TRABALHO DE GRADUAÇÃO

ESTUDO DOS ASPECTOS DE AUTENTICAÇÃO PARA SAAS

Thiago Barros Zanette da Silva

Brasília, junho de 2015

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

TRABALHO DE GRADUAÇÃO

ESTUDO DOS ASPECTOS DE AUTENTICAÇÃO PARA SAAS

Thiago Barros Zanette da Silva

Relatório submetido ao Departamento de Engenharia Elétrica
como requisito parcial para obtenção do grau
de Engenheiro de Redes de Comunicação

Banca Examinadora

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

Profª. PhD. Edna Dias Canedo, UnB/ FGA
(Examinador Externo) _____

Prof. PhD. Rafael Timóteo de Sousa Jr., UnB/ ENE
(Examinador Interno) _____

Dedicatória

Dedico este trabalho ao meu amigo Wally, onde quer que ele esteja.

Thiago Barros Zanette da Silva

Agradecimentos

Agradeço ao meu orientador e à banca examinadora.

Thiago Barros Zanette da Silva

RESUMO

A problema da falta de segurança na autenticação de usuários de serviços Web ou SaaS - *Software as Service*, tendência mundial da Internet para disponibilização de softwares via Web, é um problema grave. Atualmente são inúmeros os casos de invasão deste serviço em função da falta de implantação de soluções, muitas vezes simples, de autenticação e criptografia que garantam a autenticidade dos usuários e dos sistemas. Desta forma, é apresentada a computação em nuvem, suas principais características, motivações e problemas no que tange a segurança da informação. É proposto um conjunto de recomendações gerais de melhores práticas de segurança da informação usando como metodologia a compilação das principais recomendações propostas pelos principais autores e grupos especializados em segurança na computação em nuvem. E, finalmente, são propostas duas recomendações específicas de segurança em SaaS para dar mais segurança aos usuários contra o número crescente de invasões, sequestros de contas e de acesso não autorizado a dados sigilosos, como o caso da NSA que veio a público recentemente. Como resultado final, conclui-se que as duas soluções propostas podem ser tanto implementadas largamente por administradores de ambientes em SaaS e de computação em nuvem em geral, quanto como podem formar a base para a criação de políticas de segurança para autenticação forte, em especial em sites do governo, via ePWG - Padrões Web em Governo Eletrônico.

Palavras-chave: *computação em nuvem, segurança da informação, melhores práticas, gestão de riscos, autenticação segura.*

ABSTRACT

The problem of lack of security in user's authentication on Web service or SaaS - Software as Service, global Internet tendency for providing Web software, is a serious problem. Currently there are countless cases of invasion of this service due to the lack of implementation solutions, often simple, of authentication and encryption to ensure the authenticity of users and systems. Thus, it is presented the cloud computing, its main characteristics, motivations and concerns to information security. It is proposed a set of general recommendations for best practices on information security using as methodology the compilation of the main recommendations made by the leading authors and specialized security groups in cloud computing. And finally, two specific recommendations are proposed for SaaS security to give more security to users from the growing number of accounts invasions, hijacking and unauthorized access to sensitive data, like the case of the NSA that recently went public. As a final result, it is concluded that the two proposed solutions can be largely implemented by environments administrator's in SaaS and cloud computing in general, as well to form the basis for the creation of security policies for strong authentication, especially on government sites, via ePWG - Web Standards in Electronic Government.

Keywords: *cloud computing, information security, best practices, risk management, secure authentication.*

SUMÁRIO

1 INTRODUÇÃO 5
1.1 CONTEXTUALIZAÇÃO 5
1.2 DESCRIÇÃO DO PROBLEMA 6
1.3 OBJETIVOS 8
1.4 METODOLOGIA 8
1.5 JUSTIFICATIVA 9
1.6 ESTRUTURA DO TRABALHO 10

2 FUNDAMENTOS DA COMPUTAÇÃO EM NUVEM 12
2.1 VISÃO GERAL 12
2.2 CARACTERÍSTICAS ESSENCIAIS DA NUVEM 14
2.3 MODELOS DE SERVIÇOS 14
2.4 MODELOS DE IMPLANTAÇÃO 19
2.5 MODELOS DE REFERÊNCIA DE NUVEM 21
2.6 ÁREAS CRÍTICAS DE SEGURANÇA DA COMPUTAÇÃO EM NUVEM 23

3 PROBLEMAS DE SEGURANÇA DA INFORMAÇÃO NA COMPUTAÇÃO EM NUVEM ..25
3.1 PRINCIPAIS RISCOS 25
3.2 GOVERNANÇA E GESTÃO DE RISCOS CORPORATIVOS 26
3.3 ASPECTOS LEGAIS E DESCOBERTA ELETRÔNICA 28
3.4 CONFORMIDADE E AUDITORIA 30
3.5 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DOS DADOS 31
3.6 PORTABILIDADE E INTEROPERABILIDADE 33
3.7 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES 33
3.8 OPERAÇÕES DE DATACENTER 35
3.9 RESPOSTA A INCIDENTE, NOTIFICAÇÃO E REMEDIAÇÃO 36
3.10 SEGURANÇA DE APLICAÇÕES 37
3.11 CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES 38
3.12 GERENCIAMENTO DE IDENTIDADE E ACESSO 39
3.13 VIRTUALIZAÇÃO 40

4 RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO NA COMPUTAÇÃO EM NUVEM 43
4.1 GOVERNANÇA E GESTÃO DE RISCOS CORPORATIVOS 43
4.2 ASPECTOS LEGAIS E DESCOBERTA ELETRÔNICA 46
4.3 CONFORMIDADE E AUDITORIA 47
4.4 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DOS DADOS 49
4.5 PORTABILIDADE E INTEROPERABILIDADE 52
4.6 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES 56
4.7 OPERAÇÕES DE DATACENTER 57
4.8 RESPOSTA A INCIDENTE, NOTIFICAÇÃO E REMEDIAÇÃO 58
4.9 SEGURANÇA DE APLICAÇÕES 59
4.10 CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES 61
4.11 GERENCIAMENTO DE IDENTIDADE E ACESSO 62
4.12 VIRTUALIZAÇÃO 64

5 PROPOSTA DE AUTENTICAÇÃO E ARMAZENAMENTO SEGUROS PARA SAAS 66

5.1 AUTENTICAÇÃO DE DOIS FATORES (2FA) 66
5.2 MODELO DE CRIPTOGRAFIA FIM-A-FIM (E2EE) 70

6 CONCLUSÃO 73

REFERÊNCIAS BIBLIOGRÁFICAS 75

LISTA DE FIGURAS

1.1 Pesquisa do IDC demonstra que a preocupação com segurança é o problema número um que defronta a computação em nuvem 6

2.1 Características essenciais da nuvem 14
2.2 Modelos de serviço de nuvem 15
2.3 Visualização da arquitetura em camadas dos modelos de serviço 15
2.4 SaaS - *Software as a Service* 16
2.5 PaaS - *Platform as a Service* 17
2.6 IaaS - *Infrastructure as a Service* 18
2.7 Exemplos de serviços de SaaS, PaaS e IaaS 18
2.8 Modelos de implantação de nuvem 19
2.9 Visualização das nuvens pública, privada e híbrida 21
2.10 Modelo de referência da nuvem 22
2.11 Como a segurança é integrada nos modelos de serviço 23

5.1 Ilustração do funcionamento da 2FA, adaptado de (CERT.BR, 2014) 67
5.2 Figura 5.2. E-mail recebido do Yahoo! avisando da tentativa de entrar em minha conta a partir dos EUA 68
5.3 Comparação entre autenticação tradicional, 2FA e 2SV 69
5.4 Slide da apresentação da NSA sobre o MUSCULAR indicando o sucesso na invasão à nuvem do Google 70
5.5 Comparação entre o sistema de criptografia padrão e a E2EE 71

LISTA DE TABELAS

2.1 Comparativo das principais características dos modelos de implantação 21

LISTA DE SÍMBOLOS

Siglas

ABNT	Associação Brasileira de Normas Técnicas
API	*Application Programming Interface*
CNPq	Conselho Nacional de Pesquisa
COBIT	*Control Objectives for Information and related Technology*
COSO	*Committee of Sponsoring Organizations*
CRM	*Customer Relationship Management*
CSA	*Cloud Security Alliance*
DAM	*Database Activity Monitoring*
DES	*Data Encryption Standard*
DLP	*Data Loss Prevention*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
ePWG	Padrões Web em Governo Eletrônico
FAM	*File Activity Monitoring*
GCHQ	*Government Communications Headquarters*
IDC	*International Data Corporation*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
ISACA	*Information Systems Audit and Control Association*
ISF	*Information Security Forum*
ISO	*International Standardization Organization*
ITIL	*Information Technology Infrastructure Library*
ITU-T	*Telecommunication Standardization Sector*
LDAP	*Lightweight Directory Access Protocol*
NIST	*National Institute of Stands and Technology*
NSA	*National Security Agency*
OTP	*One-Time Password*
SABSA	*Sherwood Applied Business Security Architecture*
SAML	*Security Assertion Markup Language*
SIEM	*Security Information and Event Management*
SLA	*Service Level Agreement*
SOA	*Service-Oriented Architecture*
SPML	*Service Provisioning Mark-up Language*
SSL	*Secure Sockets Layer*

SSO	*Single Sign-On*
TIC	Tecnologia da Informação e Comunicação
TOGAF	*The Open Group Architecture Framework*
URL	*Uniform Resource Locator*
VM	*Virtual Machine*
VPN	*Virtual Private Network*

1 INTRODUÇÃO

Este capítulo apresenta considerações gerais sobre a motivação acerca do desenvolvimento deste trabalho. Além disso, é mostrada a estrutura de organização do conteúdo ao longo do trabalho.

1.1 CONTEXTUALIZAÇÃO

Ao longo dos últimos anos, houve um rápido crescimento na adoção da computação em nuvem, não só pelas empresas, mas também pelos usuários domésticos para a hospedagem de dados e implantação de serviços, principalmente em serviços SaaS, como Netflix, Dropbox e Spotify. Esta tendência deverá continuar pelos próximos anos e para 2018 é previsto que 59% das atividades na nuvem sejam em SaaS, 41% mais do que em 2013 (CISCO, 2014).

A receita gerada pelos serviços na nuvem em todo mundo alcançou US$ 68,3 bilhões em 2010, um aumento de 16,6% em relação a 2009. A indústria também espera um forte crescimento até 2014, quando a receita deverá atingir US$ 148,8 bilhões (GARTNER, 2010).

Além de estar em rápida acessão produzindo cada vez mais receitas e abrir novos horizontes para as organizações, a computação em nuvem também introduz novos riscos. A segurança na computação em nuvem não é muito diferente da que qualquer ambiente de TIC necessita. No entanto, por causa dos modelos de nuvem e tecnologias utilizadas para tornar possíveis os serviços de nuvem, a utilização da computação requer diferentes cuidados.

O IDC conduziu uma pesquisa com 244 executivos de TI sobre os serviços de nuvem. Como é mostrada na Figura (1.1), a questão da segurança encabeçou a lista de preocupações em relação à nuvem com 74,5% (IDC, 2009).

A primeira e mais óbvia preocupação é com a questão de privacidade. Como saber que seus dados estão seguros e protegidos sendo hospedados por terceiros? Há também muitas preocupações porque, a execução da lei, por meio descoberta eletrônica, tem tido mais capacidade em obter os dados mantidos na nuvem, mais do que elas são provenientes dos servidores de uma empresa. Esse é um item essencial do modelo de computação na nuvem. Pois como os usuários estão depositando seus arquivos em servidores remotos, esses arquivos podem ser capturados no momento em que trafegam na rede ou ainda podem ser capturados nos próprios servidores da empresa, inclusive por funcionários mal intencionados.

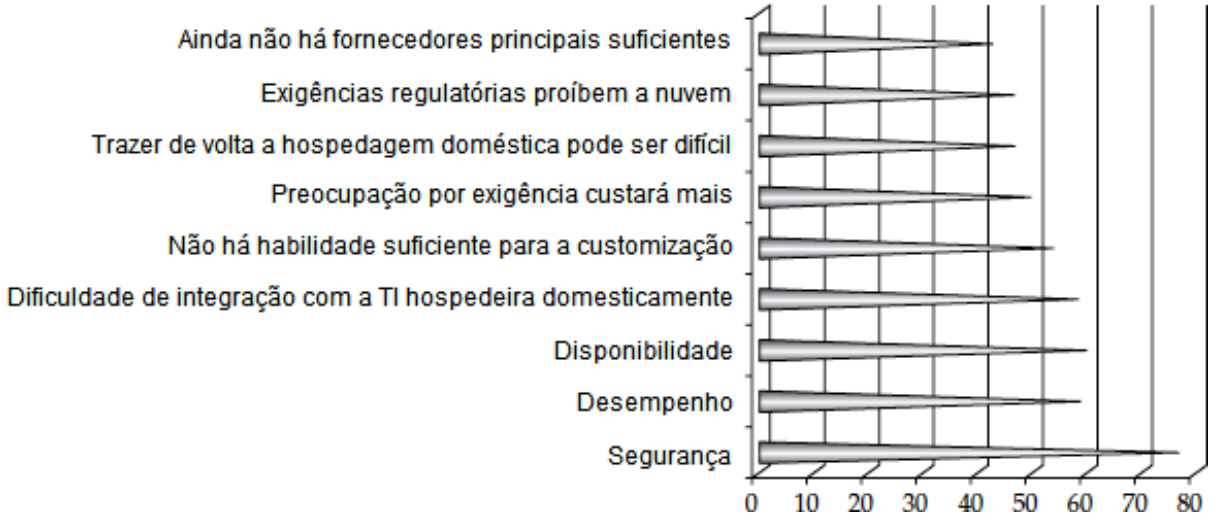

Figura 1.1. Pesquisa do IDC demonstra que a preocupação com segurança é o problema número um que defronta a computação em nuvem, adaptado de (IDC, 2009).

Mesmo que provedor de nuvem faça o melhor para proteger os dados do cliente, ele ainda pode ser alvo de *hackers*, e, nesse caso, as informações sensíveis do cliente ficarão à mercê de qualquer um que queira entrar à força e obtê-las, podendo ser apagadas ou até mesmo vendidas.

Com os serviços de computação em nuvem sendo cada vez mais sendo utilizados para o processamento de dados confidenciais em aplicações, como comercio eletrônico, as implicações em segurança e privacidade são altas e qualquer descuido nos processos de segurança pode acarretar o comprometimento dos dados, o que torna a segurança na nuvem assunto de primeira ordem. (GREENBERG, 2008).

1.2 DESCRIÇÃO DO PROBLEMA

Há um crescente no número de casos de violação de segurança de alto perfil nos últimos anos e muitos sites e serviços Web ainda não dispõem de serviços de segurança confiáveis. Há várias soluções no mercado, no entanto, essas soluções não são utilizadas em larga escala. Por isso se faz necessário definir por meio de padrões e recomendações de segurança, um conjunto de políticas que devam ser implementadas, em especial, na autenticação de usuários e armazenamento dos dados, já que é possível um atacante burlar o login em ambientes Web e invadir contas de usuários ou ainda ter seus dados expostos ou acessados indevidamente por terceiros.

Entre fevereiro e março de 2005, hackers tiveram acesso às credenciais de funcionários do eBay, site de comércio eletrônico com 140 milhões de contas ativas no mundo. Assim foram capazes de acessar áreas do banco de dados da empresa, que incluíam nome dos usuários, senhas criptografadas, endereço de e-mail, endereço físico, número de telefone e

data de nascimento (CAPUTO, 2014).

Entre os dias 17 e 19 de abril de 2011, foi descoberto que informações de contas de usuários da PlayStation Network, rede de jogos on-line da Sony, ficaram comprometidas por conta de uma "intrusão não-autorizada" na rede e, por isso, foi desligada por mais de uma semana. O nome, endereço completo, endereço de e-mail, aniversário e até a senha e login dos usuários foram roubados. (ROHR A, 2012). Isto causou um prejuízo para a Sony de US$ 24 bilhões, o maior da historia deste tipo, além de demonstrar que os dados não eram sequer criptografados (ARRUDA, 2011).

Em 23 de março de 2015, o Twitch, site de transmissões ao vivo pela internet, redefiniu as senhas de todas as 100 milhões de contas do serviço após anunciar que "pode ter havido acesso não autorizado a informações pessoais dos usuários", como nome de usuário e endereço de e-mail associado, senha, o último endereço de IP a se conectar, tipo de cartão de crédito, número truncado do cartão e data de validade, primeiro e último nome, número de telefone, endereço e data de nascimento" (G1, 2015). Mais uma vez ficou demonstrado que os dados não criptografados.

Bem como o vazamento ou a perda de dados, o sequestro de conta é também uma das consequências dos problemas de vulnerabilidade da nuvem somada à distração ou ingenuidade do usuário. *Phishing*, um dos ataques mais conhecidos, geralmente provê ao atacante alguma informação sigilosa, como a senha de usuário e a partir desta o hacker passa a ter o domínio da conta podendo utilizá-la para atacar outros usuários, descobrir outras senhas e informações, enviar informações falsas, etc. (CSA, 2010). O envenenamento de cache DNS funciona de forma semelhante. O servidor DNS retornar um endereço IP incorreto, desviando o tráfego para outro computador, o do atacante (CSA, 2013).

Em 2007, um funcionário da Salesforce.com, que oferece SaaS na área de CRM, foi alvo de um ataque de *phishing*, expondo sua senha a um atacante. Com isso, o *hacker* pode descobrir informações importantes de clientes, como o primeiro e último nomes, nome das companhias, e-mails e telefones, e passaram a enviar faturas falsas para os mesmos (MCMILLAN, 2007).

