Esses acordos são chamados de SLA (do inglês Service Level Agreement) ou acordo de nível de serviço.

3.3.1 GOVERNANÇA CORPORATIVA

A governança corporativa é o conjunto de processos, tecnologias, costumes, políticas e leis que afetam o modo em que uma empresa é dirigida. A governança corporativa ainda trata das relações entre os diversos *stakeholders* [2]e os objetivos da organização. Uma boa governança tem como base a aceitação de que os acionistas são os verdadeiros donos da corporação e que os membros da gerência da empresa

[2] *Stakeholder* – Termo que em português significa parte interessada.

são pessoas a quem foi confiado o poder de gerir a organização afim de gerar lucro aos acionistas.

Existem vários modelos de governança corporativa mas todos eles seguem cinco princípios básicos:

- Auditoria da rede de fornecedores
- Conselho e estrutura de gestão e processo
- Responsabilidade corporativa e cumprimento
- Transparência financeira e divulgação de informação
- Estrutura de propriedade e exercício dos diretos de controle

3.1.2 GESTÃO DE RISCOS

Organizações de todos os tipos e tamanhos enfrentam riscos que podem afetar a realização de seus objetivos. Todas as atividades de uma organização envolvem riscos pois todas envolvem incertezas fazer a gerencia dessas incertezas confere vantagens competitivas as organizações. Daí a importância de uma gestão de ricos. Uma gestão de riscos quando bem implementada permite que a uma organização: gerencia proativa ao invés de reativa, melhora na descoberta de oportunidades e ameaças, melhorar a governança corporativa, melhorar a confiança dos *stakeholders*, estabelecer bases sólidas para tomada de decisões, melhorar a efetividade e a ineficiência operacional, aumentar a resiliência da organização e minimizar perdas (ISO, 2009).

Gestão de riscos da informação é processo de identificar e entender a exposição a riscos e a capacidade de geri-los, alinhados com a tolerância e o apetite de assumir riscos do dono da informação. Portanto conhecer os riscos associados à adoção de um modelo ou serviço de computação em nuvem é essencial para que a decisão de se migrar, dados, processos ou aplicativos, para nuvem seja feita de forma bem planejada, de forma que a organização entenda os riscos que ela está correndo e quais ela está disposta a aceitar, quais ela quer transferir, quais reduzir e quais evitar.

Uma ponto de preocupação dos clientes de nuvem é quanto a transparência de seus provedores, pois, os clientes devem revisar os processor de gestão de riscos e governança com seus provedores e assegurar-se de que as práticas estão consistentes e alinhadas. Um outro problema é a falta de métricas para medir o desempenho e a eficácia do gerenciamento de segurança. Ainda existe o problema da dificuldade de auditar essas métricas. Os provedores também geralmente são muito fechados e a maioria deles não permite que testes de penetração e avaliação de vulnerabilidades sejam feitos por clientes. O que torna bastante difícil a descoberta de novas ameaças, que é essencial para uma boa gestão de riscos.

Os principais problemas de segurança da informação quanto a governança corporativa e gestão de riscos então são:

- Falta de conhecimento por parte dos clientes de quais são os controles de segurança empregados por seus provedores de serviço e seus fornecedores.
- Falta de envolvimento do departamento de segurança da informação para o estabelecimento dos acordos de níveis de serviço.
- Falta de métricas bem definidas para medir o desempenho do gerenciamento de segurança da informação.
- Os clientes geralmente não fazem o gerenciamento de risco específicos para a nuvem, isso faz com que as organizações desconheçam as ameaças e os critérios de aceitação dos riscos.
- Provedores de nuvem com negócios imaturos e pouco resilientes, podem levar a interrupções inesperadas de serviços acarretando prejuízos.
- Falta de conhecimento dos clientes de nuvem quanto a rede de fornecedores do seu provedor

de serviço.

3.2 ASPECTOS LEGAIS E *ELETRONIC DISCOVERY*

O uso da computação em nuvem, principalmente em implementações de nuvem pública ou comunitária, muda a dinâmica do relacionamento entre a organização e suas informações uma vez que nestes modelos de implementação, geralmente, existe um terceiro, o provedor de nuvem, que é quem tem a custódia da informação. Isso faz com que surjam novos problemas relacionados ao entendimento de como as leis se aplicam.

Um dos principais desafios da computação em nuvem é quanto à conformidade. As organizações estão preocupadas se sofrerão processos legais, ou multas, devido a possível perda de conformidade ao se utilizar de algum serviço de nuvem (WINKLER, 2011).

Eletronic discovery, ou e-discovery é o processo de coleta de informações digitais para servir de evidência em processos litigiosos. E esta é uma tarefa um tanto quanto difícil em um ambiente de nuvem devido à natureza distribuída e dinâmica dos serviços de nuvem. A multilocação ainda adiciona uma parcela a mais de dificuldade, pois, o processo de e-discovery deve ser feito de forma que ao se procurar evidencias sobre um cliente do provedor de nuvem informações de outros clientes não sejam reveladas. Portanto forte compartimentalização deve ser empregada afim de que informações que não pertençam a empresa investigada ou envolvida em processo litigioso vase.

A virtualização também introduz dificuldades ao e-discovery uma vez que informações podem ser trocadas em uma rede virtual que muitas vezes não possuem sistemas de log ou registro de ações.

Um outro risco associado as questões legais está na terminação de contratos. E se não definidos em contrato os processos de terminação do mesmo, pode provocar interrupções no serviço ou até mesmo a perda de informações, sem que nenhuma sansão seja feita ao provedor. Estes provedores que agora não mais servem a organização também podem se recusar a liberar dados que estejam em suas bases de dados e sistemas de arquivos. Portanto desde a adoção de um provedor de nuvem deve-se pensar em como se dará o término dessa relação, e tudo deve estar bem definido em contrato.

A privacidade dos dados é uma outra grande preocupação legal uma vez que muitos dados não podem ser divulgados a terceiros ou utilizados com outros propósitos. Por exemplo números de cartões de crédito não podem ser divulgados a terceiros. Com a adoção da nuvem essa preocupação torna-se ainda maior uma vez que vários clientes de nuvem, geralmente, compartilham uma mesma infraestrutura física. E a garantia de que os dados armazenados na nuvem não sejam revelados ou acessados de forma indevida é de responsabilidade do provedor, mas quem sofrerá os processos legais é a organização que armazenou na nuvem. A garantia que esses dados também serão armazenados, processados, e movimentado de forma a garantir a privacidade dos mesmos também estar em contrato. Portanto deve ser definido contratualmente que se caso haja o vazamento de dados e que isso implique em processos litigiosos quem deve arcar com os custos deve ser o provedor de nuvem (MATHER, KUMARASWAMY e LATIF, 2009).

Uma outra grande preocupação no que tange os aspectos legais da nuvem é a localização fisica dos dados. Diversas organizações principalmente governamentais não podem ter dados armazenados fora do país. E uma vez que os dados na nuvem podem ser armazenados em diversos países espalhados pelo mundo, deve ser definido por contrato que os dados ficarão dentro das premissas de um determinado país ou região. Outra ponto importante é garantir que o backup dessa informação também não esteja em local indevido uma vez que o backup contém uma cópia da informação original o mesmo também está sujeito as mesmas normas e regulações da informação original.

Os principais problemas de segurança da informação quanto aos aspectos legais e *Electronic discovery* são:

- Papéis de responsabilidade mal definidos
- Localização dos dados armazenados nos provedores de nuvem não definida em contrato
- Falta de garantias contratuais quanto aos vazamento de dados confidenciais.
- Procedimentos mal definidos de resposta a intimações judicias para descoberta de dados.
- Clausulas de termino de prestação de serviço mal definidas

3.3 CONFORMIDADE E AUDITORIA

Conformidade e auditoria são os processos internos e externos que tem como objetivo identificar os requerimentos que uma determinada organização tem que cumprir, leis, regulações, contratos com clientes etc. Esses processos também se estendem a implementação e monitoramento de políticas, processos e sistemas que façam que a organização atenda todos os requisitos legais e contratuais que estas se propôs ou que está sujeita devido a regulamentação do setor (MATHER, KUMARASWAMY e LATIF, 2009).

Funções de auditoria e conformidade sempre tiveram um papel importante em relacionamentos tradicionais de terceirização. No entanto essas funções tem uma natureza ainda mais elevada dado a natureza dinâmica dos serviços de nuvem. Provedores de nuvem tem que estabelecer, monitorar e demonstrar conformidade com um conjunto de controles que atendem as necessidades regulatórias de seus clientes. Manter esforços separados para diferentes necessidades regulatórias não é sustentável. Um abordagem pratica para auditoria e conformidade na nuvem inclui uma combinação coordenada de política interna de conformidade, conformidade regulatória, e auditoria externa. Dessa forma provedores de nuvem devem levanta os requisitos regulatórios de toda sua base planejada de clientes e implementar os processos, políticas e sistemas necessário para atender todos esses requisitos (MATHER, KUMARASWAMY e LATIF, 2009).

Os clientes de nuvem então devem então observar a capacidade do provedor de nuvem de produzir evidências de que atende os seus requisitos de conformidade. O cliente de nuvem ainda deve estar ciente de quais responsabilidades, quanto à conformidade, são suas e quais são do provedor de nuvem.

Alguns padrões de conformidade para a nuvem já estão em desenvolvimento. E estes são:

- ISO/IEC 27017: *Cloud Computing Security and Privacy Management System-Security Controls*
- ISO/IEC 27036-x: *Multipart standard for the information security of supplier relationship management that is planned to include a part relevant to the cloud supply chain*
- ITU-T X.ccsec: *Security guideline for cloud computing in telecommunication area*
- ITU-T X.srfcts: *Security requirements and framework of cloud-based telecommunication service environment*
- ITU-T X.sfce: *Security functional requirements for Software as a Service (SaaS) application environment*

Os principais problemas de segurança da informação quanto à conformidade e auditoria na nuvem são:

- Provedores fechados a auditorias por parte dos clientes.
- A falta de análise de como o serviço de nuvem contratado impacta na conformidade.
- Falta de conhecimento de quais controles de segurança são de responsabilidade do cliente e quais são de responsabilidade do provedor.
- Falta da demonstração de conformidade por parte dos provedores de nuvem.

3.4 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DOS DADOS

O gerenciamento de informações e a segurança dos dados em um ambiente de nuvem são tarefas desafiadoras, uma vez que ao se utilizar a computação em nuvem as informações da organização podem ser acessadas de diversos dispositivos: *smartphones*, *tablets*, *notebooks*, estações de trabalho basicamente qualquer aparelho capaz de rodar um navegador web. Associado grande elasticidade e a multilocação à ubiquidade da nuvem requer novas estratégias de segurança (CSABR, 2010).

O ciclo de vida da segurança de dados consiste de seis fases: criar, armazenar, utilizar, distribuir, arquivar e destruir. Entender como a nuvem influência cada uma dessas fases é extremamente importante para garantir a segurança apropriadas dos dados que estão na nuvem. Portanto, medidas como criptografia em todas as fases é importante para que se mantenha a confidencialidade dos dados.

Além das questões de criptografia outro ponto de preocupação quanto à segurança dos dados é quanto ao acesso as informações. Como a nuvem possibilidade que informações sejam acessadas de qualquer lugar do mundo por diferentes dispositivos controles de acessos bem rígidos devem ser empregados para garantir a segurança das informações na nuvem.

Outro ponto de preocupação é quanto ao armazenamento desses dados. Se os dados forem agrupados por algum tipo de padrão, se o padrão for revelado isso pode revelar informações sobre os dados mesmo que estes estejam criptografados.

A questão do backup e recuperação de dados também é outro desafio na nuvem. A segurança do backup é tão importante quanto a do próprio dado uma vez que mesmo contém uma cópia do conteúdo da informação original. Por isso, os backups devem também ser criptografados e também possuir um forte controle de acesso. A recuperação de dados também levantam preocupações quanto a velocidade em que dados perdidos sejam recuperados de forma a não comprometer os serviços e processos que utilizam esses dados.

Questões como a exclusão dos dados também levantam preocupações, pois, como o cliente de nuvem, publica e comunitária, geralmente perde o controle físico dos dados, ele precisa ter garantias de que os dados que ele mandou excluir de uma determinada base de dados é realmente excluído.

Os principais desafios relativos ao gerenciamento de informações e segurança dos dados levantados nessa pesquisa são: a localização dos dados, o acesso aos dados, a persistência dos dados, a mesclagem dos dados com os dados de outros clientes da nuvem, o *backup* e restauração dos dado, o *e-discovery*, a migração dos dados e a empregada criptografia aos dados assim como sua respectiva gerência de chaves.

Os principais problemas de segurança da informação quanto ao gerenciamento de informações e segurança dos dados na nuvem são:

- Falta de conhecimento da arquitetura em que os dados são armazenados.
- Falta de controles apropriados na transferência de dados para dentro e para fora da nuvem.
- Má utilização da criptografia.
- Dados em locais desconhecidos pelos clientes de nuvem.
- Dados de diferentes clientes misturados no provedor de nuvem.
- Provedores podem não excluir realmente os dados, mesmo que tal ação seja comandada pelo cliente.