No final de agosto de 2014, centenas de fotos íntimas de várias celebridades vazaram na internet devido a uma falha de implementação de segurança do iCloud, o sistema de armazenamento na nuvem da Apple (INFO, 2014). As imagens foram obtidas por meio do armazenamento on-line oferecido pelo iCloud para backup automático de fotos a partir de dispositivos iOS (GUSMÃO, 2014). O vazamento aumentou a preocupação acerca da privacidade e segurança dos serviços de computação em nuvem, com especial destaque para a

sua utilização para armazenar informações privadas sensíveis.

Tudo foi possível graças a uma vulnerabilidade na programação do API do Find My iPhone, serviço de localização integrado ao sistema, que não bloqueava o acesso à conta ou utilizava CAPTCHAs, após algumas tentativas de acesso sem sucesso. Com isso, foi utilizado um script em Python chamado de iBrute, permitindo que usuários mal-intencionados fizessem um ataque de força bruta às contas dos usuários do iCloud e descobrissem as senhas. Mais tarde descobriu-se que também foram utilizados outros meios, como engenharia social para descobrir a pergunta secreta que possibilita o reset das senhas das contas (GUSMÃO, 2014).

Os exemplos das empresas citadas e muitas outras mais mostram o risco à segurança das informações confiadas a elas por não seguirem os padrões e recomendações das melhores práticas de segurança na nuvem. Diante disto, é necessário definir políticas que devam ser implementadas na computação em nuvem, não só para evitar acessos não autorizados ou invasões de contas, mas como também garantir a segurança como um todo.

1.3 OBJETIVOS

A proposta geral deste trabalho é oferecer uma compilação de informações sobre computação em nuvem, seus principais problemas de segurança, e propor um conjunto de recomendações das melhores práticas de gestão de segurança da informação, a fim de se reduzir os riscos envolvidos na sua utilização.

1.3.1 OBJETIVOS ESPECÍFICOS

1. Apresentar a computação em nuvem, suas principais características e motivações, identificando e caracterizando seus principais problemas no que tange a segurança da informação.
2. Propor um conjunto de recomendações gerais de melhores práticas de segurança da informação a partir da compilação das principais recomendações propostas pelos principais autores e grupos especializados em segurança na computação em nuvem.
3. Propor duas recomendações específicas de segurança em SaaS para dar mais segurança aos usuários contra o número crescente de invasões e sequestros de contas e de acesso não autorizado a dados sigilosos, como o caso da NSA que veio a público recentemente.

1.4 METODOLOGIA

A fim de que tais objetivos fossem atingidos, o desenvolvimento do trabalho se deu em três partes.

Primeiramente foi feita uma pesquisa e um levantamento bibliográfico exploratório de fontes de pesquisa que continham os principais conceitos da computação em nuvem, em seguida uma análise dos principais problemas relacionados à segurança da informação na nuvem e, por fim, foram elaboradas recomendação de soluções baseadas na literatura.

Para o primeiro objetivo, foi feita uma pesquisa e um levantamento bibliográfico exploratório por meio de livros, artigos, estudos de caso, publicações, periódicos, e normas técnicas da ISO, ABNT e IEEE que continham os principais conceitos, características, motivações e principais áreas de preocupação quanto às ameaças à segurança da computação em nuvem hoje. Dentre as bibliografias a que mais se destacou, em razão da grande quantidade de citações de seus artigos e guias em livros e nos artigos utilizados, foi a *Cloud Security Alliance*, organização sem fins lucrativos fundada no final de 2008 principalmente por representantes industriais, corporações e associações, visando promover as boas práticas de segurança em computação em nuvem (CSA, 2009). Portanto, seus guias foram usados como base (CSA, 2011).

Em seguida para o segundo objetivo, uma análise meticulosa foi feita na bibliografia encontrada, desta vez analisando as recomendações de segurança da informação para as áreas de preocupação críticas quanto às ameaças à segurança encontradas na primeira parte (CSA, 2011). As recomendações que mais se relacionavam com os problemas encontrados na etapa anterior foram organizadas numa lista que cobre as principais ameaças e preocupações com segurança na nuvem hoje.

Finalmente para o terceiro objetivo, uma análise foi feita em dois casos recentes de vulnerabilidades na nuvem. Foram identificadas as ameaças e vulnerabilidades por meio de uma análise de riscos da segurança da informação, em seguida foram propostas duas recomendações para essas vulnerabilidades na segurança na nuvem.

1.5 JUSTIFICATIVA

O trabalho, além de esclarecer questões importantes de segurança da informação, também incentiva a adoção de boas práticas para promover a segurança nos ambientes de computação em nuvem, evitando invasões e acessos não autorizados aos dados.

Pela falta de informação dos usuários, que não sabem do risco que correm em utilizarem apenas senhas, além da utilização de criptografia feita pelos provedores, não são mais suficientes para a proteção dos dados armazenados na nuvem contra acessos não autorizados.

Sistemas inseguros de instituições governamentais, como o do CNPq e o MatrículaWeb

da UnB, que nem sequer criptografam as senhas ou outros dados dos usuários, são facilmente suscetíveis a ataques. Caso haja vazamento de dados dos usuários, se a mesma senha for reutilizar em outros serviços, o atacante terá acesso a várias informações dos usuários.

Em virtude das ações de espionagem praticadas pelos Estados Unidos, o governo investirá em um novo cabo submarino ligando Fortaleza e Portugal, buscando substituir as atuais conexões Brasil-Europa, que hoje passam pelos Estados Unidos, para evitar espionagem americana, implementado pela Telebrás a um custo de R$ 450 milhões (TORRES, 2014). Entretanto, engenheiros funcionários da Telebrás utilizam do serviço de armazenamento do Dropbox para compartilharem entre si documentos, inclusive confidenciais, de obras, projetos, da arquitetura da rede e senhas de acesso aos ativos de rede da empresa. Como é sabido, o Dropbox seria o próximo serviço a ter seus dados espionados pela NSA (HONOROF, 2013).

Por consequência, todo o investimento seria em vão, já que os Estados Unidos saberia de todo o projeto, desde seu inicio até a implantação. Mais ainda, caso um funcionário tenha sua senha da conta comprometida, qualquer um com a senha terá acesso a todos os documentos confidenciais. O acesso não autorizado os dados, como no caso da NSA, pode ser evitado utilizando o modelo de criptografia fim-a-fim. Já o acesso à conta não autorizado por qualquer um com a senha é evitado com a autenticação de dois fatores, propostas neste trabalho.

Com isso, o trabalho auxilia administradores de sites Web na implantação de soluções de segurança simples que resolvem problemas muito recorrentes e na definição de padrões de segurança para autenticação em computação em nuvem, e quem sabe, para incrementar as soluções do governo propostas no ePWG, tornando, assim, a computação em nuvem mais segura.

1.6 ESTRUTURA DO TRABALHO

Este trabalho está organizado da seguinte maneira:

No capítulo 1 são definidas as considerações gerais sobre a motivação acerca do desenvolvimento deste trabalho.

No capítulo 2 são mostrados os conceitos básicos relativos ao domínio da computação em nuvem para o embasamento teórico. São apresentadas suas cinco características essenciais, três modelos de serviço e quatro de implantação.

No capítulo 3 são apresentadas as doze áreas de atenção crítica na computação em

nuvem e apontados seus principais problemas e preocupações em relação à segurança da informação

No capítulo 4 são feitas recomendações de segurança para as áreas críticas de segurança da informação na computação em nuvem mostradas no capítulo três.

No capítulo 5 são propostas, então, duas recomendações específicas de segurança em SaaS para dar mais segurança aos usuários contra o número crescente de invasões, sequestros de contas e de acesso não autorizado a dados sigilosos, como o caso da NSA que veio a público recentemente.

No capítulo 6 são apresentadas as conclusões a respeito das recomendações propostas, a correspondência com os objetivos propostos e como os mesmos serão necessários para trabalhos futuros com o intuito de desenvolver as melhores praticas de segurança da informação na computação em nuvem.

2 FUNDAMENTOS DA COMPUTAÇÃO EM NUVEM

Este capítulo tem por finalidade esclarecer e definir os tópicos relevantes para o entendimento teórico acerca do conteúdo do trabalho. São vistos os principais assuntos relacionados à computação em nuvem, suas cinco características essenciais, três modelos de serviço e quatro de implantação.

2.1 VISÃO GERAL

A computação em nuvem ainda é um conceito considerado emergente e em evolução, por isso existem mais de 22 definições diferentes na literatura para ela (MATHER *et al*, 2009). A definição mais aceita é a do NIST. A computação em nuvem é um modelo que permiti acesso ubíquo, conveniente e sob demanda via rede a um agrupamento compartilhado e configurável de recursos computacionais, como redes, servidores, equipamentos de armazenamento, aplicações e serviços, que podem ser rapidamente fornecidos e liberados com mínimo esforço de gerenciamento ou interação com o provedor de serviços (NIST, 2011).

Em outras palavras, ela consiste na oferta a recursos de TIC sob demanda, de forma rápida, mensurável e a qualquer hora e lugar. Os clientes podem solicitar mais ou menos recursos contratados automaticamente, pagando apenas o necessário naquele momento, não precisando adquirir mais recursos do que necessitam. Como o serviço é tarifado de acordo com quantidade de recursos que o cliente consome, clientes que utilizam mais recursos pagam mais, e os que utilizam menos recursos pagam menos. De forma análoga ao serviço de água ou energia elétrica, clientes que utilizam mais pagam mais e clientes que utilizam menos pagam menos.

Assim como acontece com muitos aspectos de TIC, a evolução e combinação de diversos modelos e conceitos resultaram na definição do modelo da computação em nuvem. Alguns dos principais modelos e conceitos pré-existentes englobados ou considerados por ela são: terceirização, *utility computing*, computação em grade, computação autônoma e virtualização (CSABR, 2012).

Um conceito importante para a evolução da computação em nuvem foi o da terceirização. Ela consiste na contratação de recursos de TIC de terceiros como serviço para realização de determinada atividade dentro da organização. Um de seus maiores benefícios é permitir que a empresa abra mão da execução de um processo e o transfira para terceiros, que tenham uma base de conhecimento mais especializada, com o objetivo de agregar maior valor ao produto final. Nos casos em que serviços que são implementados em nuvens públicas ou

comunitárias, o cliente estará terceirizando os serviços de TIC. No entanto, adotar a computação em nuvem não significa terceirizar serviços, uma vez que eles podem ser implementados em nuvens privadas.

Outro conceito importante é o de *Utility Computing*, que é uma evolução da terceirização. A empresa paga apenas pelo o que efetivamente for consumido. Consiste em serviços e produtos de TIC para consumo sob demanda e como serviços utilitários com o objetivo de fornecer componentes básicos, como armazenamento, processamento e largura de banda, para consumidores de TIC que pagam por unidade utilizada sem se preocuparem com limitações, escalabilidade, integridade, disponibilidade, dentre outros aspectos. A proposta é usar os serviços de TIC em função das demandas da empresa, otimizando a infraestrutura de software, hardware e serviços (CSABR, 2012).

A computação em grade também é parte da história da computação em nuvem. O núcleo do conceito da computação em grade é utilizar os recursos ociosos de computadores, independentemente da localização física e sem investimentos em novos hardwares (INTEL, 2011). Com isso, por intermédio da formação de grandes redes de computadores, cria-se um supercomputador virtual, com a utilização dos recursos preexistentes, permitindo o desenvolvimento de aplicações antes restritas a supercomputadores caríssimos. Ela é capaz de lidar com altas taxas de processamento que é dividido entre as várias máquinas, evitando, dessa forma, o desperdício de processamento (IBM B, 2005).

A computação autônoma surgiu de um manifesto feito em 2001 pela IBM, que alertava para o crescimento da complexidade dos sistemas computacionais e a inevitável incapacidade humana de os gerenciarem. Ela propõe sistemas computacionais capazes de se auto configurar, otimizar, corrigir e proteger, dado os objetivos definidos pelo administrador (IBM A, 2005).

A virtualização é utilizada pela grande maioria dos provedores de nuvem hoje. Surgiu no ambiente de computação de grande porte, a virtualização foi trazida para microcomputadores no final da década de 90. Ela é a simulação de características físicas do *hardware* e do sistema operacional do hospedeiro por intermédio do *hypervisor*, camada de *software* entre o *hardware* e o sistema operacional, responsável por fornecer ao sistema operacional hospedeiro a simulação da máquina virtual. De maneira simples, a virtualização são várias máquinas virtuais, com sistemas operacionais e *hardwares* diferentes ou não, rodando dentro de um único sistema operacional, de forma independente. Com a virtualização, vários usuários da nuvem podem ter máquinas virtuais hospedadas numa mesma máquina física, isso recebe o nome de sistema multilocatário (VMWARE, 2009).

2.2 CARACTERÍSTICAS ESSENCIAIS DA NUVEM

Os serviços na nuvem devem oferecer cinco características essenciais para demonstrarem suas relações e diferenças em relação às abordagens tradicionais de computação (Fig. 2.1): amplo acesso à rede, rápida elasticidade, serviços mensuráveis, autosserviço sob demanda e agrupamento de recursos (NIST, 2011).

Figura 2.1. Características essenciais da nuvem, adaptado de (CSA, 2011).

Os recursos devem estar disponíveis na rede e serem acessíveis em qualquer dispositivo com acesso à rede, tais como computadores pessoais, smartphones, vídeo games, smart TVs, tablets, etc.

Os recursos também devem ser providos automaticamente de forma rápida e elástica, permitindo a adaptação à demanda do consumidor sem que haja interrupção do serviço. Para o cliente de nuvem, os recursos disponíveis para concessão devem parecem ser ilimitados e podem ser contratadas em qualquer quantidade e hora.

Os serviços oferecidos devem controlar e otimizar automaticamente os recursos, disponibilizando mecanismos apropriados de medida para o tipo de recurso utilizado, como quantidade de espaço de armazenamento, velocidade de comunicação, capacidade de processamento, número de usuários ativos, etc.

O consumidor deve ser capaz de unilateralmente aumentar ou diminuir os recursos ofertados, como o tempo de servidor e armazenamento de rede, automaticamente e conforme necessário, sem a necessidade de interação humana com o provedor do serviço.

Os recursos computacionais do provedor de serviços, como armazenamento, processamento, memória, largura de banda, e máquinas virtuais e até nuvens privadas, devem ser agrupados de forma a atender diversos consumidores através do modelo de multilocação. Deve haver uma independência na localização, onde o consumidor não tem um controle exato de onde os recursos utilizados estão localizados, mas deve ser possível especificar o local em um nível mais alto de abstração, como país, estado ou datacenter.

2.3 MODELOS DE SERVIÇOS

A computação em nuvem é dividida em três grandes classes, também conhecidas como modelos de serviço, e várias combinações derivadas de acordo com a entrega de serviços oferecida (Fig. 2.2). As três classificações fundamentais são comumente referidas como "Modelo SPI", onde "SPI" significa Software, Plataforma e Infraestrutura (como um serviço), respectivamente (NIST, 2011).

Figura 2.2. Modelos de serviço de nuvem, adaptado de (CSA, 2011).

Segundo CSABR (2012), 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 (Fig. 2.3).

Figura 2.3. Visualização da arquitetura em camadas dos modelos de serviço, adaptado de (WONG, 2014).

2.3.1 SOFTWARE COMO SERVIÇO (SaaS - *Software as a Service*)

SaaS é o topo arquitetura em camadas da nuvem, e a mais conhecida devido ao fato de que aplicações populares, como Gmail, Facebook, Internet Banking, Netflix, Google Apps, Office 365, Salesforce CRM e tantas outras, estarem alocadas nessa camada. Os serviços prestados por esta camada são tipicamente acessados por usuários finais através de navegadores da Web (Fig. 2.4). Isto permite que os clientes possam acessa-los de qualquer

lugar e a qualquer hora, permitindo uma mobilidade maior mobilidade dos funcionários da empresa. Aplicações tradicionais de desktops, tais como processamento de texto e planilhas eletrônicas, já podem ser acessadas como serviços na Web. Este modelo de entrega de aplicativos diminui a preocupação com manutenção do software para os clientes finais e simplifica o desenvolvimento e testes para os fornecedores, entretanto, é o modelo de serviço menos flexível, já que só permite configurações específicas do usuário na aplicação (VELTE *et al*, 2009).

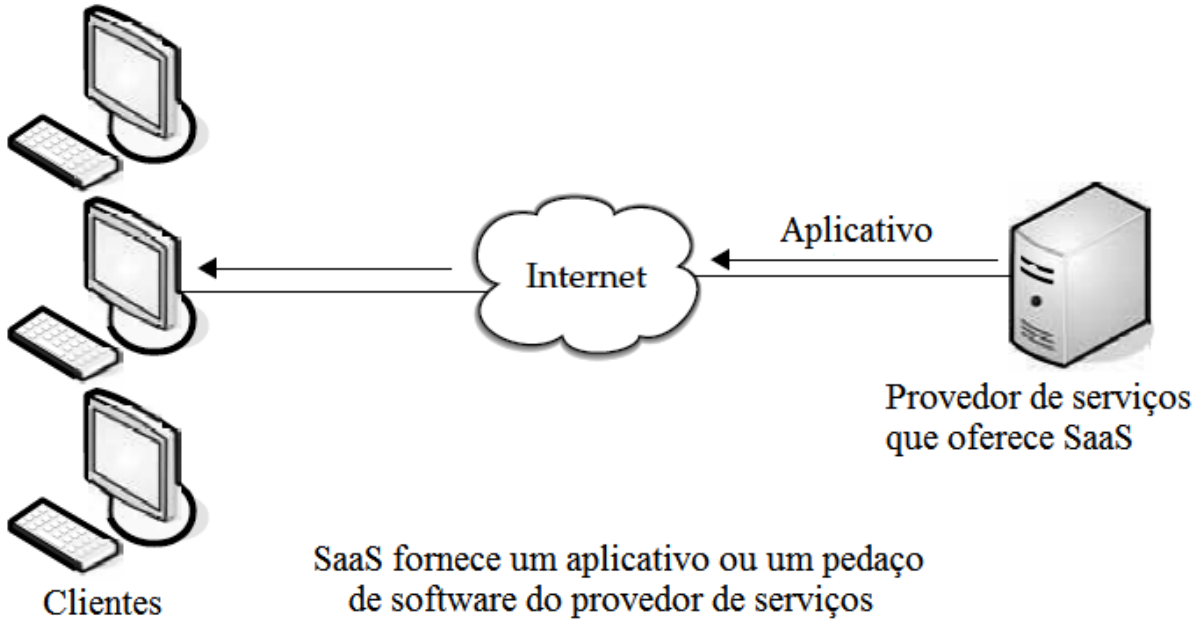

Figura 2.4. SaaS - *Software as a Service*, adaptado de (VELTE *et al*, 2009).

Contudo não exige quase nenhum esforço de configuração e manutenção do usuário. Os provedores deste tipo de serviço se encarregam de tarefas, como atualização da aplicação, monitoramento e disponibilidade, backups, balanceamento de carga, etc.

2.3.2 PLATAFORMA COMO SERVIÇO (PaaS - *Platform as a Service*)

A segunda camada é a PaaS. Nela são oferecidos serviços para que desenvolvedores de aplicações utilizem a infraestrutura da nuvem para criarem soluções e recursos necessários para armazenamento, organização de banco de dados, escalabilidade, suporte de segurança, sistemas operacionais ou novas linguagens de programação (Fig. 2.5). Como o usuário não controla ou gerência a infraestrutura da nuvem, como servidores, sistemas operacionais, armazenamento, ou redes, ele acaba sendo um modelo de nuvem menos flexível que a IaaS, porém não tão fechado quando o SaaS, já que tem o controle sobre as aplicações implementadas e configurações da aplicação referentes ao ambiente do servidor (VELTE *et al*, 2009).

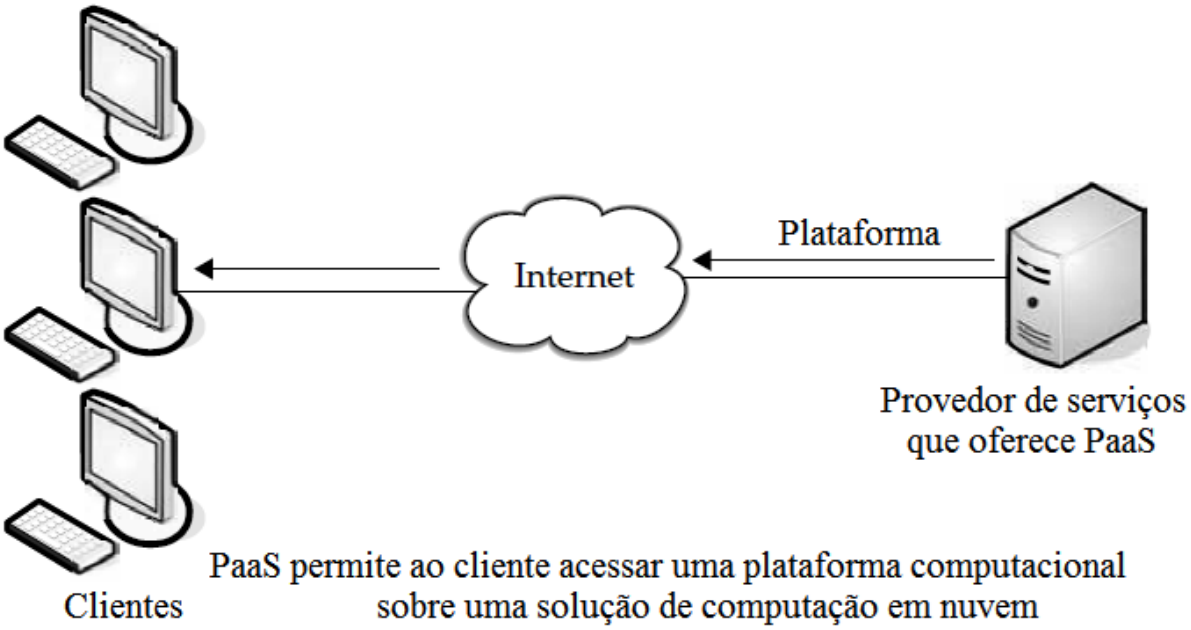

Figura 2.5. PaaS - *Platform as a Service*, adaptado de (VELTE *et al*, 2009).

Pode-se dizer que os usuários que trabalham com a PaaS criam todo o sistema que será utilizado pelo *software* para seu funcionamento. A união da PaaS e da IaaS possibilita um acesso mais regular e estruturado ao SaaS.

2.3.3 INFRAESTRUTURA COMO SERVIÇO (IaaS - *Infrastructure as a Service*)

IaaS, também conhecida como *hardware* como serviço - HaaS (do inglês hardware as a service), é a camada básica e estrutural para o funcionamento da computação em nuvem. Enquanto que SaaS e PaaS fornecem aplicações aos clientes, a IaaS limita-se a fornecer o hardware. São fornecidos recursos, geralmente virtualizados, de armazenamento, processamento, rede e outros recursos de computação fundamentais onde o usuário pode instalar e executar *softwares* em geral, incluindo aplicativos e sistemas operacionais (Fig. 2.6). Em vez de comprar servidores, software, racks e ter que pagar pelo espaço físico do datacenter, o prestador de serviço aluga esses recursos, além disso, a infraestrutura pode ser ajustada dinamicamente para cima ou para baixo, baseado nas necessidades de recursos do aplicativo (VELTE *et al*, 2009).

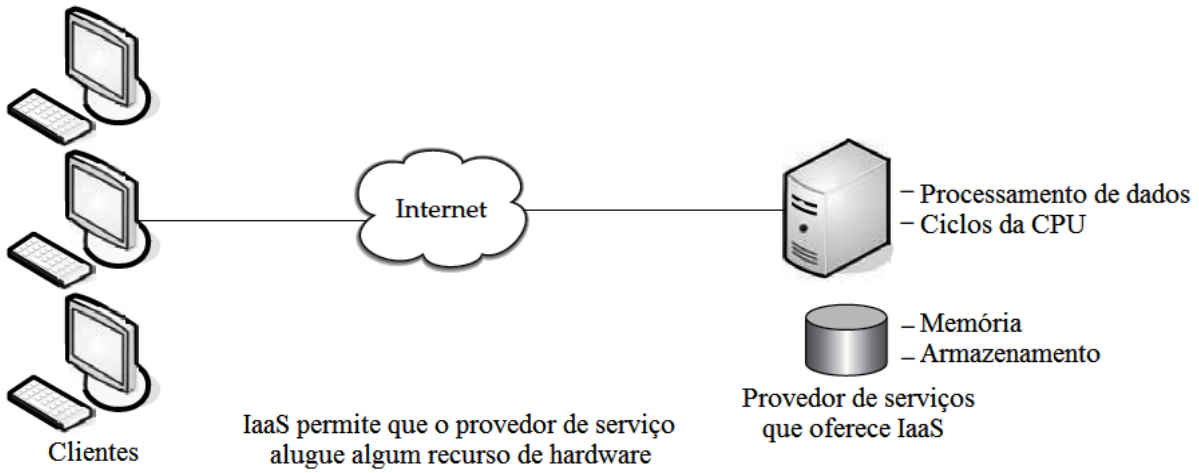

Figura 2.6. IaaS - *Infrastructure as a Service*, adaptado de (VELTE *et al*, 2009).

Como o consumidor tem controle sobre o sistema operacional, aplicações implementadas e armazenamento, isso torna a IaaS o modelo de serviço mais flexível da computação em nuvem, já que permite ao usuário configurar exatamente o que precisa, entretanto, ele não gerencia, nem controla as camadas adjacentes da infraestrutura na nuvem, toda essa atividade é coordenada por profissionais chamados de arquitetos de infraestrutura, que organizam e dão manutenção para que o serviço funcione com qualidade e eficiência.

Alguns exemplos de serviços SaaS, PaaS e IaaS são mostrados na Fig. (2.7):

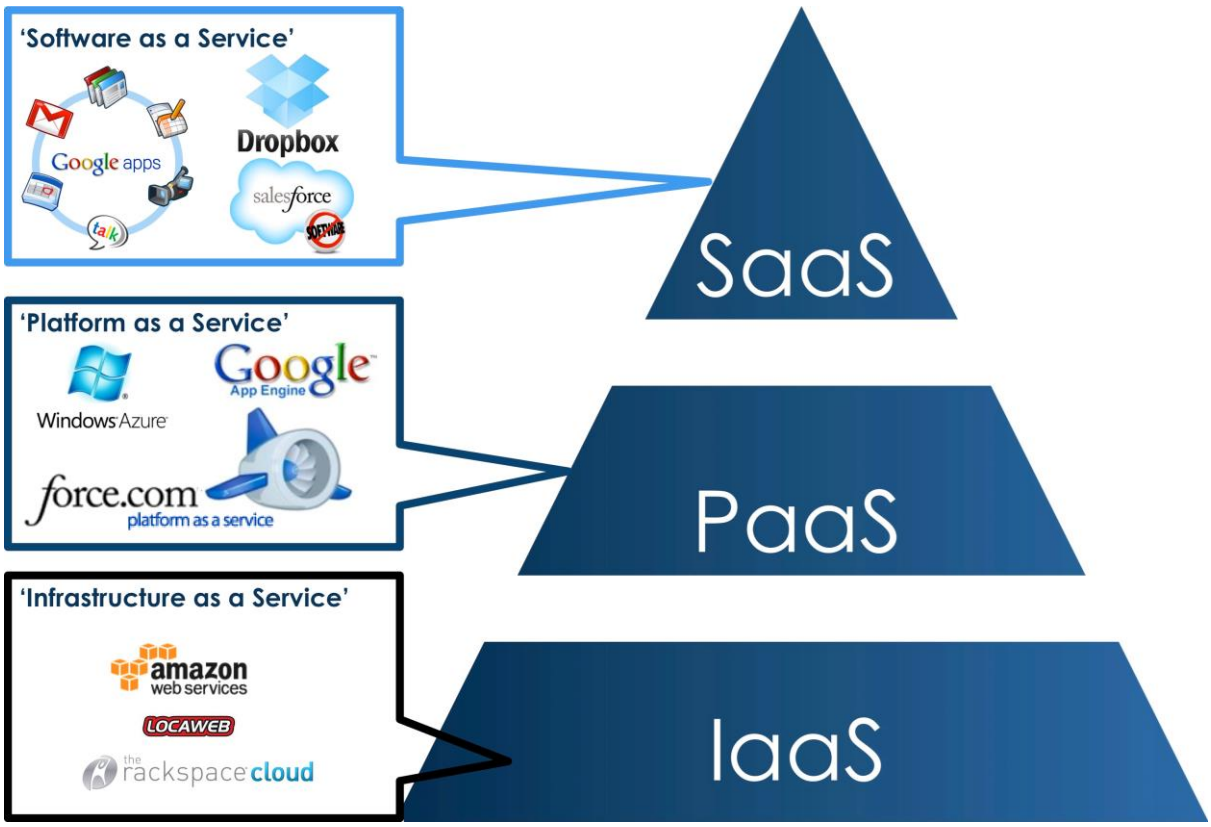

Figura 2.7. Exemplos de serviços de SaaS, PaaS e IaaS (HOST, 2014).

2.4 MODELOS DE IMPLANTAÇÃO

Seja qual for o modelo de serviço for utilizado, SaaS, PaaS ou IaaS, existem quatro modelos de implantação de nuvem: pública, privada, comunitária e híbrida (NIST, 2011). Cada um com seus benefícios de acordo com os objetivos do contratante do serviço de nuvem (Fig. 2.8).

Figura 2.8. Modelos de implantação de nuvem, adaptado de (CSA, 2011).

Embora a computação em nuvem tenha surgido a partir principalmente da oferta de serviços públicos de computação, outros modelos de implantação, com variações na distribuição e localização física, foram adotados. Alguns modelos derivados dos quatro fundamentais estão surgindo no mercado devido à demanda dos clientes e a maturidade das ofertas de mercado. Um exemplo são as nuvens virtuais privadas, que por meio de uma conexão VPN entre o datacenter privado da organização e a nuvem pública, utilizam a infraestrutura de nuvem pública de forma privada (CSA, 2011).

2.4.1 NUVEM PÚBLICA

No modelo público, os serviços são disponibilizados ao público em geral (Fig. 2.9). O provedor de serviços é responsável pela hospedagem, proteção, manutenção e gerenciamento dos dados do cliente, cobrando apenas pelos recursos utilizados, sejam eles infraestrutura física, infraestrutura de aplicação ou softwares, sendo que os clientes não tem controle algum sobre essa infraestrutura (NIST, 2011).

Por suportar múltiplos usuários, um de seus benefícios é a redução de custos, o que a torna uma boa alternativa para empresas que tenham um orçamento restrito, como startups. Entretanto, devido ao seu caráter público e ser compartilhada por diversos clientes, carrega consigo maiores preocupações com segurança.

2.4.2 NUVEM PRIVADA

No modelo privado, os serviços são disponibilizados para o uso exclusivo de uma única organização (Fig. 2.9), sendo gerenciada pela própria empresa ou por terceiros, podendo existir no local ou fora do ambiente da organização. É a própria empresa que cuida da instalação e manutenção da infraestrutura e da plataforma da nuvem (NIST, 2011).

Como a nuvem é mantida em uma rede particular, garante-se uma maior segurança e controle sobre os ativos armazenados. Entretanto, exige maior trabalho de gerenciamento e, consequentemente, maiores gastos.

2.4.3 NUVEM COMUNITÁRIA

No modelo comunitário, os serviços são disponibilizados entre várias organizações de interesses comuns, como segurança, jurisdição, conformidade ou missão, sendo administrados internamente ou por terceiros e podendo ser hospedados internamente ou externamente. (NIST, 2011). Isso faz com que empresas concorrentes possam utilizar a mesma nuvem, tendo seus dados armazenados juntos com os de outros concorrentes pertencentes à comunidade, sendo necessário um cuidado especial em relação à confidencialidade e compartilhamento dos dados utilizados na nuvem (CASTRO e SOUSA, 2010).

Ela pode ser entendida como uma nuvem de nuvens, onde cada parte é acessível pelas organizações que compartilham as infraestruturas que compõem a nuvem completa e os custos são distribuídos por menos usuários do que numa nuvem pública, mas mais do que numa privada.

2.4.4 NUVEM HÍBRIDA

O modelo híbrido caracteriza-se como sendo uma combinação de dois ou mais modelos de implantação de nuvem (pública privada ou comunitária) que permanecem como entidades únicas, mas unidas por tecnologia padronizada ou proprietária (Fig. 2.9), como a *cloud bursting* (ISACA, 2009) para balanceamento de carga entre nuvens, que permite a portabilidade de aplicações e de dados, oferecendo os benefícios da implantação de modelos múltiplos, também chamado de múltiplos sistemas em nuvem (NIST, 2011).

Este modelo permite manter sistemas na nuvem privada e outros na nuvem pública simultaneamente, como em sistemas que manipulam dados confidenciais, que podem ficar na nuvem privada, enquanto outros sistemas, que não lidam com dados sigilosos, na pública (CSA, 2011).

Um fator negativo deste modelo são os riscos em se fundir diferentes formas de implantação.

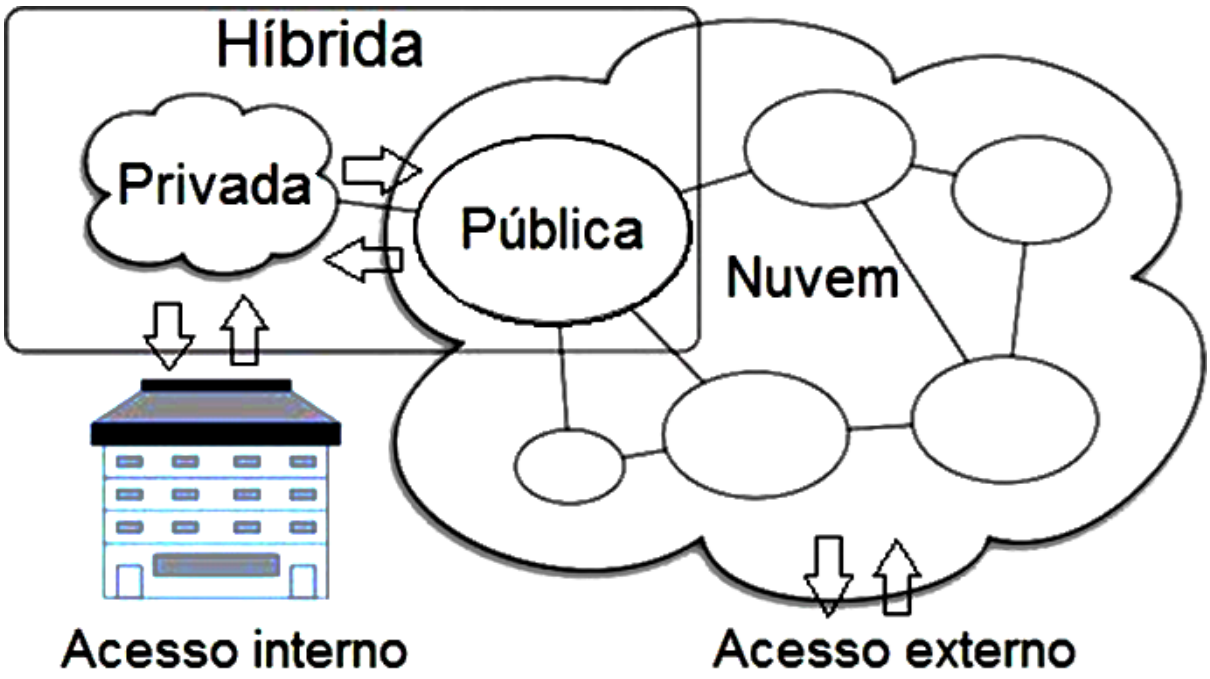

Figura 2.9. Visualização das nuvens pública, privada e híbrida, adaptado de (MATHER *et al*, 2009).