3.5 PORTABILIDADE E INTEROPERABILIDADE

A portabilidade e a interoperabilidade permitem tornar a nuvem ainda mais escalável, uma vez que se os serviços utilizados possuem as características de portabilidade e da interoperabilidade, estes serviços podem ser distribuídos através de diversos provedores de nuvem. Além disso a interoperabilidade e a portabilidade permitem que se migre serviços de um provedor para outro sem que estes tenham que ser

alterados. Portanto ao se utilizar serviços que possuam as características de portabilidade e interoperabilidade os usuários de nuvem tem a liberdade de migrar entre provedores buscando sempre aqueles que melhor atendem as suas necessidades. Por outro lado, a falta de portabilidade e interoperabilidade pode fazer com que se fique preso a um provedor e as tecnologias utilizadas pelo mesmo.

É importante que servidores de nuvem utilizem protocolos e arquiteturas abertas e padrões, pois, dessa forma se um serviço oferecido a um cliente precisar ser movido de um provedor de nuvem para outro, essa migração possa se dar de forma simplificada e sem que os clientes tenham que modificar suas aplicações ou processos para que estes funcionem no novo provedor de nuvem. Já o uso de protocolos e tecnologias proprietárias pode fazer com que os clientes de nuvem fiquem presos a um determinado provedor de serviço.

Os principais problemas de segurança a informação quanto a portabilidade e interoperabilidade são:

- O uso de tecnologias proprietárias, não padrões, que pode levar os clientes de nuvem a ficarem presos a um determinado provedor de serviços de nuvem.
- Processos mal definidos de migração.

3.6 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

É muito importante conhecer os mecanismos de segurança tradicional, planos de continuidade de negócios e recuperação de desastres do provedor de nuvem do qual se pretende contratar serviços de nuvem. Segurança tradicional aqui consiste em segurança física e do ambiente, tratada na seção 9 da ISO 27002. Nesta seção serão endereçados os principais problemas quanto à segurança tradicional, continuidade de negócios e recuperação de desastres no que tange a computação em nuvem hoje.

Segurança fisica e do ambiente consiste em prevenir o acesso não autorizado, danos e interferências as instalações e informações da organização. E para computação em nuvem não é diferente, pois, mesmo se utilizando um modelo de computação diferente, normalmente distribuído, essa infraestrutura física ainda se encontra em algum lugar. Quando se está tratando de implementações de nuvem pública ou comunitárias a segurança física do *datacenter* do provedor deve ser ainda mais reforçada, pois, neste *datacenter* podem se encontrar informações críticas de diversas pessoas e organizações (ABNT, 2005).

Os clientes de computação em nuvem também devem estar atentos se o provedor de nuvem está em conformidade com padrões globais de segurança da informação como a ISO 27001 e outros padrões da indústria como COBIT, ITIL, TOGAF, SABSA e COSO. Desse forma se tem a garantia de que o provedor emprega as melhores técnicas de gerencia de TIC e segurança da informação.

Um preocupação que muitas organizações também tem é quanto ao pessoal que trabalha no provedor de nuvem contratado. Uma vez o que provedor é que tem a custódia dos dados é importante observar quais são os processos de checagem do passado de seu pessoal, os papeis e responsabilidades dos empregados, os contratos de emprego e os processos de demissão. Uma importância maior deve ser dada ao processo de demissão uma vez que essa pode gerar descontentamento por parte do usuário e se o mesmo ainda possuir acesso após a demissão este como uma forma de vingança pode causar sérios danos ao provedor e nuvem e a seus clientes.

Continuidade de negócios e recuperação de desastres também levantam diversas duvidas e receios nos clientes de nuvem, pois, alguns provedores de nuvem não conferem transparência ou possibilidade de auditoria e teste nos planos e processos de continuidade de negócios e recuperação de desastres. Então os clientes ficam preocupados quanto ao que acontece caso algum desastre ocorra em seus provedores de nuvem, dados podem ser movidos para *datacenters* em outra localidade, serviços podem ser interrompidos, dados podem ser perdidos. Portanto é importante que ao se contratar um cliente em nuvem o cliente saiba o quais são os planos de recuperação de desastres de seus provedores e fazer exigências em contrato como tempo para retomada do serviço etc.

Os principais problemas de segurança física e do ambiente, no que tange à computação em nuvem, são:

- Os clientes de nuvem têm pouco ou nenhum conhecimento sobre os controles de segurança empregados pelos provedores de nuvem
- Processos de recuperação de desastres mal definidos nos acordos de nível de serviço.
- Plano de continuidade de negócio dos provedores muitas vezes são desconhecidos pelo cliente.
- Clientes de nuvem com pouca abertura para fazerem inspeções e auditorias nos processos e instalações do provedor.

3.7 OPERAÇÕES E *DATACENTER*

O número de provedores de computação em nuvem continua a aumentar, mais e mais organizações e pessoas passam a utilizar serviços de TIC na nuvem. Para suportar esse crescimento de usuários e provedores cada vez mais datacenter são construídos. Provedores de serviços de todos os tamanhos estão fazendo grandes investimentos em datacenters para atender a demanda crescente por serviços de nuvem. E os clientes de nuvem devem estar atentos em como os provedores de nuvem implementam as características essenciais da nuvem em seus *datacenters*. Pois se feitas de uma forma em que não se leva em conta a segurança da informação o programa de segurança já estará comprometido desde sua infraestrutura fisica. Portanto é muito importante para clientes de nuvem ou organizações que pretendam migrar para a nuvem estar ciente dos controles de segurança empregados na construção dos data centers de seus provedores.

Um outro desafio dos provedores é demonstrar aos clientes que esses novos datacenters estão de acordo com os requisitos de conformidade de sua base de clientes. O cliente de nuvem também deve ter a possibilidade de auditar os *datacenters* de seus provedores a fim de garantir que as práticas de segurança empregadas nos *datacenters* destes provedores estão de acordo com a política de segurança do cliente.

A localização dos datacenters de um provedor também deve ser um ponto observado pelos clientes de nuvem, pois, determinadas organizações não podem ter seus dados armazenados fora de uma determinada região ou país. Portanto, conhecer a localidade dos *datacenters* é um dos pontos chaves na adoção de um serviço de nuvem.

Os principais problemas e preocupações quanto aos *datacenters* que suportam o serviços oferecidos na nuvem são:

- Provedores de nuvem geralmente colocam entraves para a realização de auditorias em seus *datacenters*.
- Falta de conhecimento do local do *datacenter*.
- Clientes de nuvem geralmente tem pouco ou nenhum conhecimento de como as características essências dos serviços de computação em nuvem são implementadas e como se dá o compartilhamento dos recursos.

3.8 RESPOSTA A INCIDENTES

Resposta a incidentes é um dos principais elementos de um plano de segurança uma vez que nem o melhor planejamento de segurança possível consegue eliminar totalmente a ocorrência de alguma falha. Portanto a necessidade de se saber o que fazer quando um incidente ocorre.

As principais preocupações que a nuvem introduz quanto a resposta a incidentes são as seguintes:

A natureza sob demanda dos ambientes de nuvem pode fazer com que seja muito difícil receber a cooperação do provedor de nuvem para lidar com um incidente de segurança. Daí a importância de

situações como essa já estarem previstas em contrato pois o auxílio prestado pelo provedor de nuvem pode variar bastante de cenário para cenário.

O compartilhamento de recursos computacionais e a elasticidade da nuvem também podem complicar baste a resposta a incidentes principalmente no que tange a analise forense. Pois, ter que efetuar a analise forense nesse ambiente altamente dinâmico, desafia as necessidades básicas da análise forense. Que é de fazer os a análise do ocorrido em um cenário igual ao do incidente.

Outro problema de segurança que os clientes de nuvem devem estar atentos é quanto à privacidade de coinquilinos quando se é feita a análise de um incidente. Á verificação de logs, fluxo de rede, memória, armazenamento etc. Pode revelar informações sobre os coinquilinos[3] que compartilham os mesmos recursos físicos. Portanto revelar os dados necessários para análise de um incidente que aconteceu na instância de um usuário sem revelar informações sobre as instâncias coinquilinas é um dos desafios do provedor de nuvem e algo que os usuários de nuvem devem estar atentos.

Os clientes de nuvem também devem estar atentos ao fato de que dados que estão armazenados em um provedor de nuvem podem ser movidos para outra localização geográfica até mesmo outro país. E isso pode influenciar no que pode e o que não pode ser feito na ocorrência de um incidente. Portanto é necessário que contratos de serviços sejam bem definidos, e que tratem da questão do armazenamento de dados ou maquinas virtuais em regiões geográficas nas quais leis diferentes são aplicadas.

Os principais problemas e preocupações no que tange a resposta a incidentes são:

- Falta de formalização da definição do que é um incidente para uma organização cliente.
- Papéis mal definidos entre clientes e servidor na resposta a incidentes.

3.9 SEGURANÇA DE APLICAÇÕES

Computação em nuvem mostra-se um desafio para aplicações, pois, as aplicações na nuvem devem implementar todos os controles de segurança como se tivesse em uma rede completamente desprovida de segurança. Porém as ameaças as quais uma aplicação estará vulnerável na nuvem não são as mesmas encontradas em ambientes tradicionais. Preocupações com a multilocação e criptografia devem ser cuidadosamente tratadas desde os primeiros rascunhos do aplicação.

No que tange o ciclo de vida de desenvolvimento de uma aplicação para nuvem uma grande preocupação é quanto compatibilidade que esta terá entre provedores. Escolher tecnologia padrões que garantam que a aplicação possa ser migrada de um provedor para o outro sem grandes alterações é algo importantíssimo e os desenvolvedores devem estar atentos a isso. Um outro ponto de preocupação das organizações é quanto à conformidade de uma aplicação na nuvem, pois esta é uma tarefa bastante desafiadora em um ambiente de nuvem como relatado na seção 3.3.

A proteção dos dados também é um outro ponto importante, como esses dados serão armazenados, trocados e processados de forma a garantir sempre a integridade, confidencialidade e disponibilidade dos mesmos deve ser levado em conta no desenvolvimento da aplicação. Decidir quando e quais dados serão criptografados pela aplicação é algo importantíssimo a se fazer. A combinação de possíveis *web services* utilizados pela aplicação também deve ser tratada com cuidado e fortemente observada uma vez que um desses serviços pode introduzir brechas na segurança da aplicação. Outro ponto de preocupação é quanto o acesso a logs, principalmente em nuvens públicas onde os mesmos podem estar distribuídos através de diversas maquinas físicas a forma de obtenção dos mesmos devem estar bem definidas em SLAs.

As organizações clientes de nuvem devem então estar atentas aos novos riscos potenciais quanto ao

[3] Coinquilinos são usuários de nuvem que compartilham os mesmos recursos físicos mas que utilizam instancias virtuais diferentes.

acesso de informações sensíveis que vão estar na nuvem devido à aplicação. Os principais riscos que essas informações podem correr são: a falta de controle sobre políticas e controles de segurança; falta de visibilidade sobre os controles de segurança e sua efetividade; a falta de gerenciabilidade da segurança da aplicação que se encontra na web, principalmente quanto as políticas de acesso e auditoria; a perda de governança; o risco de uma organização não atender requisitos de conformidade que se alteraram devido a uma possível inflexibilidade de um provedor; falha de isolamento, ou seja empresas concorrentes que rodam suas aplicações em uma mesma infraestrutura como coinquilinos podem ter informações acessadas ou manipuladas por com inquilinos de forma acidental ou não; a perda de proteção dos dados devido a uma falha no armazenamento dos dados ou das chaves que os criptografam; risco de que as interfaces de gerencia e controle de acesso sejam comprometidas, comprometendo toda a aplicação.

Um outro ponto de preocupação das organizações devem ter é com a integração com sistemas de gerência de acesso e identidade. Uma vez que esses sistemas estão diretamente relacionadas com funções importantes da aplicação como a parte de cobranças, a integração entre a aplicação e o sistema de gerência de acesso e identidade deve ser tratada desde o projeto da aplicação.

Uma aplicação que roda na nuvem ainda sofre a possibilidade de um ataque do tipo DoS – Negação de serviço (do inglês Denial of Service) que consiste em tornar um serviço indisponível, geralmente devido a múltiplas conexões maliciosas.

As informações apresentadas nessa seção mostram que diversos cuidados específicos devem ser tomados para que uma aplicação rode na nuvem de forma de segura. Desde o seus desenvolvimento até sua desativação existem particularidades em aplicações que rodam em um ambiente de nuvem.

3.10 CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES

Ambientes de nuvem geralmente são compartilhados por multilocatários daí a necessidade de se proteger seus dados contra roubo. Uma vez que os múltiplos locatários que compartilham um servidor físico podem ser concorrentes e caso algum desses consiga acesso a informações privilegiadas pode acarretar sérios prejuízos para a outra parte. Até mesmo em caso de nuvens privadas é essencial que os dados sejam criptografados pois dados de determinados usuários e departamentos não devem ser vistos por outros usuários ou departamentos. Os dados na nuvem estejam esses em movimento, ociosos ou em uso devem ser criptografados para evitar que informações sigilosas sejam comprometidas.

As preocupações que um provedor de nuvem e os clientes devem ter é de quais protocolos estão utilizando para criptografar os dados. Estando sempre atento a novas falhas nesses protocolos escolhidos. Outro cuidado que uma organização deve ter é o de fazer uma avaliação dos dados pois nem todos os dados necessitam ser criptografados. Uma vez que a criptografia demanda mais processamento, podendo causar problemas de performance se utilizada em todos os dados.

O gerenciamento apropriado de chaves também é importantíssimo, pois, se as chaves forem comprometidas os dados criptografados com a mesmas também estão comprometidos. Então os repositórios de chaves na nuvem devem ser tão bem, protegidos quanto outros repositórios de informações sensíveis uma vez que o armazenamento impróprio das chaves pode ao comprometimento de informações sigilosas. Um forte controle acesso deve ser empregado a esses repositórios de chaves. O acesso deve ser restrito a chaves individuais necessárias. Ainda quanto a gerência de chaves é extrema importância que exista um backup das chaves e meios para que esta possa recuperada. Uma vez que um chave perdida implica na perda do dado criptografado também pois o mesmo não poderá mais ser descriptografado não representando nenhuma informação útil. Os clientes de nuvem também devem estar atentos aos controles de segurança empregados as mídias de backup pois estas contém cópias das informações originais e merecem tanto cuidado quanto as informações originais.

Os principais problemas no que tange a gerência de chaves e criptografia na nuvem são:

- Uso de padrões criptográficos inseguros
- Gerência de chaves ruim, resultando na perda ou comprometimento de chaves.

- Uso de algoritmos criptográficos proprietários, que podem não ser suportados por outros provedores, o que pode resultar na necessidade de reestruturação de processos e aplicações no caso de mudança de provedor.

3.11 GERENCIAMENTO DE IDENTIDADE

Com a adoção de serviços de computação em nuvem o controle da infraestrutura, dos sistemas, e das aplicações podem ser transferidos para o provedor de nuvem, dependendo do modelo de serviço contratado. Essa perda de controle desafia os controles de governança estabelecidos e confiáveis. Se não gerido adequadamente essa perda de controle pode impedir com que empresas adotem a computação em nuvem. Para compensar essa perda de controle perda de controle, nos elementos de baixo nível como rede e infraestrutura, as organizações utilizam-se de controles em um nível mais alto, geralmente em suas aplicações, esses controles geralmente se manifestam como forte autenticação. E para um gerenciamento efetivo de identidade e acesso na nuvem deve se observar três pontos cruciais: o provisionamento de identidade, a autenticação e a federação.

Um dos maiores desafios para a adoção de serviços de computação em nuvem pelas empresas é o gerenciamento seguro e ágil do provisionamento e desaprovisionamento de identidade a usuários na nuvem. Um outro ponto importante de preocupação quando se utiliza serviços de nuvem é a autenticação que na nuvem exige um bom gerenciamento de credenciais, forte autenticação, delegação de autenticação e gerenciamento de segurança (CSABR, 2010).

As identidades federadas tem um papel fundamental em gerencia de identidade e acesso na nuvem uma vez que essas permitem que organizações autentiquem seus usuários utilizando um provedor de identidade, uma terceira parte confiável responsável por autenticar um usuário. Essas estrutura centralizada de autenticação tem diversos benefícios mas deve ser muito bem gerida. Uma vez que se esta for comprometida todo o processo de autenticação também estará.

Os principais problemas de segurança da informação no que tangue o gerenciamento de identidade são:

- O uso de tecnologias proprietárias, não padrões.
- Uso de repositórios de identidade que não suportem aplicações e processos na nuvem.
- Autenticação por canais inseguros, o que pode resultar no roubo de dados de acesso.

3.12 VIRTUALIZAÇÃO

Virtualização embora não seja essencial para um ambiente computação em nuvem hoje é um dos elementos chave das ofertas de IaaS e nuvens privadas, e está cada vez mais sendo usada no plano de fundo, infraestrutura, de provedores de PaaS e SaaS. Virtualização é também é uma tecnologia muito utilizada para prover áreas de trabalho virtuais, que são muito utilizadas dentro de nuvens privadas dentro de organizações. A capacidade de prover multilocação no nível de infraestrutura, plataforma, ou aplicação também é sustentada pela virtualização. Daí a importância em conhecer os riscos introduzidos por essa em um ambiente de computação em nuvem.

Os benefícios da virtualização são bem conhecidos dentre estes destacam-se a multilocação e a melhor utilização da infraestrutura física. Provedores de nuvem podem obter maior densidade computacional, o que se traduz em maior número de clientes atendidos por servidor, assim as empresas podem diminuir o capital gasto em *hardware* de servidores e aumentar a eficiência operacional utilizando a virtualização (VMWARE, 2009).

A virtualização traz consigo além de todos os benefícios supracitados todas as preocupações de segurança de um sistema operacional rodando como hospedeiro. Também traz os problemas quanto a segurança da camada de *hypervisor*, assim como novas ameaças especificas da virtualização. A

virtualização ainda provoca impactos na segurança de rede uma vez que maquinas virtuais podem se comunicar por outros meios sem ser a rede.

As principais preocupações quanto a segurança de ambientes virtualizados na nuvem hoje são:

- **Proteção adequada de maquinas virtuais hospedeiras** - Consiste em instalar todos os mecanismo de proteção necessários em um servidor nessa máquina virtual. Maquinas virtuais mal protegidas podem levar a indisponibilidade no serviço.

- ***Instant-on gaps*** – *Instant-on gaps* são brechas na segurança ao se ligar uma máquina virtual isso se dá pela facilidade com que uma máquina virtual pode ser parada e iniciado, combinado com a velocidade que ameaças mudam, criam uma situação onde uma máquina virtual pode estar configurada de forma segura quando ela é desligada, mas quando ele é reiniciada, as ameaças evoluíram, deixando a máquina virtual vulnerável.

- **Segurança do Hypervisor** - O hypervisor precisa está trancado e fortalecido com as melhores práticas de segurança. A principal preocupação empresas e usuários que utilizam virtualização deve ser a gerência apropria das configurações do *hypervisor* e também segurança física do servidor que o hospeda.

- **Ataques inter-VM** - Virtualização tem um grande impacto na segurança de redes. Maquinas virtuais podem ser comunicar em plano de fundo de hardware sem ser a rede. Como resultado, controles de segurança de redes padrões são controlam esse trafego trocado. É importante que os clientes cobrem de seus provedores controladores de redes que possam monitorar esse trafego de dados entre maquinas virtuais também.

- **Preocupação quanto a performance** - A instalação de aplicações desenvolvidas para servidores físicos, não virtualizados, pode resultar em grande degradação da performance, tarefas como como *scan* antivírus que tem alto uso de CPU são as que mais impactam na performance. Tanto cliente como provedor de nuvem devem utilizar ferramentas próprias para ambientes virtualizado para que dessa forma não haja uma degradação da performance do ambiente virtualizado.

- **Aumento da complexidade operacional do *VM Sprawl*[4]** - A facilidade com que maquinas virtuais podem ser provisionadas levam a um aumento no número de pedidos por maquinas virtuais em empresas típicas. Isso cria uma maior superfície de ataques e aumenta as chances de uma configuração ruim ou um operador abrindo um buraco na segurança.

- **Criptografia de maquinas virtuais** - Imagens de maquinas virtuais são vulneráveis a roubos e modificações quando estas estão inativas ou rodando. A solução para esse problema é criptografar as imagens de maquinas virtuais estejam essas em uso ou inativas, mas existe um problema quanto a performance em fazê-lo. Para ambientes que necessitam de alta segurança o custo de performance vale a pena. Já para ambientes a performance é essencial pode não ser interessante que criptografia seja aplicada nessas instancias virtuais.

- **Mistura de dados** – Existe a possiblidade de que dados de diferentes maquinas virtuais possam ser misturados pelo fato de compartilhar a mesma infraestrutura física. Portanto há a necessidade de se isolar as maquinas virtuais e seus fluxos de dados.

- **Destruição de dados da máquina virtual** - Quando uma máquina virtual é movida de um servidor físico para outro, empresas precisam de garantias de que nenhum bit foi deixado para trás no disco e que esse de alguma forma possa ser recuperado por outro usuário.

- **Adulteração de maquinas virtuais** - Imagens pré-configuradas de maquinas virtuais podem

[4] VM Sprawl é definido como um grande número de maquinas virtuais em uma rede sem gerência apropriada (WARREN, 2008).

ter sido mal configuradas ou podem ter sofrido adulteração antes de serem iniciadas portanto uma vez iniciadas essas imagens adulteradas podem expor o sistema do cliente a diversas ameaças.

- **Maquinas virtuais em movimento** - A habilidade única de se mover maquinas virtuais de um servidor físico para outro, torna muito difícil a auditoria e o monitoramento de segurança. Em vários casos, maquinas virtuais podem ser realocadas em outro servidor físico sem que seja criado um alerta ou uma trilha que possa ser auditada. O cliente de nuvem deve estar atento se o provedor de nuvem possui controles e alertas para gerenciar a movimentação de maquinas virtuais.

4 RECOMENDAÇÕES

Neste capitulo serão feitas recomendações de segurança para as áreas críticas de segurança da computação em nuvem elencados pela Cloud Security Alliance (2011). Esse capitulo consiste em um compilado de recomendações baseadas principalmente nos guias da Cloud Security Alliance de (2010) e (2011).

4.1 GOVERNANÇA CORPORATIVA

Organizações de todos os tipos e tamanhos estão sujeitas a riscos. Uma vez que não se pode tirar a incerteza da equação, todas as atividades de uma organização correm riscos. E uma boa gerência desses riscos pode conferir diversas vantagens competitivas a organização.

A gestão de riscos de toda a organização é um tema bastante abrangente e foge o escopo dessa pesquisa. Aqui serão apresentadas diretrizes de gestão de riscos apenas no que tange a computação em nuvem.

Nesta seção são apresentadas recomendações de segurança feitas pela baseadas nas diretrizes da ISO 31000:2009, ISF e ISACA:

- ✓ Uma parte da redução de custos decorrente da adoção de computação em nuvem deve ser direcionada para o aumento dos controles dos recursos de segurança do provedor, aplicação de controles de segurança e avaliações e auditorias detalhadas, para garantir que as exigências de proteção de dados estão sendo continuamente verificadas.
- ✓ Tanto os clientes quanto os fornecedores de serviços de computação em nuvem devem desenvolver uma governança de segurança da informação robusta, independentemente do serviço ou modelo de implantação adotado. A governança de segurança da informação deve ser uma colaboração entre clientes e fornecedores.
- ✓ As organizações clientes de serviços de computação em nuvem, devem incluir a revisão de determinados processos e estruturas de governança de segurança da informação, bem como de controles de segurança específicos, como parte de seus cuidados na seleção de provedores de serviço de nuvem. Os processos de governança de segurança e as atividades dos fornecedores devem ser avaliados, estes devem ter a capacidade de suportar os processos dos clientes. Os processos de governa do provedor também devem ser avaliados quanto a sua maturidade e coerência com os processos de gestão de segurança da informação.
- ✓ A estrutura e os processos de governança colaborativa entre clientes e fornecedores devem ser tratadas como essenciais, tanto no âmbito da concepção e desenvolvimento de prestação de serviços, como avaliação de risco e de serviços e protocolos de gestão de riscos.
- ✓ O departamento de segurança da organização deve estar envolvido durante o estabelecimento dos SLAs, e obrigações contratuais, para assegurar que os requisitos de segurança são contratualmente aplicáveis.
- ✓ As organizações clientes devem definir métricas e padrões para medir o desempenho e eficácia do gerenciamento de segurança da informação, antes de fazer a migração para a nuvem. Estas organizações devem entender e documentar suas métricas atuais e como elas podem mudar se suas operações forem movidas para a nuvem.
- ✓ Sempre que possível, métricas e padrões de segurança devem ser incluídas em qualquer acordo de nível de serviço, SLAs, e contratos. Estas métricas e padrões devem ser documentadas e ser auditáveis.
- ✓ Com relação ao uso de serviços de nuvem para funções críticas da organização, a abordagem de gerenciamento de riscos deve incluir a identificação e avaliação de ativos, identificação e análise de ameaças e vulnerabilidades e seu potencial impacto nos ativos, análise de

probabilidade de eventos, níveis e critérios de aceitação de gerenciamento de riscos aprovado e o desenvolvimento de planos de tratamento de riscos. Os resultados dos planos de tratamento de riscos devem ser incorporados aos SLAs.