As modalidades de implantação e consumo de nuvem devem ser pensadas não só no contexto do "interno" versus "externo", como em relação à localização física dos ativos, recursos e informações, mas também no contexto de quem são os seus consumidores e de quem é o responsável pela sua governança, segurança e conformidade com políticas e padrões (CSA, 2011). A tabela (2.1) sumariza esses pontos:

Modelo de Implantação	Gerência	Propriedade	Localização	Segurança
Pública	Terceiros	Terceiros	Externa ou Interna	Baixa
Privada	Própria	Própria ou Terceiros	Interna	Alta
Comunitária	Própria ou Terceiros	Própria ou Terceiros	Externa ou Interna	Média
Híbrida	Própria ou Terceiros	Própria ou Terceiros	Externa ou Interna	Média

Tabela 2.1. Comparativo das principais características dos modelos de implantação, adaptado de (CSA, 2011).

2.5 MODELOS DE REFERÊNCIA DE NUVEM

É fundamental entender as relações e dependências entre os modelos da computação em nuvem para compreender os riscos de segurança envolvidos. A IaaS é a base de todos os serviços de nuvem, com a PaaS sendo construído com base na IaaS, e o SaaS por sua vez, sendo construído baseado na PaaS (Fig. 2.10). Desta forma, assim como as capacidades são

herdadas, também são herdadas as questões de segurança da informação e os riscos. 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 (CSA, 2011).

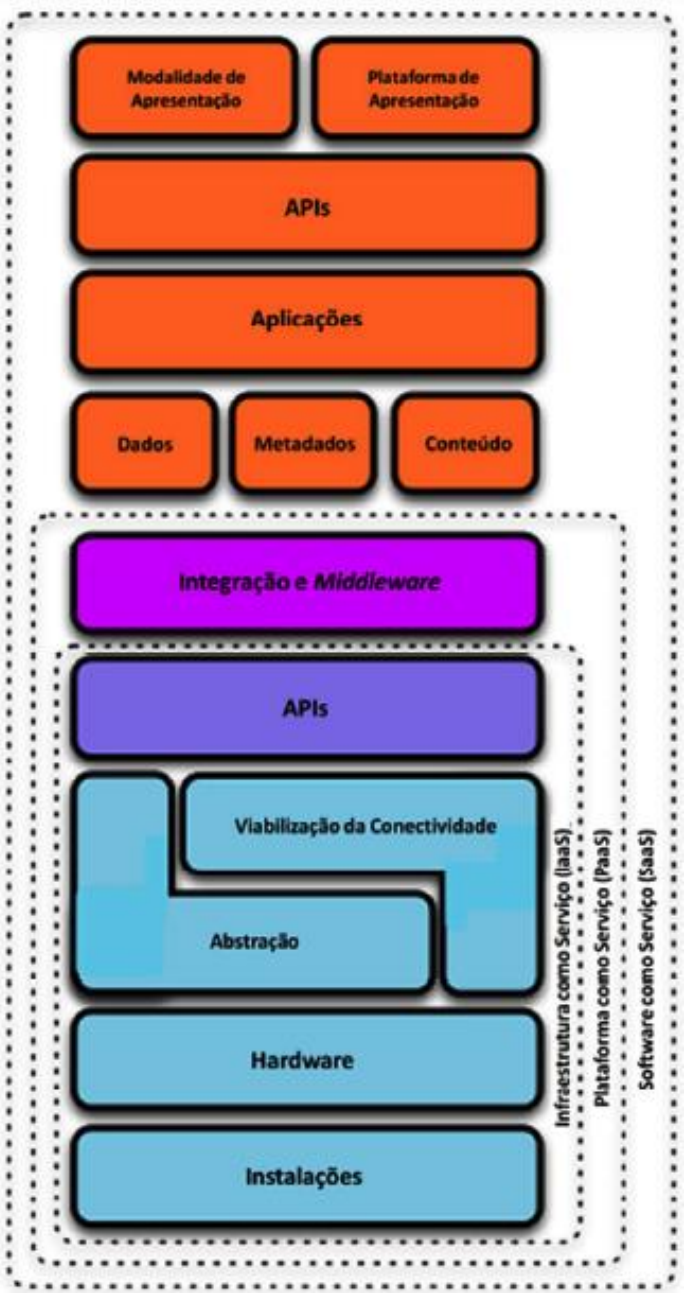

Figura 2.10. Modelo de referência da nuvem, adaptado de (CSA, 2011).

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 ou não os recursos, bem como oferecer conectividade física e lógica a esses recursos. Além disso, a IaaS fornece um conjunto de APIs que permitem aos clientes de nuvem a interação e gestão da infraestrutura (CSA, 2011).

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 (CSA, 2011).

O SaaS por sua vez, é construído sobre as pilhas da 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 (CSA, 2011).

Uma conclusão fundamental sobre a arquitetura de segurança é que quanto mais baixo o serviço contratado estiver na pilha, maior será a responsabilidade do cliente em implementar os recursos de gestão e segurança (Fig. 2.11).

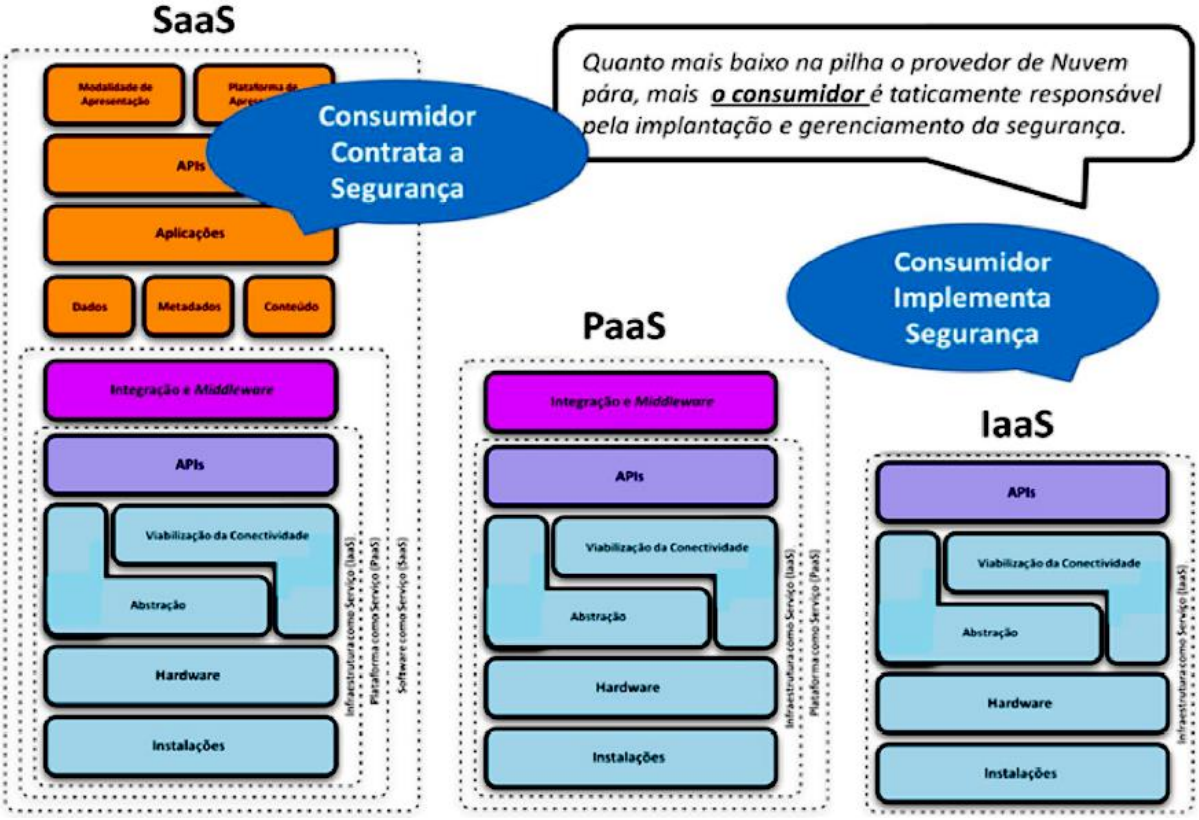

Figura 2.11. Como a segurança é integrada nos modelos de serviço, adaptado de (CSA, 2011).

2.6 ÁREAS CRÍTICAS DE SEGURANÇA DA COMPUTAÇÃO EM NUVEM

Além do domínio da arquitetura, há outros dois grandes domínios, que incluem as doze áreas de atenção crítica na computação em nuvem (CSA, 2011), que serão abordadas no capítulo três, junto com seus principais problemas e preocupações no que tange a segurança

da informação na nuvem. As recomendações para que esses problemas sejam sanados serão apresentadas no capítulo quatro. Os outros dois domínios são: domínio de governança e domínio operacional.

As áreas de governança são amplas e abordam questões políticas e estratégicas dentro de um ambiente de computação em nuvem. As áreas deste domínio são: governança e gestão de riscos corporativos; aspectos legais e descoberta eletrônica; conformidade e auditoria; gerenciamento de informações e segurança dos dados; portabilidade e interoperabilidade.

As áreas operacionais destacam mais as questões táticas de segurança e sua implementação dentro da computação em nuvem. As áreas deste domínio são: segurança tradicional, continuidade de negócios e recuperação de desastres; operações de datacenter; resposta a incidente, notificação e remediação; segurança de aplicações; criptografia e gerenciamento de chaves; gerenciamento de identidade e acesso; virtualização.

3 PROBLEMAS DE SEGURANÇA DA INFORMAÇÃO NA COMPUTAÇÃO EM NUVEM

Neste capítulo são apresentadas as doze áreas de atenção crítica na computação em nuvem e apontados seus principais problemas e preocupações em relação à segurança da informação.

3.1 PRINCIPAIS RISCOS

À medida que cresce a popularidade da computação em nuvem, também aumentam as preocupações relacionadas com as questões de segurança introduzidas através da adoção deste novo modelo. Entretanto, ela tem um tremendo potencial de trazer diversos benefícios para as organizações, dentre eles, a melhoria geral na segurança da informação, já que o objetivo principal do provedor de nuvem é fornecer recursos computacionais, recursos de TIC e informações de forma segura, além de que, os provedores utilizam as melhores práticas de segurança da informação e são especialistas na área, diferentemente da maioria das organizações onde o foco do negócio não é prover um ambiente computacional seguro.

Apesar de trazer economia e novas oportunidades de negócios para as empresas, a nuvem também introduz uma série de novos riscos de segurança da informação à organização. Por isso é importante que se conheça esses riscos associados à nuvem antes de começar a utilizá-la. WINKLER (2011) aponta os seguintes riscos como os principais:

1. **Disponibilidade de rede** - A computação em nuvem precisa de limites mínimos de largura de banda e conectividade de rede para ser utilizada. Ela deve estar disponível sempre que o usuário precisar. Se não estiver, então as consequências não são diferentes de uma situação de negação de serviço.
2. **Perda de controle físico dos dados** - Como os usuários perdem controle físico sobre seus dados e aplicações, isto resulta em inúmeros problemas. Em nuvens públicas ou comunitárias, os dados podem não permanecer no mesmo sistema, levantando várias questões legais. Os dados do usuário podem ser misturados de várias maneiras com os dados de outros. Sendo assim, os clientes precisam de garantias de que seus dados vão ser tratados de forma adequada. . A não observância da forma como os dados são tratados, armazenados, processados, criados e apagados, pode acarretar processos legais e eventuais prejuízos à organização.
3. **Incidentes de segurança** Os clientes precisam ser devidamente informados pelo provedor quando um incidente ocorrer, além de precisam de apoio do provedor para

responder, auditar ou avalia-los. Se isso a for feito, pode acarretar grandes prejuízos à organização.

4. **Continuidade de negócios e recuperação de desastres** - Os usuários de nuvem precisam estar atentos aos planos de continuidade de negócio e recuperação de desastres do provedor. Os usuários devem exigem que suas operações e serviços continuem mesmo se um desastre ocorrer no provedor de nuvem.
5. **Transparência** - O provedor de nuvem deve expor em detalhes sua política de segurança para que o cliente possa analisá-la e garantir que seja adequada a sua própria.
6. **Aspectos legais e regulatórios** - Obter padrões mínimos regulatórios de determinados segmentos de mercado envolvem requisitos não técnicos associados à maturidade da segurança da informação do provedor como um todo.
7. **Viabilidade do provedor de nuvem** - Como os provedores de nuvem são relativamente novos no mercado, ainda existem provedores que obrigam os clientes a utilizarem interfaces proprietárias, o que futuramente podem levá-los a ficarem presos ao provedor ou caso o provedor venha a fechar, o cliente ficará em uma situação difícil para trocar de provedor, pois estará utilizando tecnologia proprietária.

Além desses problemas de segurança da informação, a computação em nuvem apresenta diversos outros que serão apresentados neste capítulo, seguindo as doze áreas elencadas anteriormente pela CSA (2011).

3.2 GOVERNANÇA E GESTÃO DE RISCOS CORPORATIVOS

Esta área trata da capacidade de uma organização em governar e medir os riscos empresariais introduzidos pela computação em nuvem. Alguns dos itens abordados são: como a precedência legal em caso de violação de acordo, a capacidade da organização em avaliar adequadamente os riscos de um provedor de nuvem, a responsabilidade em proteger dados sensíveis quando usuário e provedor falharem, e como as fronteiras internacionais podem afetar estas questões (CSA, 2011).

Devido as suas características essenciais, a nuvem pode alterar todo o modo de uma organização em lidar com TIC, criando novos desafios à governança e gerenciamento corporativo (CSA, 2011). Logo, os processos de governança para nuvem devem ser bem definidos, resultando em programas de gerenciamento de segurança da informação escalonáveis com o negócio, aplicáveis em toda a organização, sustentáveis, defensáveis, mensuráveis, continuamente melhorados e com orçamentos justificáveis.

Um aspecto que a computação em nuvem traz em relação à governança corporativa é a necessidade de prover, em toda a cadeia de fornecimento da informação, um nível satisfatório de segurança da informação (CSA, 2011). Como em nuvens públicas e comunitárias o cliente perde o controle físico dos dados, mesmo que as medidas de segurança sejam tomadas pela organização, toda a segurança será comprometida, caso também não sejam tomadas pelo provedor de nuvem.

A parte fundamental da governança corporativa é o SLA entre cliente e provedor, que pode ser bastante personalizado ou padrão para todos os clientes do provedor.

3.2.1 GOVERNANÇA CORPORATIVA

A governança corporativa é o conjunto de processos, tecnologias, costumes, políticas, leis e instituições afetando o modo que uma empresa é dirigida, administrada ou controlada. Ela também inclui a relação entre os objetivos da organização e as diversas partes interessadas. A boa governança baseia-se na aceitação de que os verdadeiros proprietários da empresa são os acionistas e os membros da gerência são pessoas a quem foi confiado o poder de gerir a organização a fim de gerar lucro aos acionistas (LODI, 2000). Existem diversos modelos de governança corporativa, entretanto, todos seguem cinco princípios básicos:

1. Transparência financeira e divulgação de informação.
2. Auditoria da rede de fornecedores.
3. Conselho e estrutura de gestão e processo.
4. Estrutura de propriedade e exercício dos diretos de controle.
5. Responsabilidade corporativa e cumprimento.

3.2.2 GESTÃO DE RISCOS CORPORATIVOS

As organizações de todas as áreas e tamanhos estão sujeitas a riscos internos e externos que podem afetar o cumprimento dos seus objetivos. Por envolverem algum grau de incerteza, todas as atividades de uma organização apresentam algum tipo de risco. Por isso, se faz necessário o gerenciamento dessas incertezas, dando a organização vantagens competitivas em relação a concorrente. Quando bem implementada, a gestão de riscos proporciona uma melhora na governança corporativa, na descoberta de ameaças e oportunidades, na confiança das partes interessadas, na efetividade e ineficiência operacional, além de aumentar a resiliência da organização minimizando perdas, estabelecer bases sólidas para tomada de decisões e uma gerência proativa (ABNT, 2009).

A gestão de riscos da informação, segundo a norma NBR ISO/DIS 31000 (ABNT,

2009), é ato de identificar e conhecer a exposição aos riscos e a capacidade de gerenciá-los, nivelando pelo desejo e tolerância do proprietário das informações em assumir riscos. Desta forma, para que a migração dos dados, processos ou aplicativos para a nuvem seja bem planejada, é necessário conhecer os riscos associados a ela, a fim de que a organização entenda os riscos a que está sujeita e defina quais está disposta a aceitar, transferir, reduzir e evitar.

A transparência do provedor de nuvem é um item de preocupação que o cliente deve ter. Ele deve reavaliar os processos de governança e gestão de riscos do provedor para assegura que as práticas estejam coerentes e alinhadas às melhores práticas do mercado.

Outra preocupação é a falta de métricas para medir a eficiência e o desempenho do gerenciamento de segurança, além da dificuldade em auditar essas métricas. No geral, a maior parte dos provedores é fechada a auditorias por parte do cliente, não permitindo a realização de testes de penetração e avaliação de vulnerabilidades, tornando bastante difícil, algo fundamental para uma boa gestão de riscos, a descoberta de novas ameaças.