- ✓ O usuário e o provedor juntos devem desenvolver cenários de risco para os serviços em nuvem.
- ✓ O cliente de nuvem deve estar atento quanto a resiliência do negócio do provedor, a portabilidade dos dados e aplicações e a interoperabilidade dos serviços. De forma a não ficar preso a um provedor nem ter seus serviços interrompidos por longos períodos de tempo caso seu provedor deixe o mercado.
- ✓ O Inventario de ativos de informação do cliente de nuvem deve considerar os serviços de suporte de ativos na nuvem e sob controle do provedor.
- ✓ O serviço, e não somente o fornecedor deve ser o alvo de uma avaliação de risco.
- ✓ Quando o provedor não se demonstrar efetivo no processo de gerenciamento de riscos, os clientes devem avaliar com cuidado as habilidades tanto de provedor quanto as suas próprias afim de compensar as possíveis brechas indicadas no gerenciamento de riscos.
- ✓ Clientes de serviços na nuvem devem questionar se sua gestão definiu níveis de tolerância a riscos com relação aos serviços na nuvem e aceita qualquer risco residual inerente à utilização de serviços em nuvem.
- ✓ Os clientes de nuvem devem adotar um modelo de framework de gerenciamento de riscos para avaliar seu gerenciamento de riscos da informação e um modelo de maturidade para avaliar a efetividade do seu modelo de gestão de riscos da informação.
- ✓ Os clientes de nuvem devem estabelecer requisitos contratuais apropriados e controles tecnológicos para coletar dados necessários para informar as decisões sobre os riscos à informação.
- ✓ Os clientes de nuvem devem adotar um processo para determinar a exposição ao risco antes de elencar requisitos para um projeto de computação em nuvem.
- ✓ Quando utilizado SaaS, a maior parte da informação deve ser fornecida pelo provedor do serviço. Organizações clientes devem estruturar processos de coleta de informações analíticas nas obrigações contratuais do serviço SaaS.
- ✓ Quando utilizado o modelo PaaS, as organizações clientes devem definir a coleta de informações como feito no modelo SaaS acima, mas sempre que for possível, considerar a capacidade de implantar e coletar informações de controles, bem como a criação de itens contratuais para testar a efetividade destes controles.
- ✓ Quando utilizado um provedor de serviços sob o modelo IaaS, as organizações clientes devem definir a transparência das informações em nível contratual para que possam ser tratadas pela análise de riscos.
- ✓ Os provedores de serviço em nuvem devem incluir métricas e controles para auxiliar os clientes na implementação dos seus requisitos de gestão de risco da informação.
- ✓ Os clientes de nuvem devem considerar os serviços e a segurança em nuvem como questões de segurança da cadeia de fornecimento. Isso significa examinar e avaliar, a cadeia de suprimentos do provedor, ou seja, o relacionamento do provedor com os seus terceirizados.
- ✓ A avaliação dos fornecedores de serviços terceirizados deve concentrar-se especificamente no gerenciamento do fornecedor, nas políticas de recuperação de desastres e continuidade de negócio, e em processos e procedimentos. Deve-se igualmente, incluir o exame das instalações de *backup* e de suas instalações físicas.
- ✓ O plano de recuperação de desastres e continuidade de negócios do cliente de nuvem deve incluir cenários de perda dos serviços prestados por seu provedor e a perda de serviços terceirizados contratados pelo provedor. A realização dos testes dessa parte do plano deve ser coordenada com o provedor de serviços de nuvem.

- ✓ A regulamentação da governança de segurança de informações, a gestão de riscos e as estruturas e processos do fornecedor devem ser amplamente avaliados:
  - As organizações cliente devem solicitar uma documentação clara sobre como as instalações e os serviços do fornecedor são avaliados quanto aos riscos e auditados a respeito de controles de vulnerabilidades, qual a frequência de tais avaliações, e como as deficiências de controles são devidamente mitigadas.
  - As organizações clientes devem solicitar uma definição do que o fornecedor considera fatores críticos de sucesso de segurança da informação e serviços críticos, indicadores chave de desempenho, e como tais aspectos são mensurados relativamente à gestão de segurança de informações e serviços de TIC.
  - As organizações clientes devem examinar a abrangência dos processos de comunicação, avaliação e domínio dos requisitos legais, regulatórios, industriais e contratuais do provedor.
  - As organizações clientes devem implementar detalhados contratos para determinar papéis, funções e responsabilidades. Estas também devem assegurar que será feito uma validação legal, incluindo uma avaliação do cumprimento das normas contratuais e leis em jurisdições estrangeiras ou fora do estado.
  - As organizações clientes devem determinar se os requisitos contratuais abordam todos os aspectos materiais das relações dos provedores de serviço de nuvem, tais como a situação financeira, a reputação, controles, pessoal estratégico, planos e testes de recuperação de desastres, seguros, capacidades de comunicações e uso de terceirizados do provedor.

4.2 ASPECTOS LEGAIS E *ELETRONIC DISCOVERY*

Esta seção do trabalho endereça recomendações quanto os aspectos legais de adoção da nuvem e também da descoberta digital de evidências, chamada de *Eletronic Discovery*, na nuvem. As recomendações a seguir são apenas diretrizes é altamente recomendado a contratação de consultores jurídicos para um melhor entendimento das leis vigentes na região e no segmento de mercado em que a organização atua.

Recomendações:

- ✓ Clientes e provedores da nuvem devem estar mutuamente cientes dos respectivos papéis e responsabilidades relacionados à *Eletronic Discovery*, incluindo atividades como litígio, investigações, prover o testemunho de perito, etc.
- ✓ Provedores de nuvem são aconselhados a garantir que seus sistemas de segurança da informação atendam às necessidades do cliente para preservar os dados como autênticos e confiáveis, incluindo informações primárias e secundárias, tais como metadados e arquivos de logs.
- ✓ Dados sob a custódia dos provedores de serviços de nuvem devem receber proteção equivalente a que teriam se estivessem nas mãos de seu proprietário original ou custodiante.
- ✓ Clientes que pretendem utilizar serviços de nuvem devem elaborar de um plano para o término esperado ou inesperado da relação contratual com um prestador de serviço.
- ✓ Os clientes devem realizar uma auditoria geral pré-contratual, fazer a negociação dos termos do contrato, monitorar o pós-contrato, a rescisão contratual e a transição da custódia dos dados.
- ✓ O cliente de nuvem deve saber onde o provedor de serviços de nuvem irá hospedar os dados, pois isto é um pré-requisito para implementar as medidas necessárias para garantir conformidade com as leis locais que restringem o fluxo de dados além de determinadas fronteiras geográficas.
- ✓ Como custodiante dos dados pessoais de seus funcionários ou clientes, bem como de outros ativos de propriedade intelectual da instituição, uma empresa que utiliza serviços de

computação em nuvem deve assegurar que ele mantém a posse de seus dados em seu formato original e autêntico.

- ✓ Diversas questões de segurança, tais como suspeitas de violação de dados, devem ser abordadas através de disposições específicas do SLA, que deve esclarecer as respectivas obrigações do provedor de serviços de nuvem e do cliente.
- ✓ O provedor de serviços de nuvem e o cliente devem adotar um processo unificado para responder às intimações e outros requisitos legais.
- ✓ O contrato de serviços de nuvem deve permitir que o cliente ou terceiro designado monitore o desempenho do provedor de serviços e teste as vulnerabilidades no sistema.
- ✓ As partes em um contrato de serviços de nuvem devem assegurar que o acordo preveja a ocorrência de problemas relativos à recuperação dos dados do cliente após o término da relação contratual.
- ✓ O contrato de serviços deve fazer com que o provedor de nuvem notifique a organização cliente em caso de recebimento de uma intimação, e dar um tempo a organização para que essa possa lutar contra o acesso aos dados requisitados na intimação.

4.3 CONFORMIDADE E AUDITORIA

Conformidade e auditoria são os processos internos e externos que tem como objetivo identificar os requerimentos que uma determinada organização tem que cumprir, leis, regulações, contratos com clientes etc. Esses processos também se estendem a implementação e monitoramento de políticas, processos e sistemas que façam que a organização atenda todos os requisitos legais e contratuais que estas se propôs ou que está sujeita devido a regulamentação do setor (MATHER, KUMARASWAMY e LATIF, 2009).

Tendo em vista os problemas e dificuldades levantadas na seção 3.3 a respeito de conformidade e auditoria na nuvem. Esta seção expõe recomendações afim de resolver os problemas e superar as dificuldades encontradas em demonstrar conformidade e executar auditorias na nuvem.

Recomendações:

- ✓ As organizações clientes devem envolver os departamentos jurídicos e de contratos no processo de contratação de um provedor de nuvem. As cláusulas padrão de serviço do provedor de computação em nuvem podem não atender suas necessidades de conformidade e, por isso, é vantajoso ter pessoas das áreas jurídicas e de contratos envolvidas desde o início para garantir que o contrato de prestação de serviços seja adequado para atender as obrigações de conformidade e auditoria.
- ✓ As organizações clientes devem sempre estar atentas as cláusulas que tratam sobre o direito de auditar. Os clientes, frequentemente, terão a necessidade de auditar o provedor de serviços de computação em nuvem, dada a natureza dinâmica dos ambientes regulatório e da computação em nuvem. Uma cláusula sobre o direito de auditar deve ser obtida sempre que possível, particularmente quando se usa um provedor para um serviço onde o cliente tenha que regulamentar o cumprimento das responsabilidades. Ao longo do tempo, a necessidade deste direito deve ser reduzida e em muitos casos substituída por certificações do provedor.
- ✓ As organizações clientes de nuvem devem analisar o escopo de conformidade. E determinar se os regulamentos de conformidade aos quais a organização está sujeita serão impactados pelo uso dos serviços de computação em nuvem para um dado conjunto de aplicações e dados.
- ✓ As organizações clientes de nuvem devem analisar o impacto dos regulamentos sobre a segurança dos dados. Potenciais usuários finais dos serviços de computação em nuvem devem ponderar quais aplicações e dados estão sendo considerados para serem movidos para serviços de computação em nuvem e em que medida eles estão sujeitos aos regulamentos de conformidade.
- ✓ As organizações clientes de nuvem devem revisar os parceiros e provedores de serviços importantes. Esta é a recomendação geral para assegurar que relacionamentos com provedores

de serviços não afetem negativamente a conformidade. Avaliar quais provedores estão processando os dados sujeitos aos regulamentos de conformidade e então avaliar os controles de segurança oferecidos pelos mesmos é fundamental.

- ✓ As organizações clientes de nuvem devem entender as responsabilidades contratuais sobre a proteção de dados e os contratos relacionados. O modelo de serviços de computação em nuvem determina, de uma certa forma, se o cliente ou o provedor de serviços é responsável pela implantação de controles de segurança. Em um cenário de implantação de IaaS, o cliente tem um alto grau de controle e uma maior responsabilidade do que em um cenário de implantação de SaaS. Do ponto de vista do controle de segurança, isto significa que clientes IaaS terão que implantar muitos dos controles para a conformidade regulatório. Em um cenário SaaS, o provedor de serviços de computação em nuvem deve fornecer os controles necessários. De uma perspectiva contratual é importante entender os requisitos específicos e garantir que o contrato de serviços, bem como os SLAs, sejam tratados adequadamente.
- ✓ As organizações clients de nuvem devem analisar o impacto das regulamentações na infraestrutura do provedor. Na área de infraestrutura, mover-se para serviços de computação em nuvem também requer uma análise cuidadosa. Alguns requisitos regulatórios especificam controles que são difíceis ou impossíveis de se atingir em certos tipos de serviços de nuvem.
- ✓ As organizações clientes de nuvem devem analisar o impacto de regulamentações em políticas e procedimentos. Mover dados e aplicações para serviços de computação em nuvem provavelmente causará um impacto em políticas e procedimentos. Os clientes devem avaliar quais políticas e procedimentos relacionados com regulamentações terão de ser alterados. Exemplos de políticas e procedimentos impactados incluem relatórios de atividades, logs, retenção de dados, resposta a incidentes, controles de testes e políticas de privacidade.
- ✓ As organizações clientes de nuvem devem preparar evidências de como cada exigência está sendo cumprida. Clientes dos serviços de computação em nuvem devem desenvolver processos para coletar e armazenar evidências de conformidade, incluindo logs de auditoria e relatórios de atividades, cópias das configurações dos sistemas, relatórios de gestão de mudanças e resultados de outros procedimentos de teste. Dependendo do modelo de serviço o provedor pode precisar fornecer muitas dessas informações.
- ✓ Em muitos casos a organização não tem nenhuma influência na seleção de auditores ou avaliadores de segurança. Se uma organização participa da seleção, é altamente recomendável escolher um auditor que conheça computação em nuvem, uma vez que muitos podem não estar familiarizados com os desafios da virtualização e da computação em nuvem. Questionar sua familiaridade com as nomenclaturas IaaS, PaaS e SaaS é um bom ponto de partida.
- ✓ Provedores que buscam o fornecimento de serviços de missão crítica devem adotar os padrões da ISO/IEC 27001 para sistemas de gerenciamento de segurança da informação. Se o provedor não tiver alcançado a certificação ISO/IEC 27001, ele deve demonstrar alinhamento com as práticas da ISO 27002.

4.4 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DE DADOS

O principal objetivo da segurança da informação é proteger os dados que impulsionam sistemas e aplicações das organizações. No entanto essa é uma tarefa bastante desafiadora quando se fala de nuvem. Uma vez que a nuvem introduz novos riscos e distribui aplicações e sistemas de forma global.

Essa seção endereça recomendações feitas pela a respeito do gerenciamento de informações e segurança dos dados.

Recomendações:

- ✓ Os clientes de nuvem devem entender arquitetura de armazenamento em nuvem em uso, o que irá auxiliar a determinar quais são os riscos de segurança e potenciais controles.
- ✓ Os clientes de nuvem devem escolher armazenamento com dispersão dos dados quando possível.

- ✓ Os clientes de nuvem devem usar a segurança de ciclo de vida dos dados para identificar falhas na segurança e determinar quais são os principais controles que devem ser empregados.
- ✓ Os clientes de nuvem devem monitorar as principais bases de dados e repositórios de arquivos com DAM[5] e FAM[6] para identificar grande migrações de dados, o que pode indicar uma migração para nuvem. Dessa forma proteger as migrações.
- ✓ Os clientes de nuvem devem monitorar o acesso à internet de empregados com filtros de URL[7] e ferramentas de DLP[8] para identificar informações sensíveis que possam estar sendo movidas para a nuvem. Selecione ferramentas que incluam categorias pré-definidas para serviços de nuvem. As organizações ainda devem considerar o uso de filtros que coíbam atividades indesejadas.
- ✓ Os clientes de nuvem devem entender como criptografia é gerenciada, em ambientes onde há a multilocação. Os clientes de nuvem devem saber se existe uma única chave para todos os clientes, uma chave por cliente, ou múltiplas chaves por cliente.
- ✓ Os clientes de nuvem devem usar a descoberta de conteúdo para vasculhar o armazenamento na nuvem e identificar dados sensíveis que possam estar expostos.
- ✓ Os clientes de nuvem, quando estiverem usando serviços do tipo IaaS, devem criptografar volumes de armazenamento que contém informações sensíveis afim de limitar a exposição que pode vir a ocorrer devido a acesso não autorizado a esses volumes.
- ✓ Os clientes de nuvem devem criptografar dados que estão armazenados em *object storages*.
- ✓ Os clientes de nuvem devem criptografar dados sensíveis em aplicações e base de dados PaaS. A criptografia em nível de aplicação é recomendada.
- ✓ Se criptografia é necessária para serviços do tipo SaaS, os clientes de nuvem devem buscar provedores que ofereçam criptografia nativa. Uso criptografia de proxy se a criptografia nativa nos provedores não está disponível ou se níveis extras de segurança precisam ser garantidos.
- ✓ Os clientes de nuvem devem monitorar base dados sensíveis com DAM e gerar alertas quando políticas de segurança forem violadas.
- ✓ Os clientes de nuvem devem considerar o armazenamento que preserve a privacidade quando o acesso ou a infraestrutura se está ofertando pode revelar informações sensíveis do usuário.
- ✓ A remoção de dados de um provedor de nuvem deve ser detalhada no SLA. E deve cobrir a deleção de usuários, a migração ou exclusão dos dados, transferência de chaves etc.
- ✓ Os clientes de nuvem devem usar DLP para identificar o vazamento de informações sensíveis. Normalmente esse tipo de ferramenta só é disponível em ofertas de IaaS e nem todos os provedores de nuvem publicas o oferecem. Deve-se buscar por aqueles quem oferecem o DLP como ferramenta.
- ✓ Os clientes de nuvem devem entender como a integridade é mantida e como o comprometimento da integridade é detectado e informado aos clientes. A mesma recomendação aplica-se à confidencialidade quando apropriado.
- ✓ O provedor de serviço de nuvem deverá assegurar ao proprietário dos dados que eles proveem divulgação de todas as suas informações, ou seja completa transparência, relativas às práticas e procedimentos de segurança de acordo com o estabelecido em seus SLAs.
- ✓ Os clientes de nuvem devem garantir a identificação específica de todos os controles usados durante o ciclo de vida dos dados.

---

[5] DAM – Data Activity Monitoring

[6] FAM – File Activity Monitoring

[7] URL – Universal Resource Locator

[8] DLP – Data Loss Prevention

- ✓ Os clientes de nuvem devem garantir as especificações de qual entidade é responsável por cada controle entre o proprietário dos dados e o provedor de serviços de nuvem.
- ✓ Os clientes de nuvem devem manter uma filosofia fundamentada no conhecimento de onde seus dados estão. E também devem assegurar sua habilidade de conhecimento sobre a localização geográfica de armazenamento. Deve se estipular estes pontos nos SLAs e contratos.
- ✓ Os clientes de nuvem devem entender as circunstâncias nas quais o os dados armazenados em um provedor de nuvem podem ser apreendidos por um terceiro ou entidade governamental. É importante que os clientes de nuvem verifiquem seus SLAs com o provedor de serviço de nuvem de forma incluir, caso não esteja definido em contrato, processo de notificação prévia ao proprietário dos dados que as informações do proprietário dos dados serão apreendidas.
- ✓ Em alguns casos, uma intimação de e-discovery pode ser interposta contra o provedor de serviços de computação em nuvem. Neste caso, quando o provedor possuir custódia dos dados do cliente, o provedor de serviços de computação em nuvem deverá ser forçado a informar ao proprietário dos dados sobre essa divulgação.
- ✓ Os clientes de nuvem devem identificar limites de confiança da arquitetura de TIC e suas camadas de abstração. Possibilite aos subsistemas somente transpor os limites de confiança quando necessário e com apropriadas contramedidas para prevenir divulgação não autorizada, alteração ou destruição de dados.
- ✓ Os clientes de nuvem devem entender quais técnicas de compartimentalização são aplicadas por um provedor para isolar seus clientes uns dos outros. Um provedor poderá utilizar uma variedade de métodos dependendo dos tipos e quantidade de serviços oferecidos.
- ✓ Os clientes de nuvem devem entender as capacidades e limitações de busca de dados do provedor de serviço de nuvem quando tentar visualizar “dentro” da série de dados para descoberta de dados.
- ✓ Os proprietários de dados deverão exigir que os provedores de serviço de computação em nuvem garantam que seus dados de cópias de segurança não estejam misturados com os dados de outro cliente de serviço de nuvem.
- ✓ Os clientes de nuvem devem entender o processo de descarte de dados armazenados pelo provedor de serviço de nuvem.
- ✓ Os clientes de nuvem devem entender a segregação lógica de informação e os controles de proteção implementados.
- ✓ Os clientes de nuvem devem entender as restrições de privacidade inerentes aos dados confiados a sua companhia.
- ✓ Os clientes de nuvem devem entender as políticas e processos do provedor de serviço de nuvem para retenção e destruição de dados e como eles se comparam à sua política organizacional interna. Os clientes ainda devem estar cientes que garantir a retenção de dados pode ser mais fácil para o provedor de serviço de nuvem demonstrar, enquanto para destruição de dados pode ser muito difícil.
- ✓ Os clientes de nuvem devem negociar penalidades pagas pelo provedor de serviço de nuvem no caso de uma violação dos dados. Se viável, clientes deverão buscar ressarcimento de todos os custos por violações como parte de seus contratos com provedor. Se inviável, clientes deverão explorar outros meios de transferência de risco tais como seguro para recuperação de perdas por violação.
- ✓ Os clientes de nuvem devem Executar testes regulares de backup e recuperação para assegurar que a segregação lógica e os controles são efetivos.

4.5 PORTABILIDADE E INTEROPERABILIDADE

Portabilidade e interoperabilidade não são características essenciais da nuvem porém são duas caraterísticas que todo cliente deve buscar ao se adotar um serviço de computação em nuvem. Pois essas proporcionam a empresa em sempre buscar provedores que melhor atendam às suas necessidades e até

distribuir aplicações e serviços em múltiplos provedores garantindo assim maior resiliência e disponibilidade a seus serviços e aplicações.

Existem recomendações que se aplicam a todos os modelos de serviço de nuvem, contudo existem particularidades de cada modelo de serviço que requerem cuidados diferentes.

Recomendações:

4.5.1 PARA TODAS AS SOLUÇÕES

- ✓ Os SLAs podem variar de provedor para provedor é importante estar ciente de como o SLA pode afetar a habilidade de trocar de provedores.
- ✓ O uso padrões para autenticação e identidade como o SAML ajudam a garantir a portabilidade.
- ✓ As chaves criptográficas devem ser mantidas localmente sempre que possível.
- ✓ Os clientes, quando estiverem migrando dados de um provedor para o outro, devem se assegurar que as copias dos metadados dos arquivos foram removidas do antigo provedor para que estas não gerem uma possível oportunidade de revelar informações indesejadas.
- ✓ A substituição do provedor de serviços de nuvem é, em praticamente todos os casos, uma transação de negócios negativa para pelo menos uma das partes, o que pode causar uma reação inesperada do antigo provedor da nuvem. Isto deve ser planejado no processo de contratação, no seu plano de continuidade de negócios, e como parte da governança global da organização.
- ✓ Os clientes de nuvem devem entender o tamanho dos conjuntos de dados hospedados em um provedor de nuvem. O tamanho dos dados pode causar uma interrupção do serviço durante a transição, ou um período de transição maior do que o previsto.
- ✓ Os clientes de nuvem devem documentar a arquitetura de segurança e a configuração individual de cada componente de controle de segurança, de forma que eles possam ser utilizados para ajudar nas auditorias internas, bem como para facilitar a migração para novos provedores.

4.5.2 PARA SOLUÇÕES EM NUVEM IaaS

- ✓ Os clientes de nuvem devem entender como imagens de máquinas virtuais podem ser capturadas e portadas para o novo provedor de nuvem que pode utilizar uma tecnologia diferente de virtualização.
- ✓ Os clientes de nuvem devem identificar e eliminar todas as extensões específicas do provedor no ambiente de máquina virtual.
- ✓ Se não for possível eliminar extensões proprietárias, os clientes de nuvem devem documentar todas essas extensões não proprietárias.
- ✓ Os clientes de nuvem devem entender quais práticas são utilizadas para garantir uma desalocação apropriada das imagens de maquinas virtuais depois que uma aplicação é portada de um provedor de nuvem.
- ✓ Os clientes de nuvem devem compreender as práticas utilizadas na desmontagem dos discos e dispositivos de armazenamento.
- ✓ Os clientes de nuvem devem identificar e entender as dependências de hardware ou plataforma antes de migra aplicação ou dados.
- ✓ Os clientes de nuvem devem solicitar acesso a logs do sistema, rastros e registros de acesso e de faturamento do provedor de nuvem.
- ✓ Os clientes de nuvem devem identificar opções para continuar ou expandir o serviço com o provedor de nuvem antigo, em parte ou no todo, caso o novo provedor de serviços demonstre ser inferior.
- ✓ Os clientes de nuvem devem determinar se existem quaisquer funções de nível gerencial, interfaces ou APIs utilizadas que são incompatíveis ou não implantadas no novo provedor.

- ✓ Os clientes de nuvem devem entender quais são custos envolvidos em mover dados para fora e para dentro de um provedor de serviços de nuvem.
- ✓ Os clientes de nuvem devem determinar quais meios são os mais eficientes para se mover dados para nuvem.

4.5.3 PARA SOLUÇÕES EM NUVEM PaaS

- ✓ Quando possível, os clientes de nuvem devem utilizar componentes de uma plataforma com sintaxes padronizadas, APIs abertas e normas abertas.
- ✓ Os clientes de nuvem devem entender quais ferramentas estão disponíveis para a transmissão segura dos dados, para backup e para restauração.
- ✓ Os clientes de nuvem devem entender e documentar os componentes da aplicação e módulos específicos para o provedor de PaaS e desenvolver a arquitetura de uma aplicação com camadas de abstração para minimizar o acesso direto aos módulos proprietários.
- ✓ Os clientes de nuvem devem compreender como serviços de monitoramento, logs e auditoria podem ser transferidos para o novo provedor.
- ✓ Os clientes de nuvem devem entender quais proteções são providas para os dados na nuvem.
- ✓ Os clientes de nuvem devem entender as funções de controle fornecidas pelo provedor de nuvem antigo e como será feita a transferência para o novo provedor.
- ✓ Os clientes de nuvem, quando migrarem para uma nova plataforma, devem conhecer os impactos no desempenho e na disponibilidade da aplicação e como estes impactos são calculados.
- ✓ Os clientes de nuvem devem fazer antes e depois da migração, para verificar se os serviços ou aplicações estão operando corretamente. Os clientes também devem estar cientes que a responsabilidade de testar é de ambos, provedor e usuário e que as responsabilidades de cada um são bem conhecidas e documentadas.

4.5.4 PARA SOLUÇÕES EM NUVEM SaaS

- ✓ Os clientes de nuvem devem executar extrações de dados e backups regularmente para formatos que possam ser utilizados fora do provedor de SaaS.
- ✓ Os clientes de nuvem devem entender quando os metadados podem ser preservados e migrados.
- ✓ Os clientes de nuvem devem compreender se todas as ferramentas personalizadas terão que ser recodificadas ou se o novo provedor fornecerá novas ferramentas.
- ✓ Os clientes de nuvem devem assegurar a consistência eficaz dos controles entre o antigo e o novo provedor.
- ✓ Os clientes de nuvem devem assegurar a possibilidade de migração de backups e outras cópias de logs, registros de acesso e qualquer outra informação pertinente que possa ser necessária por razões legais e conformidade.
- ✓ Os clientes de nuvem devem entender o gerenciamento, o monitoramento e as interfaces de relatórios e suas integrações entre os ambientes.
- ✓ Os clientes de nuvem devem verificar se há uma disposição do novo provedor de testar e avaliar a aplicação antes da migração.
- ✓ Os clientes de nuvem devem testar e avaliar todas aplicações antes de migra-las. Os devem ser feitos mais de uma vez quando possível para garantir que a aplicação está funcionando corretamente no novo provedor.

4.5.5 PARA SOLUÇÕES EM NUVEM PRIVADA

- ✓ Os clientes de nuvem devem assegurar a interoperabilidade entre *hypervisors* comuns como KVM, VMware e Xen[9].
- ✓ Os clientes de nuvem devem assegurar-se de que APIs padrões estão sendo usadas para funções de gerencia como gerencia de usuários e privilégios, gestão de imagens de maquinas virtuais, gerencia de maquinas virtuais, gestão de redes virtuais etc.