Os principais problemas de segurança da informação na governança e gestão de riscos corporativos na nuvem são:

1. A falta de envolvimento do departamento de segurança da informação para o estabelecimento dos SLAs.
2. A falta de métricas bem definidas para medir o desempenho do gerenciamento de segurança da informação.
3. A falta de conhecimento por parte do cliente de quais os controles de segurança são empregados pelo provedor de serviço e seus fornecedores.
4. A falta de conhecimento do cliente de nuvem quanto à rede de fornecedores do seu provedor de serviço.
5. O cliente geralmente não faz o gerenciamento de riscos específico para a nuvem, levando a organização a desconhecer as ameaças e os critérios de aceitação dos riscos.
6. Os provedores de nuvem com negócios imaturos e pouco resilientes podem levar a interrupções inesperadas de serviços acarretando prejuízos.

3.3 ASPECTOS LEGAIS E DESCOBERTA ELETRÔNICA

Esta área trata de problemas legais na utilização da computação em nuvem. Os assuntos abordados incluem os requisitos de proteção da informação e de sistemas informáticos, leis de

divulgação de violações de segurança, os requisitos regulatórios, requisitos de privacidade, as leis internacionais, etc. (CSA, 2011).

Principalmente em nuvens públicas ou comunitárias, a computação em nuvem transforma a dinâmica no relacionamento entre a organização e suas informações, já que envolve a presença de um terceiro, o provedor de nuvem, que tem a custódia das informações. Isto cria novas questões em relação ao entendimento de como as leis se aplicam.

A conformidade é um dos principais problemas da computação em nuvem. Ao utilizar dos serviços da nuvem, a organização fica receosa de sofrer algum processo legal ou receber multas em virtude da possível perda de conformidade (WINKLER, 2011).

A descoberta eletrônica consiste no processo de coletar, preservar e analisar informações digitais para serem usadas como evidências em processos litigiosos ou investigações (ROUSE, 2010). Em virtude da natureza dinâmica e distribuída, os serviços de nuvem dificultam a descoberta eletrônica. Além disso, há ainda o problema da multilocação, já que a descoberta eletrônica deve ser realizada de modo que informações de outros clientes do provedor não sejam expostas ao se coletar informações sobre um determinado cliente (CSA, 2011). Por isso, o provedor de nuvem deve utilizar uma forte compartimentalização para evitar o vazamento de informações de empresas não investigadas ou envolvidas em processos litigiosos.

A virtualização traz também o problema da possibilidade da ocorrência de trocas de informações em uma rede virtual que muitas vezes não possuí registro das ações ou sistemas de log (VMWARE, 2009).

Os processos de término de contratos, se não forem definidos em contrato, podem causar interrupções nos serviços e até a perda das informações sem que o provedor seja punido. O provedor que não presta mais serviços à organização pode também se negar a disponibilizar os dados que estavam em sua posse. (CSA, 2011). Por isso, antes mesmo da adoção de um provedor de nuvem, é preciso prever como será o fim da relação de prestação de serviços, tudo devendo estar definido em contrato.

Muitos dados, como números de cartões de crédito, não podem ser expostos a terceiros ou utilizados com propósitos diferentes e a adesão à nuvem torna a preocupação com a privacidade dos dados ainda maior, além de ser comum vários clientes dividindo a mesma infraestrutura física. Cabe ao provedor à responsabilidade de garantir que os dados armazenados não sejam acessados indevidamente ou expostos, apesar de que a organização que os armazenou na nuvem é quem sofrerá os processos legais. Assim sendo, deve ser

definido em contrato que, em caso de vazamento de dados com implicações de processos litigiosos, o provedor de nuvem que deverá arcar com os custos, além de dar garantias de que os dados serão armazenados, processador e movimentados de forma que sua privacidade seja assegurada (MATHER *et al*, 2009).

Outro aspecto que requer atenção é a localização física dos dados, já que varias organizações, como as governamentais, não podem ter seus dados armazenados fora dos países de origem. Deve ser acordado em contrato que os dados ficarão armazenados em uma determinada região ou país, devido ao fato de que os dados na nuvem podem ser armazenados em inúmeros datacenters espalhados em países pelo mundo. O mesmo vale para os backups das informações (MATHER *et al*, 2009).

Os principais problemas de segurança da informação nos aspectos legais e descoberta eletrônica na nuvem são:

1. As cláusulas de término de prestação de serviço mal definidas.
2. A falta de garantias contratuais quanto a vazamentos de dados confidenciais.
3. A localização dos dados armazenados nos provedores de nuvem não definida em contrato.
4. Os papéis de responsabilidade mal definidos.
5. Os procedimentos mal definidos de resposta a intimações judicias para descoberta de dados.

3.4 CONFORMIDADE E AUDITORIA

Esta área trata da manutenção e comprovação de conformidade na computação em nuvem. Questões relativas à avaliação da forma como a nuvem afeta o cumprimento das políticas de segurança interna, bem como diversos requisitos de conformidade regulatórios, legislativos e outros são discutidos. Este domínio inclui algumas orientações de como provar a conformidade durante uma auditoria (CSA, 2011).

A conformidade e auditoria são processos internos e externos com o propósito de apontar os requisitos especificados, como regulações, leis e contratos com clientes, que a organização deve atender. Também abrangem a implementação e monitoramento de processos, sistemas e políticas com o intuito de que a organização cumpra todos os requisitos legais e contratuais acordados ou a que está sujeita (MATHER *et al*, 2009).

No modelo tradicional de terceirização, a conformidade e auditoria têm um papel

importante. Na computação em nuvem, essa importância é ainda maior por causa da natureza dinâmica dos serviços de nuvem. O provedor de nuvem tem que instaurar, monitorar e demonstrar conformidade junto com um conjunto de controles que atendam as exigências regulatórias do cliente. Uma abordagem prática para conformidade e auditoria na nuvem engloba uma união coordenada de política interna de conformidade, conformidade regulatória, e auditoria externa. Assim, o provedor de nuvem deve conhecer os requisitos regulatórios de todos seus clientes e implementar os processos, sistemas e políticas necessários para atender esses requisitos (MATHER *et al*, 2009).

O cliente deve então verificar a capacidade do provedor de nuvem em produzir provas de que atende os requisitos de conformidade, além de saber quais responsabilidades são suas e quais são do provedor de nuvem quanto à conformidade.

Os seguintes padrões de conformidade para a nuvem já estão em desenvolvimento pela ISO/IEC e ITU-T:

- 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* (ISO, 2014).
- ISO/IEC 27017: *Cloud Computing Security and Privacy Management System-Security Controls* (ISO, 2015).
- 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 SaaS application environment.*

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

1. A falta de conhecimento de quais controles de segurança são de responsabilidade do cliente e quais são do provedor.
2. A falta da demonstração de conformidade por parte do provedor de nuvem.
3. A falta de análise de como o serviço de nuvem contratado impacta na conformidade.
4. Provedores fechados a auditorias por parte do cliente.

3.5 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DOS DADOS

Esta área trata do gerenciamento dos dados colocados na nuvem. Itens em torno da identificação e controle de dados na nuvem, bem como controles compensatórios que podem ser usados para lidar com a perda de controle físico ao migrar dados para a nuvem, além de itens, como quem é responsável pela confidencialidade, integridade e disponibilidade dos dados (CSA, 2011).

Ao migrar para a computação em nuvem, a organização pode acessar suas informações de praticamente qualquer dispositivo com um navegador Web, como notebooks, smartphones, tablets, e estações de trabalho. O gerenciamento e a segurança desses dados e informações em conjunto com a rápida elasticidade, multilocação e onipresença da nuvem, são atividades desafiadoras que requerem novos planos de segurança (CSA, 2011).

Saber como a nuvem influência cada uma das seis fases do ciclo de vida da segurança dos dados - criar, armazenar, utilizar, distribuir, arquivar e destruir - é de extrema necessidade para assegurar a segurança dos dados na nuvem adequadamente (MOGULL, 2011). Por isso, se faz necessário adotar medidas para preservar a confidencialidade dos dados, como a utilização de criptografia em todas as fases.

Outra preocupação em relação à segurança dos dados, além da criptografia, é sobre o acesso às informações. Como a nuvem permite acessar as informações de qualquer dispositivo e lugar do mundo, para assegurar a segurança das informações, deve-se investir em controles rígidos de acesso.

O armazenamento dos dados também é outro item importante que merece atenção, já que se os dados forem agrupados segundo um padrão e ele for identificado, ainda que os dados estejam criptografados, informações sobre os dados seriam reveladas.

Tão imprescindível quanto à segurança dos próprios dados, é a segurança dos backups, visto que são nada mais que cópias dos dados originais. Dessa maneira, devem também ser criptografados e possuir um forte controle de acesso. A recuperação de dados exige cuidados em relação à velocidade com que os dados perdidos são recuperados para não prejudicar processos e serviços que estejam utilizam estes dados.

A exclusão dos dados também requer atenção, visto que como em nuvens públicas e comunitárias o cliente perde o controle físico dos dados, é necessário assegurar que os dados que ele mandou excluir realmente foram excluídos.

Os principais problemas de segurança da informação no gerenciamento de informações e segurança dos dados na nuvem são:

1. A má utilização da criptografia.

2. Os dados de diferentes clientes misturados no mesmo provedor de nuvem.
3. Os dados armazenados em locais desconhecidos pelo cliente de nuvem.
4. A falta de controles apropriados na transferência de dados para dentro e para fora da nuvem.
5. A falta de conhecimento da arquitetura em que os dados são armazenados.
6. A não exclusão dos dados pelo provedor, mesmo que tenha sido feita pelo cliente.

3.6 PORTABILIDADE E INTEROPERABILIDADE

Esta área trata da habilidade em migrar dados e serviços de um provedor de nuvem para outro, ou levá-lo totalmente de volta para a empresa. Problemas de interoperabilidade entre os fornecedores também são discutidos (CSA, 2011).

Portabilidade e interoperabilidade oferecem uma escalabilidade sem precedentes para a nuvem, já que os serviços utilizados podem ser distribuídos através de diversos provedores de nuvem, além de permitirem a migração de serviços de um provedor para outro sem que eles precisem ser alterados (CSA, 2011). Ao utilizar serviços com essas características, o usuário tem a liberdade de migrar entre provedores em busca daquele que melhor atende as suas necessidades. No entanto, a falta de portabilidade e interoperabilidade pode deixar o cliente refém do provedor e de suas tecnologias utilizadas.

.O uso de e tecnologias e protocolos proprietários pode fazer com que o cliente fique preso ao provedor de serviço (CSA, 2011). O provedor de nuvem deve utilizar arquiteturas e protocolos padrões e abertos para que, caso o cliente queira migrar o serviço oferecido para outro provedor, a migração seja simples, sem que o cliente tenha que remodelar os processos e aplicações para funcionarem no novo provedor.

Os principais problemas de segurança da informação na portabilidade e interoperabilidade na nuvem são:

1. Processos de migração mal definidos.
2. O uso de tecnologias proprietárias, o que pode levar o cliente a ficar preso a um determinado provedor de serviços de nuvem.

3.7 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

Esta área trata de como a computação em nuvem afeta os processos e procedimentos

operacionais usados para implementar a segurança, continuidade de negócios e recuperação de desastres. O foco é discutir e analisar os possíveis riscos da computação em nuvem, na esperança de aumentar o diálogo e debate sobre a grande procura de melhores modelos de gestão de riscos corporativos. Além disso, a seção aborda sobre como identificar onde a computação em nuvem pode ajudar a diminuir certos riscos de segurança, e onde implica no aumento dos riscos em outras áreas (CSA, 2011).

É fundamental conhecer os modelos e mecanismos de segurança tradicional, plano de negócios e recuperação de desastres do provedor de nuvem. Segurança tradicional na nuvem compreende a segurança física e a do ambiente. Ela é tratada na seção 9 da norma NBR ISO/IEC 27002 (ABNT, 2013). Nesta seção são mostrados os principais problemas quanto à segurança tradicional, continuidade de negócios e recuperação de desastres no que diz respeito à computação em nuvem hoje.

A segurança física e a do ambiente compreendem a prevenção ao acesso não autorizado, danos e interferências às instalações, equipamentos e informações da organização. Mesmo a nuvem sendo um modelo diferente de computação, distribuído, a segurança não é diferente, já que a infraestrutura física, como os datacenters, encontra-se ainda em algum lugar. Em nuvens publicas e comunitárias, a segurança física deve ser ainda mais robusta, uma vez que nessas nuvens encontram-se dados críticos e sigilosos de diversas organizações e pessoas (ABNT, 2013).

O provedor de nuvem deve está em acordo com padrões globais de segurança da informação, como a norma NBR ISO/IEC 27001 (ABNT, 2013) ou outros padrões da indústria, como COBIT, COSO, ITIL, SABSA e TOGAF. Assim, o provedor da garantias de que emprega as melhores praticas e técnicas na gerência de TIC e segurança da informação (CSA, 2011).

Uma preocupação fundamental que o provedor deve ter é em relação aos seus funcionários. Como a custodia dos dados é do provedor, é imprescindível atentar-se aos processos de checagem do passado dos funcionários, seus papeis e responsabilidades, os contratos de emprego e os processos de demissão (CSA, 2011). Um enfoque maior deve ser dado a este último, devido a um possível descontentamento por parte do funcionário, que se ainda tiver algum tipo acesso aos dados, pode provocar sérios danos ao provedor e seus clientes por vingança.

Alguns provedores de nuvem não são transparentes e não permitem auditorias e testes em seus planos de continuidade de negócios e recuperação de desastres (CSA, 2011). Isso deixa o cliente receoso com o que possa vir a ocorrer em caso de desastre no provedor, como

dados serem perdidos, movidos para datacenters em outra localidade ou serviços serem interrompidos. Por isso, o plano de recuperação de desastres do provedor deve estar descrito em contrato.

Os principais problemas de segurança da informação na segurança tradicional, continuidade de negócios e recuperação de desastres na nuvem são:

1. Processos de recuperação de desastres mal definidos nos SLAs.
2. O plano de continuidade de negócios do provedor muitas vezes é desconhecido pelo cliente.
3. O cliente de nuvem com pouca abertura para fazer inspeções e auditorias nos processos e instalações do provedor.
4. O cliente de nuvem tem pouco ou nenhum conhecimento sobre os controles de segurança empregado pelo provedor de nuvem.

3.8 OPERAÇÕES DE DATACENTER

Esta área trata de como avaliar a arquitetura e a operação de um fornecedor de datacenter. Ela foca principalmente em ajudar o usuário a identificar características comuns de datacenters que podem ser prejudiciais para os serviços em andamento, bem como características que são fundamentais para a estabilidade em longo prazo (CSA, 2011).

À medida que mais e mais consumidores e empresas migram para a nuvem, o número de provedores de nuvem também aumenta. Para atender a esta demanda, os provedores de todos os tipos e tamanhos fazem investimentos grandes em datacenters e o cliente de nuvem deve prestar atenção em como as características essenciais da nuvem são implementadas nos datacenters pelo provedor, uma vez que, se forem feitas sem considerarem a segurança da informação, o plano de segurança estará prejudicado desde a sua infraestrutura física (CSA, 2011). Dito isto, é fundamental conhecer os controles de segurança que o provedor utiliza nos datacenters antes do cliente ou organização migrar para a nuvem.

Outra questão para o provedor é de evidenciar ao cliente que esses novos datacenters estão em concordância com os seus requisitos de conformidade, e também, de dar a oportunidade de auditar seus datacenters para assegurar que as práticas de segurança empregadas estejam em harmonia com a sua política de segurança.

A localização dos datacenters é um item fundamental para a migração para a nuvem, por existirem clientes e organização que não podem ter seus dados armazenados em

datacenters em determinados países ou regiões, a localização dos datacenters do provedor deve também ser analisada.

Os principais problemas de segurança da informação na operação de datacenter na nuvem são:

1. A falta de conhecimento do local do datacenter.
2. O provedor de nuvem geralmente coloca entraves para a realização de auditorias em seus datacenters.
3. O cliente de nuvem geralmente tem pouco ou nenhum conhecimento de como as características essências da computação em nuvem são implementadas e como se dá o compartilhamento dos recursos.

3.9 RESPOSTA A INCIDENTE, NOTIFICAÇÃO E REMEDIAÇÃO

Esta área trata da adequada e correta detecção de incidentes, a resposta, notificação e correção. Itens que devem estar presentes tanto no provedor, quanto no usuário para permitir bom tratamento de incidentes e forenses computacional. Este domínio ajuda a compreender as complexidades que a nuvem traz para o programa de gestão de incidentes da organização (CSA, 2011).

Como nem com o melhor planejamento de segurança existente é possível eliminar completamente a ocorrência de falhas, a resposta a incidente é um item essencial no plano de segurança, por isso é imprescindível saber o que fazer quando ocorre um incidente.

Pela sua característica sob demanda, ambientes de nuvem podem dificultar a cooperação do provedor de nuvem em casos de incidente de segurança. Por isso, é fundamental que situações como essa estejam previstas em contrato, já que a assistência dada pelo provedor pode variar bastante de um caso para outro (CSA, 2011).

O agrupamento de recursos junto com a rápida elasticidade da nuvem pode prejudicar baste à resposta a incidente também, especialmente a atividade de análise forense devido ao ambiente altamente dinâmico da nuvem que desafia as necessidades básicas forenses, que é analisar o ocorrido em um cenário igual ao do incidente (CSA, 2011).

O agrupamento de recursos também pode causar problemas de privacidade. A análise de incidente feita através da verificação de logs, armazenamento, memória ou fluxo de rede, por exemplo, pode expor informações sobre coinquilinos, usuários de nuvem que compartilham dos mesmos recursos físicos, mas utilizam instâncias virtuais diferentes. Desse modo, o

provedor e o cliente de nuvem devem estar atentos a apenas revelarem os dados essenciais para a análise do incidente ocorrido na instância do usuário, sem que ocorra a exposição de informações dos coinquilinos (CSA, 2011).