4.5.6 PARA SOLUÇÕES EM NUVEM PÚBLICA

- ✓ Os clientes de nuvem devem assegurar que o provedor de nuvem exponha interfaces comuns ou padrões para acessar todas as funções de nuvem nos serviços ofertados.

4.5.7 PARA SOLUÇÕES EM NUVEM HIBRIDA

- ✓ Os clientes de nuvem devem assegurar que o provedor de nuvem exponha interfaces comuns ou padrões para acessar todas as funções de nuvem nos serviços ofertados.
- ✓ Os clientes de nuvem devem assegurar-se da habilidade de federação com provedores de nuvem diferentes para possibilitar maiores níveis de escalabilidade.

4.6 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

É muito importante conhecer os mecanismos de segurança tradicional, planos de continuidade de negócios e recuperação de desastres do provedor de nuvem do qual se pretende contratar serviços de nuvem. Segurança tradicional aqui consiste em segurança física e do ambiente, tratada na seção 9 da ISO 27002. Então essa seção endereça recomendações da ISO 27002 que podem ser aplicadas também em ambientes de nuvem.

Recomendações:

- ✓ Os clientes de nuvem devem ter em mente que a centralização dos dados significa que o risco de fraude interna partindo de dentro do provedor de serviços de nuvem é uma preocupação significativa.
- ✓ Provedores de serviço de nuvem devem considerar adotar como padrão de segurança os requisitos mais rigorosos dos clientes.
- ✓ Os provedores devem ter uma segregação robusta das responsabilidades das funções, verificar os antecedentes dos funcionários, exigir / aplicar acordos de não-divulgação de dados para os seus funcionários e limitar o acesso às informações dos clientes aos funcionários na medida do que for absolutamente necessário para a execução de suas funções.
- ✓ Os clientes devem efetuar inspeções aos locais das instalações de seu provedor de nuvem sempre que possível. Preferencialmente te forma não anunciada.
- ✓ Os clientes devem inspecionar os planos de recuperação de desastres e de continuidade de negócios de seus provedores de nuvem.
- ✓ Os clientes devem identificar as interdependências físicas na infraestrutura do provedor.
- ✓ Os clientes de nuvem devem Garantir que há um detalhamento formal estabelecido no contrato para definir claramente as obrigações contratuais relacionadas com segurança, recuperação e acesso aos dados.

[9] Ferramentas populares de virtualização.

- ✓ Clientes devem solicitar a documentação dos controles de segurança internos e externos do provedor e a adesão aos padrões da indústria.
- ✓ Os clientes de nuvem devem assegurar-se de que os objetivos de tempo de recuperação do cliente são totalmente compreendidos e definidos nas relações contratuais e baseados no processo de planejamento tecnológico. Os clientes ainda devem se certificar de que os roteiros, políticas e capacidades operacionais satisfaçam estes requisitos.
- ✓ Clientes precisam confirmar que o provedor tem uma política de plano de continuidade de negócios aprovada pelo conselho de administração do provedor.
- ✓ Clientes devem procurar evidências de apoio efetivo da gestão e revisão periódica do programa de continuidade de negócios para garantir que este esteja ativo.
- ✓ Clientes devem verificar se o programa de continuidade de negócios é certificado com normas internacionalmente reconhecidas como a BS 25999[10].
- ✓ Clientes devem verificar se o provedor tem algum recurso on-line dedicado à segurança e plano de continuidade de negócio, onde a visão geral do programa e as fichas técnicas estejam disponíveis para consulta.
- ✓ Provedores de IaaS devem ter acordos com outros provedores de IaaS e ter já ter ferramentas prontas para caso haja alguma falha em sua infraestrutura esse possa recuperar os serviços rapidamente.
- ✓ Os clientes de nuvem devem revisar todas essas recomendações regularmente, pois, a natureza dinâmica da computação em nuvem e sua relativa juventude requerem ciclos mais frequentes de todas as atividades endereçadas nessa seção para a descoberta de mudanças não comunicadas aos clientes.

4.7 OPERAÇÕES E *DATACENTER*

Essa seção endereça recomendações quanto a segurança da informação que usuários de nuvem podem tomar como base na hora de avaliar a segurança dos *data centers* dos provedores.

Recomendações:

- ✓ Quaisquer que sejam as certificações que os provedores de nuvem mantêm, é importante obter o compromisso e a permissão de conduzir auditorias feitas pelo cliente ou por terceiros.
- ✓ Os clientes de serviços de nuvem devem compreender como os provedores implementam as características essenciais da nuvem.
- ✓ Ainda que as arquiteturas tecnológicas dos provedores de nuvem variem, todos eles devem poder demonstrar divisão compreensiva de sistemas, redes, gerenciamento, provisão e pessoal.
- ✓ Os clientes de nuvem devem compreender como a democratização de recursos ocorre dentro da nuvem de seu provedor para prever melhor a disponibilidade e desempenho do sistema durante suas flutuações de negócios. Se possível, descubra os outros clientes do provedor de nuvem para avaliar o impacto que as flutuações de negócios deles podem ter sobre a sua vivência como cliente do provedor de nuvem. Contudo, isso não substitui a garantia de que os acordos acerca do nível de serviço estejam claramente definidos, mensuráveis, executáveis e adequados para a sua necessidade.
- ✓ Os clientes dos serviços de nuvem devem entender as políticas e procedimentos de correção do provedor e como eles podem influenciar os seus ambientes. Essa compreensão deve estar refletida no contrato.
- ✓ A contínua melhoria é particularmente importante em um ambiente de nuvem, pois qualquer melhoria nas políticas, processos e procedimentos, ou ferramentas para um cliente determinado

[10] Padrão de gestão de continuidade de negócios.

podem resultar em melhoria do serviço para todos os clientes. Procure por provedores de nuvem com processos de melhoria contínua.

- ✓ Organizações que estão construindo data centers de nuvem devem incorporar processo, práticas e softwares para entender e reagir as tecnologias rodando dentro de seus *data centers*.
- ✓ A localização dos data centers é importante. Se aplicações são distribuídas através muitos data centers um acréscimo de latência.
- ✓ Os clientes de nuvem devem entender e documentar quem é responsável por atender os requisitos de conformidade, cliente ou provedor. Também devem entender o papel de seus provedores quando avaliando conformidade.

4.8 RESPOSTA A INICIDENTE, NOTIFICAÇÃO E REMEDIAÇÃO

Resposta a incidentes é um dos principais elementos de um plano de segurança uma vez que nem o melhor planejamento de segurança possível consegue eliminar totalmente a ocorrência de alguma falha. Portanto a necessidade de se saber o que fazer quando um incidente ocorre.

Então nessa seção são endereçadas as recomendações a respeito da Resposta a incidentes em um ambiente de nuvem.

Recomendações:

- ✓ Clientes de computação em nuvem precisam definir claramente e comunicar aos provedores o que eles consideram incidentes e o que consideram meros eventos antes de implementar o serviço.
- ✓ Clientes de computação em nuvem podem vir a ter um envolvimento limitado com as atividades de resposta a incidente do provedor. Portanto, é crucial para os clientes entender os canais de comunicação predefinidos para contatar a equipe de resposta a incidentes.
- ✓ Clientes de computação em nuvem devem investigar quais ferramentas de detecção e analise de incidentes o provedor utiliza para garantir que eles sejam compatíveis com seus próprios sistemas. Um formato de log proprietário ou incomum poderia ser um grande problema em investigações conjuntas, particularmente aqueles que envolvam questões legais ou intervenção governamental.
- ✓ Sistemas e aplicações desenvolvidas com baixo nível de segurança podem facilmente sobrecarregar qualquer capacidade de resposta a incidente. A condução de uma avaliação de riscos adequada nos sistemas e a utilização da prática de segurança em camadas são essenciais para reduzir as chances de um incidente de segurança.
- ✓ Centros de operações de segurança normalmente assumem um modelo único de governança relacionado à resposta a incidente, o qual não é apropriado para provedores multilocatários de nuvem. Um processo robusto e definido de gestão de eventos e informações de segurança – SIEM (do inglês Security Information and Event Management), que identifica as fontes disponíveis de informação como logs de aplicações, logs de firewalls e etc. E as combina com uma plataforma comum de análise e notificação, pode ajudar consideravelmente o centro de operações de segurança na detecção de incidentes dentro da plataforma de computação em nuvem.
- ✓ Qualquer dado classificado como privado para efeito regulatório em relação a roubo de informações deve ser sempre criptografado para reduzir as consequências de um incidente de roubo de dado.
- ✓ Alguns provedores de computação em nuvem podem hospedar um número significativo de clientes com aplicações únicas. Esses provedores de computação em nuvem devem considerar estruturas de registros de camada de aplicação com o intuito de rastrear incidentes a um cliente

em especifico. Esses provedores de computação em nuvem devem também criar um registro de proprietários das aplicações por interface de aplicação (URL, serviços de SOA[11], etc.).

4.9 SEGURANÇA DE APLICAÇÕES

Segurança de aplicações é algo baste desafiador em um ambiente de nuvem uma vez que a nuvem introduz novas ameaças. Na nuvem o ideal é implementar todo os controles de segurança na aplicação como se estivesse em um ambiente totalmente desconfiável. De forma que se um determinado controle de segurança, por exemplo criptografia, não for oferecido por uma camada inferior a aplicação já supriu essa deficiência. Então nessa seção são endereçadas recomendações de segurança para aplicações.

Recomendações.

- ✓ Uma análise de riscos da aplicação para segurança e privacidade de ser feita e mantida pela organização.
- ✓ Riscos relativos ao modelo de serviço e implementação devem ser analisados.
- ✓ Vetores de ataque e analise de impacto especificas de arquiteturas de nuvem devem ser catalogadas e mantidas.
- ✓ Frameworks de arquiteturas seguras de software devem ser desenvolvidas.
- ✓ Os clientes de nuvem devem categorizar as vulnerabilidades baseadas em sua criticidade e tenha um processo para sua remediação.
- ✓ Para aplicações sendo migradas para ambientes de IaaS ou PaaS avaliações devem ser feitas para assegurar que os controles de segurança de nível mais baixo como a segregação de maquinas virtuais foi feita e não representam problemas de segurança para a aplicação.
- ✓ A segurança no ciclo de vida de desenvolvimento de software é importante e deve abordar em alto nível estas principais áreas de diferenciação com desenvolvimento baseado em nuvem: ameaças atualizadas e modelos de confiança, ferramentas de avaliação de aplicações para ambientes de nuvem, processos de segurança no ciclo de vida de desenvolvimento de software e checkpoints de qualidade para contabilizar mudanças arquiteturais de segurança de aplicações.
- ✓ Os modelos de serviço IaaS, PaaS e SaaS criam diferentes limites de confiança para o ciclo de vida de desenvolvimento de software. E essas diferenças devem ser levadas em conta durante o desenvolvimento, teste e implantação das aplicações.
- ✓ Para IaaS, um fator crítico de sucesso é a presença de imagens de máquinas virtuais confiáveis. A melhor alternativa é a organização utilizar suas próprias imagens de maquinas virtuais já de acordo com suas políticas internas políticas internas e requisitos de conformidade.
- ✓ As melhores práticas disponíveis para fortificar sistemas host dentro de DMZs (do inglês DeMilitarized Zone) devem ser aplicadas para máquinas virtuais.
- ✓ A proteção da comunicação entre servidores deve ser uma regra. Não deve se assumir nenhum canal seguro entre servidores mesmo que este estejam em uma mesma máquina fisica.
- ✓ Cuidado adicional deve ser tomado no gerenciamento de arquivos usados para os log e depuração das aplicações.
- ✓ Métricas precisam ser aplicadas para avaliar a eficácia de programas de segurança de aplicação. Entre as métricas diretas específicas de segurança disponíveis estão escores de vulnerabilidade e cobertura de correções. Essas métricas podem indicar a qualidade da codificação de aplicação. Métricas de manipulação indireta de dados tais como o percentual de dados cifrados, podem indicar que decisões responsáveis estão sendo tomadas a partir de uma perspectiva de arquitetura da aplicação.

[11] Service-Oriented Architecture.

- ✓ Provedores de nuvem devem suportar ferramentas de segurança de análise dinâmica para aplicações web às aplicações hospedadas em seus ambientes.
- ✓ Clientes devem obter permissão contratual para realizar avaliações de vulnerabilidades remotas. Muitos provedores de nuvem restringem avaliações de vulnerabilidades devido à incapacidade do provedor de distinguir tais testes de ataques reais e para evitar potenciais impactos sobre outros clientes.
- ✓ Criptografia deve ser empregada sempre que se tratar de dados sensíveis.

4.10 CRIPTOGRAFIA E GERÊNCIA DE CHAVES

A criptografia é uma das principais ferramentas para garantir a confidencialidade dos dados. E na nuvem isso não é diferente. Informações sensíveis devem ser sempre criptografadas além disso um cuidado especial deve ser tomado quanto a gerência das chaves utilizadas na criptografia. Portanto abaixo são elencadas recomendações quanto a criptografia e gerencia de chaves:

- ✓ Use as melhores práticas de gerenciamento de chaves sempre que estiver qualquer forma de criptografia.
- ✓ Use tecnologia de prateleira sempre que possível para obter as melhores práticas de fontes confiáveis.
- ✓ É altamente recomendado que a organização mantenham suas próprias chaves. Caso essa não possua maturidade necessária, ela deve utilizar o serviço de gerência de chaves de uma fonte confiável.
- ✓ Use algoritmos criptográficos de confiabilidade comprovada.
- ✓ Evite padrões antigos e comprovadamente inseguros de criptografia como o DES.
- ✓ Restrinja o acesso indevido a mesmo a informações criptografadas.
- ✓ Quando se estiver criptografando base de dados, não criptografe colunas de indexação em base de dados. Pois fazer isso pode resultar consultas bastante lentas.
- ✓ Utilize criptografia para separar a posse dos dados do uso dos dados.
- ✓ Segregue o gerenciamento de chaves do provedor de nuvem que hospeda os dados, criando uma cadeia de separação. Isso protege tanto o provedor quanto o cliente de nuvem de conflitos quando houver obrigação de fornecer dados devido a um mandato legal.
- ✓ Nos casos onde o provedor de nuvem deve efetuar o gerenciamento de chaves, os clientes devem saber se o provedor possui processos definidos para um ciclo de vida do gerenciamento de chaves: como as chaves são geradas, utilizadas, armazenadas, submetidas a backup, recuperadas e apagadas. Além disso, os clientes devem tomar conhecimento se a mesma chave é utilizada para todos os clientes ou se cada cliente tem seu próprio conjunto de chaves.
- ✓ Os clientes de nuvem devem se assegurar de que dados regulamentados ou sensíveis de clientes sejam criptografados quando estiverem em trânsito através da rede interna do provedor de nuvem, além de serem criptografados quando estiverem em repouso. A responsabilidade de implementar tal recomendação é do cliente de nuvem em ambientes IaaS, de ambos, provedor e cliente, em ambientes PaaS e do provedor de nuvem em ambientes SaaS.
- ✓ Em ambientes IaaS, os clientes de nuvem devem saber como as informações sensíveis quando não protegidos por criptografia tradicional podem ser expostas durante seu uso. Por exemplo, arquivos de swap de máquinas virtuais e outros locais temporários de armazenamento de dados podem também necessitar ser criptografados.

4.11 GERENCIAMENTO DE IDENTIDADE E ACESSO

O gerenciamento de acesso e identidade na nuvem é um ponto muito importante, pois em implementações de nuvem públicas e comunitárias os clientes de nuvem, geralmente, perdem o controle físico dos dados e muitas vezes suprem essa deficiência com um forte gerenciamento de acesso e

identidade. Então nessa seção são apresentadas recomendações para se implementar um bom gerenciamento de acesso e identidade para serviços de nuvem.

4.11.1 PROVISIONAMENTO DE IDENTIDADE

- ✓ As capacidades oferecidas pelos provedores de nuvem atualmente não são adequadas às exigências das empresas. Os clientes devem evitar soluções proprietárias assim como criar conectores personalizados unicamente para os provedores de nuvem, já que isto aumenta a complexidade do gerenciamento.
- ✓ Os clientes devem usar conectores padrão fornecidos pelos provedores de nuvem como uma medida prática, preferencialmente construídos no esquema SPML. Se seu provedor de nuvem não oferece SPML, o cliente deve solicitá-lo.
- ✓ Os clientes de nuvem devem modificar seus repositórios de identidade de que suportem as aplicações e processos na nuvem.

4.11.2 AUTENTICAÇÃO

4.11.2.1 OPÇÕES DO CLIENTE DE NUVEM

- ✓ Os clientes de nuvem devem considerar autenticar seus usuários através de Provedores de Identidade (PId) e estabelecer conexão com o provedor de nuvem através do uso de federação de acesso.
- ✓ Os clientes de nuvem devem considerar usar autenticação centrada em usuário como do Google, Yahoo, OpenID, Live ID, etc., para permitir o uso de um conjunto único de credenciais válido para múltiplos sites.
- ✓ Qualquer provedor de SaaS que requeira métodos proprietários para delegar a autenticação (ex. manipulação de confiança por meio de um cookie criptografado compartilhado ou outros meios) deve ser evitado. A preferência geral deve ser para o uso de padrões abertos.
- ✓ Para o clientes de nuvem que tem boa expertise em TIC, estabelecer uma VPN[12] dedicada é boa opção, uma vez que pode-se aproveitar sistemas e processos já existentes.
- ✓ Algumas possíveis soluções incluem a criação de um túnel da VPN dedicado para a rede corporativa ou da federação. Um túnel da VPN dedicado funciona melhor quando a aplicação usa os sistemas existentes de gerenciamento de identidade (como uma solução de autenticação baseada em SSO[13] ou LDAP[14] que fornece uma fonte autorizada de dados de identidade).
- ✓ Em casos onde um túnel VPN dedicado não é factível, as aplicações devem ser desenhadas para aceitar os pedidos de autenticação em vários formatos (SAML[15], Federação-WS, etc.), combinadas com criptografia padrão de rede como SSL[16]. Esta abordagem permite às organizações implantar SSO federados não apenas dentro da empresa, mas também para aplicações na nuvem.
- ✓ OpenID é outra opção quando a aplicação é direcionada para além dos usuários corporativos. Contudo, pelo fato do controle das credenciais do OpenID estar fora da empresa, os privilégios de acesso fornecido a estes usuários deve ser limitado.

---

[12] VPN – *Virtual Private Network*

[13] SSO – *Single Sign-On*

[14] LDAP - *Lightweight Directory Access Protocol*

[15] SAML - Security Assertion Markup Language

[16] SSL – Secure Sockets Layer

- ✓ Qualquer serviço local de autenticação implementado pelo provedor de serviços de nuvem deve estar em conformidade com o OAuth. Utilizando uma solução com suporte a OAuth as empresas podem evitar ficar presas a credenciais de autenticação fornecidas por um fabricante.
- ✓ Para permitir a autenticação forte as aplicações de nuvem devem suportar a característica de delegar a autenticação para a empresa que está consumindo os serviços através de protocolos como o SAML.
- ✓ Os provedores de nuvem devem considerar o suporte a várias opções de autenticação forte, tais como senhas de um único uso, biometria, certificados digitais e Kerberos. Isto oferecerá outra opção às empresas de usar sua infraestrutura existente.

4.11.3 RECOMENDAÇÕES DE FEDERAÇÃO

- ✓ Em um ambiente de computação em nuvem, a federação de identidade é chave para permitir a empresas aliadas se autenticar, prover Login Único – SSO (do inglês Single-Sign-On) e trocar atributos de identidade entre o provedor de serviços e o provedor de Identidade. As organizações, ao considerar o gerenciamento de identidades federadas na nuvem devem entender os vários desafios e possíveis soluções relacionadas ao gerenciamento do ciclo de vida da identidade, métodos de autenticação, formatos de token e não-repúdio.
- ✓ As empresas que buscam por um provedor de nuvem devem verificar se o provedor suporta ao menos um dos padrões proeminentes. O SAML está despontando como um padrão de federação amplamente suportado e é utilizado pelos principais provedores de SaaS e PaaS. O suporte a múltiplos padrões permite um alto grau de flexibilidade.
- ✓ Os provedores de nuvem devem ter flexibilidade para aceitar os formatos padrão de federação de diferentes provedores de identidade.

4.11.4 RECOMENDAÇÕES DE CONTROLE DE ACESSO

Ao selecionar ou revisar a adequação das soluções de controle de acesso para serviços de nuvem existem muitos aspectos que implicam considerar o seguinte:

- ✓ Os clientes de nuvem devem revisar a adequação do modelo de controle de acesso para o tipo de serviço ou dados.
- ✓ Os clientes de nuvem devem avaliar o suporte às políticas de privacidade necessárias para os dados.
- ✓ Os clientes de nuvem devem selecionar um formato no qual especificará a política e a informação do usuário.
- ✓ Os clientes de nuvem devem registrar as informações necessárias para auditorias.

4.12 VIRTUALIZAÇÃO

A virtualização embora não seja um característica essencial da nuvem é amplamente utilizada por provedores de nuvem. E com a utilização da mesma há a introdução de diversos novos riscos. E essa seção tem como objetivo elencar recomendações de segurança para mitigar esses riscos.

Recomendações:

- ✓ Clientes de nuvem devem identificar quais tipos de virtualização seu provedor de nuvem usa, se houver.
- ✓ Sistemas operacionais virtualizados devem ser protegidos por tecnologia de terceiros para fornecer controles de segurança em camadas e reduzir a dependência unicamente sobre o provedor de plataforma.

- ✓ Os clientes devem compreender quais controles de segurança estão implementados em suas máquinas virtuais além de entenderem como é feito o isolamento incorporado do hypervisor – tais como detecção de intrusões, antivírus, escaneamento de vulnerabilidades, etc.
- ✓ Configurações seguras de maquinais de virtuais, que sigam ou excedam os padrões definidos pelas melhores práticas devem ser implementadas nas maquinais virtuais para evitar problemas de instant-on gaps.
- ✓ Os cliente de nuvem devem compreender quais controles de segurança estão implementados externamente às máquinas virtuais para proteger interfaces administrativas expostas para eles.
- ✓ Os clientes de nuvem devem validar a procedência e integridade de qualquer máquina virtual ou modelo originado do provedor de nuvem antes de utilizá-la.
- ✓ Mecanismos de segurança específicos de máquinas virtuais embarcados dentro das APIs do hypervisor devem ser utilizados para prover monitoração granular do tráfego trocado entre as maquinas virtuais no plano de fundo, que é invisível aos controles tradicionais de segurança de rede.
- ✓ Acesso administrativo e controle de sistemas operacionais virtualizados são cruciais e devem incluir uma forte autenticação integrada ao gerenciamento de identidade, assim como mecanismos de registro à prova de falsificação e ferramentas de monitoramento de integridade.
- ✓ Os cliente de nuvem devem considerar a eficácia e viabilidade de segregar máquinas virtuais criando zonas de segurança por tipo de uso, etapas de produção e sensibilidade dos dados em componentes físicos de hardware separados como servidores, armazenamento, etc.
- ✓ Os clientes de nuvem devem ter acesso um mecanismo de relatórios que forneça evidências de isolação e emita alertas caso ocorra uma violação.
- ✓ Os clients de nuvem devem estar cientes de situações de multilocação envolvendo suas máquinas virtuais onde preocupações regulatórias podem requerer sua segregação.

5 SEGURANÇA COMO UM SERVIÇO

A computação em nuvem oferece as organizações muitas vantagens e economias. No entanto uma das maiores barreiras a adoção da computação em nuvem é o sentimento de falta de segurança que muitas organizações tem na computação em nuvem. A segurança como um serviço além de um serviço da nuvem é uma nova tendência que vem diminuindo essa percepção de que a nuvem é um ambiente inseguro (CARVALHO, 2011).

Assim como no SaaS (Software como serviço), o modelo de negócio de segurança como serviço (SecaaS) é baseado em assinatura. Na SecaaS existem dois tipos emergentes de provedores. O primeiro tipo são empresas já estabelecidas no ramo de segurança da informação que estão mudando seus métodos de entrega de serviços para incluir serviços entregues através da nuvem. O segundo tipo são startups que estão emergindo nesse campo como puros provedores de segurança da informação como um serviço da nuvem (CSA, 2011).

Computação em nuvem representa uma das mais significantes mudanças que indústria de tecnologia da informação e comunicação experienciou. Uma das grandes inovações proporcionadas pela nuvem é a centralização de recursos de segurança. No contexto de nuvem um cliente pode escolher quais dos serviços de segurança serão adquiridos em que quantidade e ainda onde e quando serão implementados. Ou seja como qualquer outro serviço da nuvem a segurança como um serviço pode ser provida sob demanda, de forma rápida e escalável com pouco ou nenhuma interação humana em sua aquisição.

Existem diversos benefícios estratégicos em se utilizar serviços de segurança centralizados. Pode-se apontar como sendo os principais: uma agregação maior de conhecimento sobre problemas e soluções no que tange a segurança informação, uma grande base informações sobre segurança da informação facilmente acessível, um banco de profissionais de segurança disponíveis a todo momento e sob demanda. A segurança como serviço ainda possibilita que os clientes comparem ofertas baseadas em padrões de segurança a banco de profissionais disponíveis. Dessa forma os clientes podem tomar a decisão de contratar o provedor de segurança que melhor atenda suas necessidades (CSA, 2011).

Organizações que fazem uso de segurança como serviço ainda tem uma vantagem competitiva sobre seus concorrentes uma vez que as organizações que se utilizam do SecaaS tem acesso antecipado a informações referentes a novos riscos e ameaças. Além disso organizações que fazem o uso de SecaaS conseguem evitar caros processos litigiosos ou multas pois os provedores ofertam serviços de análise de conformidade e já proveem as organizações clientes todo o predicado obrigatório de conformidades necessário para atuar em uma determinada área.