A localização dos dados armazenados no provedor de nuvem pode ter influência no que possa não ser feito na ocorrência de um incidente. Como os dados podem ser transferidos para outra região ou até mesmo outro país com leis diferentes, os contratos de serviço devem tratar da região ou país onde os dados e as máquinas virtuais serão armazenados (CSA, 2011).

É necessário que contratos de serviços sejam bem definidos, e que tratem da questão do armazenamento de dados ou máquinas virtuais em regiões geográficas nas quais leis diferentes são aplicadas.

Os principais problemas de segurança da informação na resposta a incidente, notificação e remediação na nuvem são:

1. Papéis mal definidos entre cliente e servidor na resposta a incidente.
2. A falta de formalização da definição do que é um incidente para a organização cliente.

3.10 SEGURANÇA DE APLICAÇÕES

Esta área trata da proteção ao *software* aplicativo executado ou desenvolvido na nuvem. Isto inclui itens como, se é apropriado migrar ou projetar um aplicativo para ser executado na nuvem, e em caso afirmativo, que tipo de modelo de serviço em nuvem é mais adequado: SaaS, PaaS ou IaaS. Algumas questões de segurança específicas relacionadas com a nuvem também são discutidas (CSA, 2011).

Desde o seu desenvolvimento até sua desativação, existem particularidades nas aplicações que rodam na nuvem. As aplicações devem ter todos os controles de segurança implementados, como se estivesse em uma rede totalmente carente de segurança, o que torna um desafio para os desenvolvedores. Entretanto, a aplicação na nuvem estará vulnerável a ameaças diferentes das encontradas em ambientes costumeiros. A criptografia e multilocação também necessitam de atenção e devem ser discutidas desde o inicio da concepção da aplicação.

A compatibilidade da aplicação entre provedores gera uma grande preocupação. É primordial que os desenvolvedores utilizem tecnologias abertas ou padrões para garantirem que ela possa ser migrada de um provedor para o outro sem que haja necessidade de grandes alterações (CSA, 2011). Outro item bastante desafiador é a conformidade da aplicação na nuvem, como descrito anteriormente.

A proteção aos dados deve ser levada em conta também no desenvolvimento da aplicação e como eles serão armazenados, trocados e processados a fim de se garantir a integridade, confidencialidade e disponibilidade. É de extrema importância determinar quais dados serão criptografados pela aplicação e quando. A forma de acesso aos logs deve estar definida nos SLAs, especialmente em nuvens públicas onde os logs podem estar espalhados em diversas máquinas físicas (CSA, 2011). O cliente deve estar ciente dos novos riscos em potencial devido ao acesso de informações sensíveis que vão estar na aplicação na nuvem.

Sistemas de gerência de acesso e identidade estão diretamente relacionados com funções importantes da aplicação, como a parte de cobranças, e devem ser integrados a aplicação (CSA, 2011).

Os principais problemas de segurança da informação na segurança de aplicações na nuvem são:

1. A possibilidade de um ataque de negação de serviço, geralmente devido a múltiplas conexões maliciosas.
2. A falta de controle sobre políticas e controles de segurança.
3. A falta de visibilidade sobre os controles de segurança e sua efetividade.
4. A falta de gerenciamento da segurança da aplicação que se encontra na Web, principalmente quanto às políticas de acesso e auditoria.
5. A perda de governança.
6. O risco de uma organização não atender os requisitos de conformidade que foram alteraram devido à inflexibilidade do provedor.
7. Falha de isolamento. Empresas concorrentes com aplicações em uma mesma infraestrutura podem ter informações acessadas ou manipuladas por coinquilinos.
8. A perda de proteção dos dados devido a uma falha no armazenamento dos dados ou das chaves que os criptografam.
9. O risco do comprometimento das interfaces de gerência e controle de acesso.

3.11 CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES

Esta área trata de identificar o uso de criptografia e gerenciamento de chaves escalável. Ela não é prescritiva, mas é mais informativa em discutir por que eles são necessários e identificar as questões que surgem na utilização, tanto para proteger o acesso aos recursos,

quanto os dados (CSA, 2011).

Sendo a nuvem geralmente compartilhada por muitos multilocatários, o provedor tem a necessidade de proteger os dados do cliente contra roubos, vazamentos ou acessos não autorizados. Empresas concorrentes compartilhando o mesmo servidor físico pode ocasionar sérios prejuízos a uma empresa, caso a concorrente consiga acesso às informações da outra (CSA, 2011). Mesmo em nuvens privadas, onde a segurança é mais alta, é fundamental a criptografia dos dados, já que os dados de determinados departamentos ou usuários não devem ser vistos por outros. Estando em uso, movimento ou ociosos, os dados na nuvem devem ser criptografados para evitar o comprometimento de informações sigilosas.

O provedor e o cliente de nuvem devem ter atenção sobre os protocolos utilizados na criptografia dos dados, estando atentos a novas falhas que possam surgir (CSA, 2011). Criptografar os dados exige maior utilização de processamento, o que pode acarretar problemas no desempenho. Por isso, a organização deve avaliar se os dados precisam ser criptografados.

Um gerenciamento de chaves apropriado também é de extrema importância, já que se as chaves forem comprometidas, os dados criptografados também serão (CSA, 2011). Por isso, os repositórios de chaves na nuvem devem ser tão bem protegidos quanto outros repositórios de informações sensíveis, empregando um forte controle de acesso restrito às chaves individuais necessárias.

Também é de extremamente necessário que se faça backup das chaves e meios para que esta possa ser recuperada em caso de perda ou corrompimento, já que se a chave for perdida ou corrompida, os dados criptografados também serão, uma vez que não poderão mais ser descriptografados (CSA, 2011). As mídias de backup merecem tanto cuidado em relação à segurança quanto as originais, dado que contêm cópias das informações originais.

Os principais problemas de segurança da informação na criptografia e gerenciamento de chaves na nuvem são:

1. A gerência de chaves ruim, resultando no comprometimento ou perda de chaves.
2. O uso de padrões criptográficos inseguros.
3. O uso de algoritmos criptográficos proprietários, que podem não ser suportados por outros provedores, podendo resultar na necessidade de reestruturação de aplicações e processos em caso de mudança de provedor.

3.12 GERENCIAMENTO DE IDENTIDADE E ACESSO

Esta área trata do gerenciamento de identidade e promoção dos serviços de diretório para fornecer controle de acesso. O foco está em questões encontradas quando se pretende migar a identidade de uma organização para a nuvem. Ela fornece critérios para avaliar a prontidão da organização para realizar a gestão da identidade e acesso baseados na nuvem (CSA, 2011).

Dependendo do modelo de serviço escolhido, o controle das aplicações, da infraestrutura ou dos sistemas pode ser transferido para o provedor de nuvem, criando um desafio em relação aos controles de governança confiáveis já estabelecidos. Uma forma de equilibrar essa perda do controle sobre os elementos de baixo nível, como infraestrutura e rede, é a utilizações desses controles em níveis mais altos, como as aplicações, com uma forte autenticação pelos clientes (CSA, 2011). Três pontos são fundamentais para o gerenciamento de identidade e acesso eficaz: concessão de identidade, autenticação e federação.

Um dos maiores problemas para a adoção da computação em nuvem é o gerenciamento ágil e seguro da concessão e revogação de identidade aos usuários na nuvem. Outro problema é a autenticação de usuários de um jeito gerenciável e confiável, o que na exige um bom gerenciamento de credenciais, delegação de autenticação, forte autenticação, e gerenciamento de segurança (CSA, 2011).

O gerenciamento de identidade federada tem uma parte essencial na gerência de identidade e acesso por possibilitar que organização autentique os usuários utilizando um provedor de identidade (CSA, 2011). Apesar de trazer vários benefícios, essa estrutura de autenticação centralizada deve ser muito bem gerida, visto que se esta for comprometida, todo o processo de autenticação também será.

Os principais problemas de segurança da informação no gerenciamento de identidade e acesso na nuvem são:

1. A autenticação por canais inseguros, o que pode resultar no roubo de dados de acesso.
2. O uso de repositórios de identidade que não suportem aplicações e processos na nuvem.
3. O uso de tecnologias proprietárias.

3.13 VIRTUALIZAÇÃO

Esta área trata do uso da virtualização na computação em nuvem. São abordados itens como os riscos associados à multilocação, o isolamento e co-residência de VMs, e vulnerabilidades no hypervisor. É dado foco nas questões de segurança em torno do sistema e *hardware* de virtualização, em vez de um levantamento mais geral de todas as formas de

virtualização (CSA, 2011).

Ainda que não seja uma característica essencial da nuvem, a virtualização atualmente é um dos itens fundamentais em nuvens privadas e na IaaS, e vem sendo cada vez mais empregada no plano de fundo de provedores de SaaS e PaaS. É também, naturalmente, uma tecnologia chave em áreas de trabalho virtuais, muito utilizadas em nuvens privadas e públicas (CSA, 2011). Como a multilocação na aplicação, plataforma e infraestrutura também é feita pela virtualização, é importante saber os riscos introduzidos por ela na nuvem.

A multilocação e a melhor utilização da infraestrutura física são uma das vantagens da virtualização (CSA, 2011). Com ela, o cliente tem uma redução no capital gasto na compra de *hardware*, como servidores, aumentando a eficiência operacional.

Entretanto, a virtualização não traz só benefícios, mas também todas as preocupações de segurança de um sistema operacional rodando como hospedeiro, além de novas, como sobre a camada de *hypervisor* (VMWARE, 211).

Os principais problemas de segurança da informação na virtualização na nuvem são:

1. **Falta de segurança do *hypervisor*** - É necessário trancar e fortalecer o *hypervisor* utilizando as melhores práticas de segurança. A preocupação fundamental que usuários de virtualização e empresas devem ter é de gerenciar as configurações e operações do *hypervisor* apropriadamente, além da segurança física do servidor onde é hospedado.
2. **Proteção inadequada de máquinas virtuais hospedeiras** - Consiste em instalar todos os mecanismos de proteção necessários em um servidor, como firewalls e antivírus, na máquina virtual. Máquinas virtuais mal protegidas podem levar a indisponibilidade no serviço.
3. **Ataques inter-VM e pontos cegos** - A virtualização tem um profundo impacto na segurança de redes. Como as máquinas virtuais podem ser comunicar através de um plano de fundo do hardware, em vez da rede, isso faz com que os controles de segurança de redes padrões não controlem esse tráfego. É necessário monitorar esse tráfego de dados entre as máquinas virtuais também.
4. ***Instant-on gaps*** - A facilidade com que uma máquina virtual pode ser parada ou iniciada, combinado com a velocidade com que as ameaças evoluem, cria uma brecha na segurança, onde uma máquina virtual está configurada seguramente quando é desligada, mas quando é iniciada novamente, as ameaças evoluíram, deixando a vulnerável.

5. **Aumento da complexidade operacional do VM *Sprawl*** - Devido à facilidade com que as máquinas virtuais podem ser providenciadas, há uma crescente no número de pedidos nas empresas. Se não existir uma gerência adequada desse grande número de máquinas virtuais pela empresa, cria-se uma superfície maior para ataques, além de aumentar as chances de uma configuração ou operação mal feita, abrindo uma brecha na segurança.
6. **Criptografia de máquinas virtuais** - Quando estão inativas ou até mesmo rodando, as máquinas virtuais são vulneráveis a modificações e até a roubos. Por isso, elas devem ser criptografadas, estando em uso ou inativas. Entretanto, isso traz problemas quanto ao desempenho. Caso o ambiente necessite de alta segurança, essa perda de desempenho é compensadora. Já se o desempenho no ambiente for necessário, a criptografia pode não ser interessante.
7. **Não destruição de dados da máquina virtual** - O cliente de nuvem precisa de garantias do provedor de que nenhum bit sequer vá ser deixado no disco do servidor físico anterior, quando uma máquina virtual for movida de um servidor físico para outro, evitando que algum dado possa ser recuperado por alguém de alguma forma.
8. **Adulteração de máquinas virtuais** - Imagens de máquinas virtuais pré-configuradas podem ter sido mal configuradas ou adulteradas antes de serem iniciadas, expondo o cliente a diversas ameaças.
9. **Máquinas virtuais em movimento** - Mover máquinas virtuais de um servidor físico para outro traz dificuldades ao monitoramento de segurança e à auditoria. Em muitos casos, as máquinas virtuais podem ser realocadas em outro servidor físico sem que um alerta seja disparado ou uma trilha criada para que possa ser auditada. O cliente de nuvem deve saber se o provedor possui alertas e controles para gerenciar essa movimentação.
10. **Mistura de dados** - Devido ao fato de compartilharem da mesma infraestrutura física, dados de diferentes máquinas virtuais podem ser misturados. Por isso, as máquinas virtuais e seus fluxos de dados devem se isolados.
11. **Preocupação quanto ao desempenho** - Instalar programas feitos para servidores físicos, como antivírus, em servidores virtuais pode ocasionar em grande perda de desempenho, já que tarefas de segurança, como a varredura do antivírus, consomem muito da CPU. Em ambientes virtualizados, cliente e provedor devem usar ferramentas próprias para este ambiente, evitando a perda de desempenho.

4 RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO NA COMPUTAÇÃO EM NUVEM

Neste capítulo são feitas recomendações de segurança para as áreas críticas de segurança da computação em nuvem mostradas no capítulo anterior. As recomendações se baseiam em livros, artigos, estudos de caso, publicações, periódicos e normas técnicas da ISO, ABNT, IEEE e, principalmente, no guia da CSA de 2011.

4.1 GOVERNANÇA E GESTÃO DE RISCOS CORPORATIVOS

Aqui são apresentadas diretrizes de gestão de riscos apenas no que se refere à computação em nuvem baseadas nas normas NBR ISO/DIS 31000 (ABNT, 2009), ISF e ISACA.

As recomendações são:

1. O cliente de nuvem deve investir uma parte da redução de custos decorrente da adoção da computação em nuvem no 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.
2. Tanto o cliente quanto o fornecedor de serviços de computação em nuvem devem criar uma governança de segurança da informação robusta, independentemente do serviço ou modelo adotado. Ela deve ser uma colaboração entre clientes e fornecedores para alcançar os objetivos acordados.
3. O cliente de nuvem deve incluir a revisão de determinadas estruturas e processos 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 do fornecedor devem ser avaliados sob sua capacidade de suportar os processos do cliente, bem como sua coerência e maturidade com os processos de gestão de segurança de informações. Os controles de segurança dos provedores de nuvem devem claramente suportar estes processos de gestão e serem comprovadamente baseados no risco.
4. A estrutura e os processos de governança colaborativa entre clientes e fornecedores devem ser tratados como fundamentais tanto na avaliação de risco e de serviços, e protocolos de gestão de riscos, quanto no âmbito da concepção e desenvolvimento de

prestação de serviços, então integrados nos SLAs.

5. O departamento de segurança do cliente deve estar presente durante a definição dos SLAs, e obrigações contratuais, para assegurar que os requisitos de segurança sejam contratualmente aplicáveis.
6. O cliente de nuvem deve fixar padrões e métricas para mensurar o desempenho e eficácia do gerenciamento de segurança da informação antes de migrar para a nuvem. Além disso, entender e documentar as métricas atuais e como elas podem mudar com a migração para a nuvem, onde são usadas métricas diferentes.
7. Sempre que for possível, devem-se incluir padrões e métricas documentados e auditáveis de segurança em qualquer SLA, e contratos. Estas métricas e padrões devem ser documentados e auditados.
8. A abordagem de gerenciamento de riscos no uso de serviços de nuvem para funções críticas do cliente deve incluir a identificação e avaliação de ativos, identificação e análise de ameaças e vulnerabilidades e potenciais impactos nos ativos, análise de probabilidade de eventos, critérios e níveis 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 incluídos nos SLAs.
9. O usuário e o provedor de nuvem devem desenvolver em conjunto cenários de risco para os serviços em nuvem.
10. O cliente de nuvem deve ser atencioso quanto à resiliência do negócio do provedor, a portabilidade dos dados e aplicações e a interoperabilidade dos serviços para não ficar preso a um provedor, nem ter seus serviços interrompidos por muito tempo, caso o provedor deixe o mercado.
11. O inventário de ativos de informação do cliente de nuvem deve considerar os serviços de suporte de ativos na nuvem e sob controle do provedor.
12. O serviço junto com o fornecedor devem ser os alvos de uma avaliação de riscos.
13. Quando o provedor não se mostrar eficaz no processo de gerenciamento de riscos, o cliente deve avaliar com cuidado as habilidades tanto do provedor quanto as suas próprias, a fim de compensar as possíveis brechas indicadas no gerenciamento de riscos.
14. O cliente de serviços na nuvem deve 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.