5.1 DIVERSIDADE DE OFERTAS DE SEGURANÇA COMO SERVIÇO

Segurança como um serviço é mais que um modelo de terceirização para gestão de segurança. É um componente essencial em assegurar a resiliência e a continuidade do negócio. Devido a seu modelo elástico de serviços entregues através da nuvem, clientes precisam apenas pagar pela quantidade que eles necessitam, como o número de estações de trabalho a serem protegidas e não pela infraestrutura de suporte e o pessoal para suportar vários serviços de segurança. Um provedor geralmente consegue oferecer maior expertise de segurança do que é normalmente disponível em uma organização que opta por fazer ela mesma sua segurança da informação (MATHER, KUMARASWAMY e LATIF, 2009). Além do mais a contração de um serviço de segurança da nuvem permite que os usuários desse serviço foquem no seu negócio e deixem segurança com empresas especializadas em garanti-la.

As ofertas de hoje em SecaaS envolvem diferentes serviços para melhorar a segurança da informação: segurança de e-mail; segurança da web; gestão de vulnerabilidades; e identity-as-a-service na tradução literal, Identidade como um Serviço (IDaaS), prevenção de perda de dados, avaliações de segurança, prevenção, detecção e gestão de intrusão e outros (CSA, 2011).

Abaixo uma breve descrição dos principais serviços de segurança ofertados por provedores de nuvem levantados pela Cloud Security Alliance (2011):

- Serviço de identidade e de gerencia de acesso - Identidade como serviço é um termo genérico que cobre um de muitos serviços que podem compreender um ecossistema de identidade. Esses serviços de identidade devem prover controles para identidades, acesso, e gestão de privilégios. Serviços de identidade precisam incluir pessoas, processos, e sistemas que são usados para gerir o acesso a recursos organizacionais assegurando que a identidade da entidade de quem pretende acessar determinada informação foi verificada, então conceder o nível correto de acesso baseado nessa identidade. Ainda está incluso nesse serviço a gerência de logs de autenticação. Esses logs devem ser completamente auditáveis pelo cliente ou por terceiros.

- Prevenção de perda de dados - Esse serviço consiste em Monitorar, proteger, e demonstrar proteção de dados ociosos, em uso ou em movimento estejam esses dados na nuvem ou em computadores nas premissas da organização. Esse serviço é comumente chamado DLP (Data *Loss Prevention* - Prevenção contra perda de dados) ele oferece proteção aos dados de uma organização. O DLP é implementado normalmente rodando como um cliente em computadores ou servidores da organização reforçando políticas sobre quais ações são autorizadas para um determinado conteúdo ou arquivo. Utilizando-se do DLP o usuário pode especificar por exemplo que nenhum arquivo que contenham números que se pareçam com C.P.F. ou números de cartão de crédito pode ser envidado por e-mail, ou que todo arquivo armazenado em um *pendrive* seja automaticamente criptografado e que somente outra máquina da organização com um cliente DLP rodando e bem configurado possa descriptografar esses dados. As possibilidades de controle são infinitas realmente limitadas apenas as políticas da organização cliente.

- Segurança Web - Segurança web consiste na proteção em tempo real, oferecida para qualquer diapositivo final pertencente a uma organização, ou seja, estações de trabalho, smartphones, notebooks de stakeholders etc. Todo trafego web desses dispositivos é enviado ao provedor de segurança web como serviço, e então esse trafego é escaneado em busca de malwares e outras ameaças, e apenas tráfego limpo, livre de malwares ou ameaças conhecidas, é entregue aos usuários finais. Utilizando-se desse serviço organizações ainda podem reforçar suas políticas de conteúdo web pois esse serviço permite a organização bloquear que certos conteúdos de web sites possam ser acessados de dispositivos pertencentes a organização ou de dentro da rede da organização. Utilizando-se desse serviço também pode-se definir janelas de tempo em que esta é permitida a navegação web. Segurança web como serviço ainda envolve examinar o trafego que sai da organização para web de forma a barrar que qualquer informação sensível seja envidada para fora da organização sem autorização.

- Segurança de E-mail - O serviço de segurança de e-mail prove controle sobre os e-mail que chegam e saem, protegendo a organização contra phishing, anexos maliciosos, reforçando politicas coorporativas como uso aceitável, prevenção de spam e proteção contra vazamento de informação confidencial. Esse serviço ainda permite que uma redução da carga nos servidores uma vez que menos e-mails, apenas e-mails livres de phishing, malwares ou propagandas, serão redirecionados para o cliente. E com isso ainda há um aumento na efetive dos esforços anti-malware da organização.

- Avaliações de segurança - O serviço de avaliação de segurança consiste em auditorias feitas sobre os serviços de nuvem ou sobre os sistemas dentro das premissas da organização ou de empresas terceirizadas contratadas para prover soluções de TIC. No modelo de entrega do SecaaS, assinantes podem obter esses serviços de avaliação com todas as características da nuvem: elasticidade, pouco *overhead* de administração, pagar apenas por aqui que usar e baixo investimento inicial.

- Prevenção, detecção e gestão de intrusão - Esse serviço consiste em prover uma visão granular do que está acontecendo dentro de uma rede de uma empresa. Os sistemas de detecção/prevenção de intrusão monitoram o trafego da rede e compara a atividade a um padrão de utilização também faz o uso de regras predefinidas de atividades proibidas dentro da rede.

Em infraestruturas tradicionais os campos de atuação dos sistemas de detecção/prevenção de intrusão podem se estender até DMZ's segmentadas por firewalls ou roteadores onde web servers corporativos são localizados ou monitorando conexões a um base de dados interna. Na nuvem, Sistemas de detecção de intrusão geralmente focam seus esforços em infraestruturas virtuais e atividades cross-hypervisor onde ataques pode corromper múltiplos inquilinos ao mesmo tempo e criar um verdadeiro caos no sistema.

- Segurança da informação e gestão de eventos (SIEM - *System Information and Event Managment*) - Esse serviço consiste em reunir logs e dados de eventos das redes virtuais e reais pertencentes a organização. Essas informação então é correlatada e analisada para prover relatórios e alertas em tempo real sobre eventos que podem necessitar de interação humana ou algum tipo de resposta especifica. Esses dados e logs devem ser armazenados de forma que não possam ser adulterados para futuras auditorias ou para que possam ser utilizados em eventuais processos judiciais.

- Criptografia - Criptografia é o processo de transformar dados legíveis, em claro, em dados cifrados, sem significado algum nem revela nenhuma informação sobre o dado em claro. Esse processo é feito através de algoritmos que tornam computacionalmente impraticável descriptografar os dados sem a chave apropriada. Portanto apenas quem possui a chave correta para descriptografar um arquivo criptografado tomará conhecimento do real conteúdo do arquivo. A gerência dos algoritmos utilizados e das chaves utilizadas é o principal foco de serviço de segurança da nuvem.

- Continuidade de negócio e recuperação de desastres - Continuidade de negócios e recuperação de desastre são as medidas de segurança que visam assegurar resiliência operacional no caso da ocorrência de um desastre. Desastres não apenas grandes catástrofes naturais como tempestades, terremotos ou incêndios. Desastre para uma organização é qualquer evento que cause uma interrupção abrupta de um processo essencial para o funcionamento da empresa. Daí a importância de se precaver contra cenários desse tipo. E esse serviço de segurança tem como objetivo prover uma gestão de continuidade de negócios e recuperação de desastre de forma que mesmo se verdadeiros desastres ocorrerem a organização já anteviu esse cenário e já tem medidas prontas para serem postas em prática.

- Segurança de redes - Esse serviço consiste em oferecer segurança da rede como um todo incluindo as redes virtuais que ligam as maquinas virtuais. Portanto é necessário que os controles aqui empregados tenham forte ligação com o hypervisor para que nenhum tráfego nem real nem virtual seja invisível aos controles empregados por esse serviço. E como todos os serviços aqui apresentados como este consiste em uma oferta da nuvem confere aos clientes toda a elasticidade e economia associados a esse modelo de prover serviços.

6 CONCLUSÕES

Para atingir o primeiro o objetivo foi feita uma pesquisa bibliográfica exploratória por meio de livros e artigos sobre o assunto os quais foram consultados a fim de apresentar a computação em nuvem, suas principais características e motivações. Para atingir o segundo objetivo, foi realizada uma minuciosa exploração, dos livros e artigos encontrados na primeira etapa do trabalho, afim de encontrar as principais ameaças que os clientes de computação em nuvem estão sujeitos, e as principais preocupações das organizações que ainda permanecem receosas quando a adoção da nuvem. Para atingir o terceiro objetivo, uma nova análise minuciosa dos livros e artigos foi feita agora com o objetivo de encontrar e compilar as recomendações de segurança da informação apresentadas nesses documentos. Um trabalho de filtragem por recomendações mais relevantes também feito, o critério usado nesse filtro foi o de quais recomendações mais se relacionavam com os problemas encontrados na segunda etapa do trabalho. No total foi feito um compilado de 214 recomendações de segurança da informação. Dessa forma todos os objetivos propostos no trabalho foram alcançados.

Então a grande contribuição desse trabalho foi reunir, em português, um compilado de informações acerca de problemas e recomendações de segurança da informação de soluções de TIC baseadas computação em nuvem.

Para trabalhos futuros uma análise críticas das recomendações aqui propostas pode ser feita afim de encontrar novas brechas de segurança não cobertas pelas recomendações e outros problemas de segurança não elencados no capítulo 3. Também pode-se utilizar esse trabalho como ponto de partida para a construção de uma ferramenta que automatize a avalição de riscos envolvidos na adoção da computação em nuvem.

REFERÊCIAS BIBLIOGRÁFICAS

ABNT. ABNT NBR ISO/IEC 27002: Tecnologia da Informação - Técnica de Segurança - Código de prática para a gestão da segurança informação, 2005. 120.

CARVALHO, M. SECaaS - Security as a Service. **ISSA Journal**, outubro 2011. Disponivel em: <http://pt.scribd.com/doc/106917829/SECaaS-%E2%80%93-Security-as-a-Service>. Acesso em: 23 janeiro 2013.

CASTRO, R. D. C. C. D.; SOUSA, V. L. P. **Segurança em Cloud Computing - Governança e Gerenciamento de Riscos de Segurança**. III Congresso Tecnológico do InfoBrasil. Fortaleza: [s.n.]. 2010.

CLOUD SECURITY ALLIANCE - BRAZILIAN CHAPTER. Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem V2.1, 2010. Disponivel em: <https://cloudsecurityalliance.org/guidance/CSAGuidance-pt-BR.pdf>. Acesso em: 23 janeiro 2013.

CLOUD SECURITY ALLIANCE - BRAZILIAN CHAPTER. Adoção de Computação em Nuvem e suas Motivações, agosto 2012. Disponivel em: <https://chapters.cloudsecurityalliance.org/brazil/files/2012/08/WhitePaper-Adoc%CC%A7a%CC%83oDeComputac%CC%A7a%CC%83oEmNuvemESuasMotivac%CC%A7o%CC%83es-Ago_2012-V1.0.pdf>. Acesso em: 23 janeiro 2013.

CLOUD SECURITY ALLIANCE. Top Threats to Cloud Computing V1.0, março 2010. Disponivel em: <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>. Acesso em: 23 janeiro 2013.

CLOUD SECURITY ALLIANCE. Defined Categories of Service V1.0, 2011. Disponivel em: <https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf>. Acesso em: 23 janeiro 2013.

CLOUD SECURITY ALLIANCE. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, 2011. Disponivel em: <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>. Acesso em: 23 janeiro 2013.

INTEL. Next Generation Center: Grid Computing, 2011. Disponivel em: <http://pt.scribd.com/doc/3808477/-Services-Grid-Computing>. Acesso em: 23 janeiro 2013.

ISO - INTERNETIONAL ORGANIZATION FOR STANDARDIZATION. ISO/DIS 31000: Risk Managment - Principles and guidelines on implementation, 2009.

MATHER, T.; KUMARASWAMY, S.; LATIF, S. **Cloud Security and Privacy:** An Enterprise Perspective on Risks and Compliance. 1st. ed. Sebastopol: O'Reilly, 2009.

MATTOS, D. M. F. Grupo de Teleinformática e Automação. **Universidade Federal do Rio de Janeiro**, 2008. Disponivel em: <http://www.gta.ufrj.br/grad/08_1/virtual/OqueohypervisorouVMM(VirtualMachineMonit.html>. Acesso em: 11 abril 2013.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing, Gaithersburg, dezembro 2011. Disponivel em: <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>. Acesso em: 23 janeiro 2013.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Special Publication 800-145: The NIST Definition of Cloud Computing, Gaithersburg, setembro 2011. Disponivel em: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. Acesso em: 23 janeiro 2013.

SILVA, A. L. J. M. **Cloud Computing: Segurança e Privacidade da Informação na Nuvem**. IESF – Instituto Superior de Estudos Financeiros e Fiscais. [S.l.]. 2012.

VMWARE. Securing the Cloud: A Review of Cloud Computing, Security Implications and Best Pratices, 2009. Disponivel em: <http://www.savvis.com/en-us/info_center/documents/savvis_vmw_whitepaper_0809.pdf>. Acesso em: 23 janeiro 2013.

WARREN, S. Thech Republic, 2008. Disponivel em: <http://www.techrepublic.com/blog/virtualization-coach/what-is-your-best-definition-of-vm-sprawl/151>. Acesso em: 12 abril 2013.

WINKLER, V. J. R. **Securing the Cloud**. Waltham: Syngress, 2011.