15. O cliente de nuvem deve 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.
16. O cliente de nuvem deve estipular requisitos contratuais apropriados e controles tecnológicos para coletar dados necessários para informar as decisões sobre os riscos à informação.
17. O cliente de nuvem deve escolher um processo para definir a exposição ao risco antes de especificar os requisitos para um projeto de computação em nuvem.
18. Quando SaaS for utilizado, a maior parte da informação deve ser fornecida pelo provedor do serviço. O cliente deve estruturar processos de coleta de informações analíticas nas obrigações contratuais do serviço SaaS.
19. Quando PaaS for utilizado, o cliente deve definir a coleta de informações como feito no modelo SaaS acima, mas sempre que possível, devem ser consideradas a capacidade de implantar e coletar informações de controles, bem como a criação de itens contratuais para testar a efetividade destes controles.
20. Quando IaaS for utilizado, o cliente deve estabelecer a transparência das informações em nível contratual para que possam ser tratadas pela análise de riscos.
21. O provedor de serviços de nuvem deve incluir controles e métricas para auxiliar o cliente na implementação dos seus requisitos de gestão de risco da informação.
22. O cliente de nuvem deve tratar os serviços e a segurança da nuvem como questões de segurança da cadeia de suprimentos. Isso significa examinar e avaliar, a cadeia de suprimentos do provedor, ou seja, o relacionamento do provedor com seus terceirizados.
23. A crítica aos fornecedores de serviços terceirizados deve ser focada especificamente no gerenciamento do fornecedor, nas políticas de e continuidade de negócio e recuperação de desastres, e em processos e procedimentos. Deve-se igualmente, averiguar as instalações de backup e de suas instalações físicas.
24. O plano de continuidade de negócios e recuperação de desastres do cliente de nuvem deve incluir cenários de perda dos serviços prestados por seu provedor e também dos serviços terceirizados contratados pelo provedor. A realização dos testes dessa parte do plano deve ser coordenada com o provedor de serviços de nuvem.
25. A regulamentação da governança de segurança de informações, a gestão de riscos e as estruturas e processos do fornecedor devem ser amplamente avaliados:

1. O cliente deve requisitar uma documentação clara sobre como as instalações e os serviços do fornecedor são avaliados quanto aos riscos e auditados acerca de controles de vulnerabilidades, a frequência das avaliações, e como as deficiências de controles são reduzidas.
2. O cliente deve requisitar uma definição do que o fornecedor considera serviços críticos e fatores de sucesso de segurança da informação, indicadores chave de desempenho, e estes aspectos são medidos em relação à gestão de segurança de informações e serviços de TIC.
3. O cliente deve examinar a amplitude dos processos de comunicação, avaliação e domínio dos requisitos legais, regulatórios, industriais e contratuais do provedor.
4. O cliente deve implantar contratos detalhados para determinar papéis, funções e responsabilidades assegurando que será feito uma validação legal, incluindo uma avaliação do cumprimento das normas contratuais e leis em jurisdições estrangeiras ou fora do estado.
5. O cliente deve determinar se os requisitos contratuais tratam de todos os aspectos materiais das relações dos provedores de serviço de nuvem, tais como a situação financeira, a reputação, pessoal estratégico, controles, planos e testes de recuperação de desastres, capacidades de comunicações, seguros e uso de terceirizados do provedor.

4.2 ASPECTOS LEGAIS E DESCOBERTA ELETRÔNICA

As recomendações apresentadas são apenas diretrizes. É aconselhada fortemente a contratação de consultores jurídicos especializados para um melhor entendimento das leis vigentes na região e no segmento de mercado em que a organização atua.

As recomendações são:

1. O cliente e o provedor de nuvem devem estar cientes dos respectivos papéis e responsabilidades relacionados à descoberta eletrônica, incluindo atividades como investigações, litígio, prover o testemunho de perito, etc.
2. O provedor de nuvem deve garantir que seus sistemas de segurança da informação atendam às necessidades do cliente para preservar os dados como confiáveis e autênticos, incluindo informações primárias e secundárias, como arquivos de logs e metadados.

3. Os dados sob a responsabilidade do provedor de serviços de nuvem devem receber proteção equivalente a que teriam se estivessem nas mãos de seu proprietário original ou custodiante.
4. O cliente de nuvem deve elaborar de um plano para o término esperado ou inesperado da relação contratual com o prestador de serviço para o retorno ou descarte seguros dos ativos.
5. O cliente de nuvem deve fazer uma auditoria geral pré-contratual, negociação dos termos do contrato, monitorar o pós-contrato, a rescisão contratual e a transição da custódia dos dados.
6. O cliente de nuvem deve saber onde o provedor de serviços de nuvem irá hospedar os dados, uma vez que, isto é pré-requisito para implementar as medidas necessárias para garantir a conformidade com as leis locais que restringem o fluxo de dados além de determinadas fronteiras geográficas.
7. O cliente de nuvem deve assegurar que ele mantém a posse de seus dados em seu formato original e autêntico, como custodiante dos dados pessoais de seus funcionários ou clientes, bem como de outros ativos de propriedade intelectual da instituição.
8. Diversas questões de segurança, como suspeitas de violação de dados, devem ser tratados através de disposições específicas do SLA, que deve esclarecer as respectivas obrigações do provedor de serviços de nuvem e do cliente.
9. O provedor de serviços de nuvem e o cliente devem acordar um processo unificado para responder às intimações, citações e outros requisitos legais.
10. O SLA deve fazer com que o provedor de nuvem notifique o cliente em caso de recebimento de intimação, e dar tempo suficiente ao cliente para que essa possa pleitear contra o acesso aos dados requisitados na intimação.
11. O SLA deve permitir que o cliente ou terceiro designado monitore o desempenho do provedor de serviços e teste as vulnerabilidades no sistema.
12. O SLA deve prever a ocorrência de problemas relativos à recuperação dos dados do cliente após o término da relação contratual.

4.3 CONFORMIDADE E AUDITORIA

As recomendações são:

1. O cliente de nuvem deve envolver o departamento jurídico e de contratos no processo

de contratação de um provedor de nuvem. As cláusulas padrão de serviço do provedor de nuvem podem não atender suas necessidades de conformidade. 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.

2. Dada a natureza dinâmica dos ambientes regulatórios e da nuvem, o cliente de nuvem, frequentemente, terá a necessidade de auditar o provedor de serviços de computação em nuvem. Uma cláusula sobre o direito de auditar deve ser obtida sempre que possível, particularmente quando um provedor for usado para um serviço onde o cliente tenha que regulamentar o cumprimento das responsabilidades. Ao longo do tempo, deve se reduzir a necessidade deste direito e em muitos casos substituída por certificações do provedor.
3. O cliente de nuvem deve analisar o escopo de conformidade e definir se os regulamentos de conformidade aos quais a organização está sujeita serão impactados pelo uso dos serviços de nuvem para um dado conjunto de aplicações e dados.
4. O cliente de nuvem deve analisar o impacto dos regulamentos sobre a segurança dos dados, além de quais dados e aplicações serão movidos para serviços na nuvem e em que medida eles estão sujeitos aos regulamentos de conformidade.
5. O cliente de nuvem deve revisar os provedores de serviços e parceiros importantes para assegurar que o relacionamento com os provedores de serviços não afete negativamente a conformidade, além de determinar quais provedores estão processando os dados sujeitos aos regulamentos de conformidade e avaliar os controles de segurança oferecidos pelos mesmos.
6. O cliente de nuvem deve saber as responsabilidades contratuais que tem sobre a proteção dos dados e os contratos relacionados. De certa forma, o modelo de serviços de computação em nuvem escolhido determina se o cliente ou o provedor de serviços é o responsável pela implantação de controles de segurança. Na IaaS, o cliente tem um alto grau de controle e uma maior responsabilidade do que no SaaS, ou seja, clientes IaaS terão que implantar muito dos controles para a conformidade regulatória. Já no SaaS, é o provedor de serviços que deve fornecer os controles necessários. De uma perspectiva contratual é importante conhecer os requisitos específicos e garantir que o contrato de serviços, bem como os SLAs, sejam tratados adequadamente.
7. O cliente de nuvem deve averiguar o impacto das regulamentações na infraestrutura do

provedor. Migrar para serviços de computação em nuvem também requer uma análise cuidadosa na área de infraestrutura. Alguns requisitos regulatórios especificam controles que são difíceis ou impossíveis de se atingir em certos tipos de serviços de nuvem.

8. O cliente de nuvem deve analisar o impacto das regulamentações nas políticas e procedimentos. Migrar dados e aplicações para serviços de computação em nuvem provavelmente causará um impacto nas políticas e procedimentos. O cliente deve avaliar quais políticas e procedimentos relacionados com as regulamentações deverão ser modificados, como relatórios de atividades, retenção dos dados, logs, resposta a incidente, controles de testes e políticas de privacidade.
9. O cliente de nuvem deve fomentar evidências de como cada exigência está sendo cumprida, além de 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.
10. Em muitos casos o cliente não tem nenhuma influência na seleção de auditores ou avaliadores de segurança. Se o cliente participar da seleção, é altamente recomendável escolher um auditor que conheça a computação em nuvem, haja vista que muitos podem não estar familiarizados com os desafios da computação em nuvem e da virtualização. Questionar sua familiaridade com as nomenclaturas SaaS, PaaS e IaaS é um bom começo.
11. O provedor que busca o fornecimento de serviços críticos deve adotar os padrões da norma NBR ISO/IEC 27001 (ABNT, 2013) para sistemas de gerenciamento de segurança da informação. Se o provedor não tiver a certificação ISO/IEC 27001, ele deve ao menos demonstrar alinhamento com as práticas da norma NBR ISO/IEC 27002 (ABNT, 2013).

4.4 GERENCIAMENTO DE INFORMAÇÕES E SEGURANÇA DOS DADOS

As recomendações são:

1. O cliente de nuvem deve conhecer a arquitetura de armazenamento em nuvem em uso, o que irá auxiliar a determinar quais são os riscos de segurança e potenciais controles.
2. O cliente de nuvem deve escolher armazenamento com dispersão de dados sempre que

possível.

3. O cliente de nuvem deve usar a segurança de ciclo de vida dos dados para identificar brechas na segurança e determinar os controles mais adequados a serem empregados.
4. O cliente de nuvem deve monitorar o banco de dados e repositórios de arquivos com DAM e FAM para identificar grandes migrações de dados, o que pode indicar uma migração de dados para a nuvem a fim de proteger as migrações.
5. O cliente de nuvem deve monitorar o acesso dos empregados à internet com filtros de URL e ferramentas de DLP para identificar migração de informações sensíveis para a nuvem. Selecione ferramentas que incluam categorias pré-definidas para serviços de nuvem, além do uso de filtros para bloquear atividades inapropriadas.
6. O cliente de nuvem deve saber como criptografia é gerenciada em ambiente multilocatário. Se existe apenas uma chave para todos os locatários, uma chave por locatário, ou múltiplas chaves por locatário e se há um sistema para prevenir diferentes locatários de terem as mesmas chaves criptográficas.
7. O cliente de nuvem deve usar a descoberta de conteúdo para varrer o armazenamento na nuvem e identificar dados sensíveis expostos.
8. O cliente de nuvem deve criptografar dados armazenados em *object storages* com encriptação de arquivo/pasta ou cliente/agente
9. No SaaS, o cliente de nuvem deve buscar um provedor que ofereça criptografia nativa. Caso não seja possível ou níveis extras de segurança precisem ser garantidos, deve-se usar criptografia de proxy.
10. Na PaaS, o cliente de nuvem deve usar criptografia em nível de aplicação nos dados sensíveis em aplicações e armazenamento de preferência.
11. Na IaaS, o cliente deve criptografar os volumes com informações sensíveis para limitar a exposição caso ocorra um acesso não autorizado aos volumes.
12. O cliente de nuvem deve usar DLP para identificar o vazamento de informações sensíveis. Normalmente é disponível apenas para IaaS e em alguns provedores de nuvens. Deve-se buscar aqueles que ofereçam o DLP como ferramenta.
13. O cliente de nuvem deve monitorar base de dados sensíveis com DAM e gerar alertas quando as políticas de segurança forem violadas.
14. O cliente de nuvem deve considerar o armazenamento que preserve a privacidade quando forem ofertadas aplicações ou a infraestrutura, onde acesso normal poderia

revelar informações sensíveis do usuário.

15. A remoção de dados de um provedor de nuvem deve ser detalhada no SLA, que deve cobrir a exclusão de contas de usuário, migração ou exclusão dos dados, transferência de chaves etc.
16. O cliente de nuvem deve saber como a integridade é mantida e como o comprometimento da integridade é detectado e informado ao cliente pelo provedor. A mesma recomendação aplica-se à confidencialidade quando apropriado.
17. O provedor de nuvem deve garantir ao proprietário dos dados que eles proveem a divulgação de todas as suas informações, isto é, completa transparência, relativas às práticas e procedimentos de segurança de acordo com os SLAs.
18. O cliente de nuvem deve garantir a identificação específica de todos os controles usados durante o ciclo de vida dos dados, além das especificações de qual entidade é responsável por cada controle entre o proprietário dos dados e o provedor de serviços de nuvem.
19. O cliente de nuvem deve manter uma filosofia fundamentada no conhecimento de onde seus dados estão, além de assegurar sua habilidade de conhecimento sobre a localização geográfica de armazenamento. Estes pontos devem estar nos SLAs e contratos.
20. O cliente de nuvem deve saber em quais circunstâncias os dados armazenados em um provedor de nuvem podem ser apreendidos por um terceiro ou entidade governamental. É importante incluir nos SLAs com o provedor processo de notificação prévia ao proprietário dos dados que as informações do proprietário dos dados serão apreendidas.
21. Se uma intimação ou citação de descoberta eletrônica for interposta contra o provedor de serviços, o provedor deverá informar ao proprietário dos dados sobre essa divulgação, caso o provedor possuir custódia dos dados do cliente.
22. O cliente de nuvem deve conhecer os limites de confiança da arquitetura de TIC e suas camadas de abstração, possibilitando aos subsistemas somente ultrapassarem os limites de confiança quando necessário e com contramedidas apropriadas para prevenir divulgação não autorizada, alteração ou destruição de dados.
23. O cliente de nuvem deve conhecer quais são as técnicas de compartimentalização utilizadas pelo provedor para isolar seus clientes uns dos outros. Um provedor pode utilizar uma variedade de métodos dependendo dos tipos e quantidade de serviços oferecidos.

24. O cliente de nuvem deve conhecer as capacidades e limitações de busca de dados do provedor de serviços quando tentar visualizar “dentro” da série de dados para a descoberta de dados.
25. O proprietário de dados deve solicitar que o provedor de serviço garanta que seus dados de backup não estejam misturados com os de outro cliente de serviço de nuvem.
26. O cliente de nuvem deve conhecer o processo de descarte de dados armazenados pelo provedor de serviços.
27. O cliente de nuvem deve conhecer a separação lógica de informação e os controles de proteção implementados pelo provedor.
28. O cliente de nuvem deve conhecer as restrições de privacidade inerentes aos dados confiados a sua companhia.
29. O cliente de nuvem deve conhecer os processos e políticas do provedor de serviços para retenção e destruição de dados e como eles se comparam à sua política organizacional interna. Ainda deve saber que garantir a retenção de dados pode ser mais fácil para o provedor de serviços demonstrar, enquanto para a destruição de dados pode ser muito difícil.
30. O cliente de nuvem deve negociar penalidades pagas pelo provedor caso haja violação dos dados. Se viável, o cliente deve buscar o ressarcimento de todos os custos por violações como parte de seus contratos com o provedor. Se inviável, o cliente deve explorar outros meios de transferência de risco, como seguro para recuperação de perdas por violação.
31. O cliente de nuvem deve executar testes de backup e recuperação regulares para garantir que a separação lógica e os controles são efetivos.

4.5 PORTABILIDADE E INTEROPERABILIDADE

Existem recomendações que se aplicam a todos as soluções em nuvem, no entanto, existem particularidades de cada modelo de serviço e implantação que requerem cuidados diferentes.

As recomendações são:

4.5.1 PARA TODAS AS SOLUÇÕES

1. Como os SLAs podem variar entre provedores diferentes, é necessário saber como eles podem afetar a habilidade de trocar de provedores.

2. Usar padrões abertos para autenticação e identidade como o SAML ajudam a garantir a portabilidade.
3. As chaves criptográficas devem ser mantidas sob custódia localmente sempre que possível.
4. O cliente de nuvem, quando estiver migrando dados de um provedor para o outro, deve se certificar de que as cópias dos dados e seus metadados no antigo provedor foram seguramente removidas para que estas não gerem uma possível oportunidade de revelar informações indesejadas.
5. Em praticamente todos os casos a troca do provedor de serviços de nuvem é 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.
6. O cliente de nuvem deve conhecer o tamanho dos conjuntos de dados hospedados no provedor. O tamanho dos dados pode causar interrupção do serviço durante a transição, ou um período de transição maior do que o previsto.
7. O cliente de nuvem deve 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 SaaS

1. O cliente de nuvem deve executar a extrações dos dados e backups regularmente para formatos que possam ser utilizados fora do provedor de SaaS.
2. O cliente de nuvem deve saber se os metadados podem ser preservados e migrados.
3. O cliente de nuvem deve saber que quaisquer ferramentas personalizadas terão que ser recodificadas, ou se o novo provedor providenciará estas ferramentas.
4. O cliente de nuvem deve garantir a eficácia da consistência dos controles entre o antigo e o novo provedor.
5. O cliente de nuvem deve garantir a possibilidade de migração de backups e cópias de logs, registros de acesso e qualquer outra informação relevante que possa ser necessária por razões legais e conformidade.
6. O cliente de nuvem deve conhecer o gerenciamento, monitoramento e as interfaces de

relatórios e suas integrações entre os ambientes.

7. O cliente de nuvem deve verificar se o novo provedor está disposto a testar e avaliar a aplicação antes da migração.
8. O cliente de nuvem deve testar e avaliar as aplicações, mais de uma vez se possível, antes de migra-las para garantir que a aplicação esteja funcionando corretamente no novo provedor.

4.5.3 PARA SOLUÇÕES PaaS

1. O cliente de nuvem deve utilizar componentes de uma plataforma com sintaxes padronizadas, APIs e normas abertas quando possível.
2. O cliente de nuvem deve saber quais ferramentas estão disponíveis para a transmissão segura dos dados, para backup e para restauração.
3. O cliente de nuvem deve conhecer e documentar os componentes da aplicação e módulos específicos para o provedor de PaaS e desenvolver a arquitetura da aplicação com camadas de abstração para minimizar o acesso direto aos módulos proprietários.
4. O cliente de nuvem deve saber como os serviços de monitoramento, logs e auditoria podem ser migrados para o novo provedor.
5. O cliente de nuvem deve saber quais proteções são fornecidas pelo provedor de nuvem antigo e novo.
6. O cliente de nuvem deve saber as funções de controle fornecidas pelo provedor de nuvem antigo e como será feita a migração para o novo provedor.
7. O cliente de nuvem deve conhecer os impactos no desempenho e na disponibilidade da aplicação e como estes impactos são calculados quando migrarem para uma nova plataforma.
8. O cliente de nuvem deve fazer testes antes e depois da migração para verificar se os serviços e aplicações estão funcionando corretamente. A responsabilidade dos testes é de ambos, provedor e usuário, sendo as responsabilidades de cada um bem conhecidas e documentadas.

4.5.4 PARA SOLUÇÕES IaaS

1. O cliente de nuvem deve saber como as imagens das máquinas virtuais podem ser capturadas e migradas para o novo provedor de nuvem que pode utilizar uma tecnologia diferente de virtualização.

2. O cliente de nuvem deve identificar e eliminar todas as extensões específicas do provedor no ambiente de máquina virtual. Se não for possível, deve documentar todas as extensões não proprietárias.
3. O cliente de nuvem deve saber quais são as práticas utilizadas para garantir a transferência apropriada das imagens de máquinas virtuais depois que uma aplicação for migrada do provedor de nuvem.
4. O cliente de nuvem deve saber quais são as práticas utilizadas na desmontagem dos discos e dispositivos de armazenamento.
5. O cliente de nuvem deve identificar e conhecer as dependências de hardware ou plataforma antes de migra a aplicação ou os dados.
6. O cliente de nuvem deve requerer o acesso aos logs do sistema, rastros e registros de acesso e de faturamento do provedor de nuvem anterior.
7. O cliente de nuvem deve identificar opções para continuar ou expandir o serviço com o provedor de nuvem anterior, em parte ou no todo, caso o novo provedor de serviços demonstre ser inferior.
8. O cliente de nuvem deve determinar se existem quaisquer funções de nível gerencial, interfaces ou APIs utilizadas que são incompatíveis ou não implantadas no novo provedor.
9. O cliente de nuvem deve saber quais são os custos envolvidos para migrar dados para fora e para dentro de um provedor de nuvem.
10. O cliente de nuvem deve determinar os meios mais eficientes para migrar dados para a nuvem.

4.5.5 PARA SOLUÇÕES EM NUVEM PÚBLICA

1. O cliente de nuvem deve garantir que o provedor de nuvem exponha interfaces comuns ou abertas para o acesso de todas as funções da nuvem nos serviços ofertados.

4.5.6 PARA SOLUÇÕES EM NUVEM PRIVADA

1. O cliente de nuvem deve garantir a interoperabilidade entre *hypervisors* comuns de ferramentas populares de virtualização, como VMware, KVM, e Xen.
2. O cliente de nuvem deve garantir que APIs padrões são usadas para funções de gerencia, como de usuários e privilégios, imagens de máquinas virtuais, máquinas virtuais, redes virtuais, serviços, armazenamento, infraestrutura e informação.

4.5.7 PARA SOLUÇÕES EM NUVEM HÍBRIDA

1. O cliente de nuvem deve garantir que o provedor de nuvem exponha interfaces comuns ou abertas para o acesso de todas as funções da nuvem nos serviços ofertados, assim como na nuvem pública.
2. O cliente de nuvem deve garantir a habilidade de federar com diferentes provedores de nuvem para permitir maiores níveis de escalabilidade.

4.6 SEGURANÇA TRADICIONAL, CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

Aqui são apresentadas recomendações de segurança tradicional, que consiste na segurança física e do ambiente, tratada na seção 9 da norma NBR ISO/IEC 27002 (ABNT, 2013).

As recomendações são:

1. O cliente de nuvem deve saber que a centralização dos dados é uma preocupação significativa, já que há o risco de fraude interna partindo de dentro do provedor de serviços de nuvem.
2. O provedor de serviço de nuvem deve adotar os requisitos mais rigorosos dos clientes como padrão de segurança, devendo se mostrar economicamente eficazes no longo prazo na redução de riscos.
3. O provedor deve ter uma divisão robusta das responsabilidades das funções, verificar os antecedentes dos funcionários, exigir e 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 estritamente necessário para a execução de suas funções.
4. O cliente de nuvem deve efetuar inspeções aos locais das instalações do provedor de nuvem sempre que possível, de preferência sem aviso prévio.
5. O cliente de nuvem deve inspecionar os planos de recuperação de desastres e de continuidade de negócios do provedor de nuvem.
6. O cliente de nuvem deve identificar as interdependências físicas na infraestrutura do provedor.
7. O cliente de nuvem deve garantir que o contrato tenha um detalhamento formal para definir claramente as obrigações contratuais relacionadas com segurança, recuperação e acesso aos dados.

8. O cliente de nuvem deve requerer a documentação dos controles de segurança internos e externos do provedor e a adesão aos padrões da indústria.
9. O cliente de nuvem deve assegurar que seus objetivos de tempo de recuperação são totalmente entendidos e definidos nas relações contratuais e baseados no processo de planejamento tecnológico, além de se certificar de que os roteiros, políticas e capacidades operacionais satisfaçam estes requisitos.
10. O cliente de nuvem precisa confirmar que o provedor tem uma política de plano de continuidade de negócios aprovada pelo conselho de administração do provedor.
11. O cliente de nuvem deve procurar evidências de apoio efetivo da gestão e revisão periódica do programa de continuidade de negócios para garantir que este esteja operante.
12. O cliente de nuvem deve verificar se o programa de gestão de continuidade de negócios é certificado por normas internacionalmente reconhecidas como a BS 25999.
13. O cliente de nuvem deve verificar se o provedor tem algum recurso on-line dedicado à segurança e melhores práticas correntes, onde a visão geral do programa e as fichas técnicas estejam disponíveis para consulta.
14. O provedor de IaaS deve ter acordos contratuais e corporativos com outros provedores de IaaS e ter ferramentas prontas para rapidamente recuperar o sistema em caso de falha.
15. O cliente de nuvem deve revisar com frequência todas as atividades desta seção para a descoberta de mudanças não comunicadas ao cliente

4.7 OPERAÇÕES DE DATACENTER

As recomendações são:

1. O provedor deve obter o compromisso e a permissão de conduzir auditorias feitas pelo cliente ou por terceiros, quaisquer que sejam as certificações que o provedor de nuvem mantém.
2. O cliente de serviços de nuvem deve saber como o provedor implementa as cinco características essenciais da nuvem.
3. O provedor deve poder demonstrar sua divisão compreensiva de sistemas, redes, gerenciamento, provisão e pessoal, ainda que as arquiteturas tecnológicas dos provedores de nuvem variem.

4. O cliente de nuvem deve saber como a democratização de recursos ocorre dentro da nuvem do provedor para prever melhor a disponibilidade e desempenho do sistema durante suas flutuações de negócios. Se possível, também descobrir 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. Porém, isso não substitui a garantia de que os SLAs estejam claramente definidos, mensuráveis, executáveis e adequados para a sua necessidade.
5. O cliente de nuvem deve conhecer as políticas e procedimentos de correção do provedor e como eles podem influenciar os seus ambientes. Esta compreensão deve estar no contrato.
6. O cliente de nuvem deve procurar provedores de nuvem com processos padrão de melhoria contínua, pois qualquer melhoria nas políticas, processos e procedimentos, ou ferramentas para um determinado cliente pode resultar na melhoria do serviço para todos os clientes.
7. A organização que está construindo datacenters de nuvem deve incorporar gerenciamento de processos, práticas e *software* para conhecer e reagir às tecnologias rodando dentro dos datacenters.
8. A organização deve saber que a localização dos datacenters é importante. Se as aplicações forem distribuídas através de muitos datacenters, haverá um aumento da latência entre os datacenters.
9. O cliente de nuvem deve conhecer e documentar quem é responsável, o cliente ou o provedor, por atender os requisitos de conformidade e os papeis quando a conformidade.

4.8 RESPOSTA A INCIDENTE, NOTIFICAÇÃO E REMEDIAÇÃO

As recomendações são:

1. O cliente de nuvem precisa definir claramente e comunicar ao provedor o que ele considera incidente e um mero evento antes de implementar o serviço.
2. O cliente de nuvem pode vir a ter um envolvimento limitado com as atividades de resposta a incidente do provedor. Portanto, é crucial o cliente conhecer os canais de comunicação predefinidos para contatar a equipe de resposta a incidente.
3. O cliente de nuvem deve investigar quais ferramentas de detecção e análise de incidente

o provedor utiliza para garantir que elas sejam compatíveis com seus próprios sistemas. Um formato de log proprietário ou incomum poderia ser um problema em investigações conjuntas, particularmente as que envolvam intervenção governamental ou questões legais.

4. Aplicações e sistemas desenvolvidos com baixo nível de segurança podem sobrecarregar qualquer capacidade de resposta a incidente. 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.
5. Centros de operações de segurança geralmente 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 bem coordenado de SIEM, que identifica as fontes disponíveis de informação, como logs de aplicações e firewalls, 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.
6. Qualquer dado classificado como privado deve ser sempre criptografado para reduzir as consequências de um incidente de roubo de dados.
7. Provedores de nuvem podem hospedar um número grande de clientes com aplicações únicas. Estes provedores devem considerar estruturas de registros de camada de aplicação com o objetivo de rastrear incidentes de um cliente em especifico, além de criar um registro de proprietários das aplicações por interface de aplicação, como serviços de SOA e URL.

4.9 SEGURANÇA DE APLICAÇÕES

As recomendações são:

1. Deve ser feita uma análise de riscos das aplicações para segurança, privacidade, confiança, integridade e disponibilidade, e modelos de ameaça desenvolvidos e mantidos pela organização.
2. Riscos do ponto de vista relativos ao modelo de serviço e implementação devem ser analisados.
3. Vetores de ataque e análises de impacto especificas das arquiteturas da nuvem devem ser catalogadas e mantidas.

4. *Frameworks* de arquitetura segura de *software* devem ser desenvolvidos e mantidos.
5. O cliente de nuvem deve classificar as vulnerabilidades criticamente baseado no seu impacto e ter um processo para remediação.
6. Aplicações sendo migradas de IaaS ou PaaS, devem ser avaliadas para garantir que os controles de segurança de nível mais baixo, como a segregação de máquinas virtuais e a segurança de virtualização, foram efetivamente postos em prática e não representam problemas de segurança para a aplicação.
7. A segurança no ciclo de vida de desenvolvimento de *software* deve tratar em alto nível de três áreas principais de diferenciação com desenvolvimento baseado em nuvem: ameaças atualizadas e modelos de confiança, ferramentas de avaliação de aplicações para ambientes de nuvem e processos de segurança no ciclo de vida de desenvolvimento de *software* e checkpoints de qualidade para contabilizar mudanças na arquitetura de segurança de aplicações.
8. SaaS, PaaS e IaaS criam diferentes limites de confiança para o ciclo de vida de desenvolvimento de *software*, que devem ser avaliados durante o desenvolvimento, teste e implantação das aplicações.
9. Para IaaS, um fator fundamental é a presença de imagens de máquinas virtuais confiáveis. A melhor escolha é a organização fazer o uso das suas próprias imagens contendo seus requisitos de conformidade e políticas internas.
10. As melhores práticas de segurança devem ser aplicadas para máquinas virtuais para fortalecer os sistemas hospedeiros dentro de DMZs.
11. Proteger a comunicação entre servidores deve ser uma regra. Não se deve supor que haja um canal seguro entre os servidores, estando numa mesma máquina física ou num datacenter comum.
12. É fundamental proteger e gerenciar arquivos de log e depuração das aplicações, assim como a localização destes.
13. Métricas, como escores de vulnerabilidade e cobertura de correções precisam ser aplicadas para avaliar a eficiência de programas de segurança de aplicação. Essas métricas podem mostrar a qualidade da codificação de aplicação. Métricas de manipulação indireta de dados, como o percentual de dados cifrados podem indicar que decisões responsáveis estão sendo tomadas a partir de uma perspectiva de arquitetura da aplicação.

14. O provedor de nuvem deve suportar ferramentas de segurança de análise dinâmica para aplicações Web às aplicações hospedadas em seu ambiente.
15. O cliente de nuvem deve obter permissão contratual para realizar avaliações de vulnerabilidades remotas. Muitos provedores de nuvem restringem as avaliações devido à incapacidade do provedor de distinguir tais testes de ataques reais e para evitar potenciais impactos sobre outros clientes.
16. Qualquer dado classificado como privado deve ser sempre criptografado para reduzir as consequências de um incidente de roubo de dados.

4.10 CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES

As recomendações são:

1. Deve-se utilizar das melhores práticas de gerenciamento de chaves quando estiver lidando com qualquer forma de criptografia.
2. Deve-se utilizar tecnologia pronta sempre que possível para obter as melhores práticas de fontes confiáveis.
3. É altamente recomendado que a organização mantenha suas próprias chaves ou use o serviço de criptografia uma fonte confiável.
4. Deve-se utilizar algoritmos padrões de confiabilidade comprovada. Algoritmos de encriptação proprietários são facilmente quebrados e sem confiabilidade comprovada
5. É altamente recomendado evitar padrões antigos e inseguros de criptografia, como o DES.
6. Deve-se limitar o acesso até mesmo às informações criptografadas.
7. Ao criptografar banco de dados, não se deve criptografar as colunas indexadas ou chaves primárias, por resultar em consultas bastante lentas.
8. Deve-se usar criptografia para separar a posse dos dados do uso dos dados.
9. Separar o gerenciamento de chaves do provedor de nuvem que hospeda os dados cria uma cadeia de separação, protegendo tanto o provedor quanto o cliente de conflitos quando houver obrigação de fornecer dados devido a um mandato legal.
10. Em casos onde o provedor de nuvem efetuar o gerenciamento de chaves, o cliente deve 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, o cliente deve tomar conhecimento se a mesma chave é utilizada para todos os clientes ou se cada cliente tem seu próprio conjunto de chaves.

11. O cliente de nuvem deve assegurar que os dados sensíveis ou regulamentados sejam criptografados quando estiverem em trânsito através da rede interna do provedor, além de serem criptografados quando não estiverem em uso. A responsabilidade dessa implementação é do provedor no SaaS, de ambos na PaaS e do cliente na IaaS.
12. Em IaaS, o cliente de nuvem deve saber como as informações sensíveis podem ser expostas durante o uso, quando não forem protegidos por criptografia tradicional, como em arquivos de *swap* de máquinas virtuais e outros locais temporários de armazenamento de dados que também podem necessitar ser criptografados.

4.11 GERENCIAMENTO DE IDENTIDADE E ACESSO

As recomendações são:

4.11.1 PARA CONCESSÃO DE IDENTIDADE

1. O cliente de nuvem deve evitar soluções proprietárias ou criar conectores personalizados unicamente para os provedores de nuvem, já que isto aumenta a complexidade do gerenciamento.
2. O cliente de nuvem deve usar conectores de padrões fornecidos pelo provedor de nuvem como uma medida prática e de preferência construídos no esquema SPML. Se o provedor não oferecer SPML, o cliente deve solicitá-lo.
3. O cliente de nuvem deve modificar seus repositórios de identidade para incluírem as aplicações e processos na nuvem.

4.11.2 PARA AUTENTICAÇÃO

1. O cliente de nuvem deve considerar autenticar seus usuários através dos seus provedores de identidade e estabelecer uma confiança com o provedor SaaS através de federação de acesso.
2. O cliente de nuvem deve considerar usar autenticação centrada em usuário, como do Google, Yahoo, Live ID e OpenID, para permitir o uso de um conjunto único de credenciais válido para múltiplos sites.
3. O cliente de nuvem deve evitar qualquer provedor de SaaS que exija métodos proprietários para delegar a autenticação, como manipulação de confiança por meio de

um cookie criptografado compartilhado, deve ser evitado. A preferência geral deve ser para o uso de padrões abertos.

4. O cliente de nuvem com conhecimento em TIC pode estabelecer uma VPN dedicada, uma vez que pode-se aproveitar processos e sistemas já existentes.
5. O cliente de nuvem pode criar um túnel VPN dedicado para a rede corporativa ou da federação. Um túnel VPN dedicado funciona melhor quando a aplicação usa os sistemas existentes de gerenciamento de identidade, como uma solução de autenticação baseada em SSO ou LDAP, que fornece uma fonte autorizada de dados de identidade.
6. Caso um túnel VPN dedicado não for possível, as aplicações devem ser desenhadas para aceitarem os pedidos de autenticação em vários formatos, como SAML e Federação-WS, e combinadas com criptografia padrão de rede, como SSL. Isso permite às organizações implantarem SSO federados não apenas dentro da empresa, mas também para aplicações na nuvem.
7. OpenID é outra opção quando a aplicação é direcionada para além dos usuários corporativos. Porém, pelo fato do controle das credenciais do OpenID estar fora da empresa, os privilégios de acesso fornecido a estes usuários deve ser limitado.
8. Qualquer serviço local de autenticação implementado pelo provedor de serviços de nuvem deve estar em harmonia com o OAuth. Utilizando uma solução com suporte a OAuth a empresa evita ficar presa a credenciais de autenticação fornecidas por um fabricante.
9. Para permitir a autenticação forte, as aplicações de nuvem devem delegar a autenticação para a empresa que está consumindo os serviços, como o SAML.
10. O provedor de nuvem deve considerar o suporte a várias opções de autenticação forte, como senhas de acesso único, biometria, certificados digitais e Kerberos. Isto oferecerá outra opção às empresas de usar sua infraestrutura existente.

4.11.3 PARA FEDERAÇÃO

1. Na computação em nuvem, a federação de identidade é chave para permitir que a empresa aliada se autentique, provenha SSO e troque atributos de identidade entre o provedor de serviços e o provedor de identidade. Ao considerar o gerenciamento de identidade federada na nuvem, a organização deve conhecer os vários desafios e possíveis soluções relacionadas ao gerenciamento do ciclo de vida da identidade, métodos de autenticação, formatos de token e não-repúdio.

2. A empresa que busca um provedor de nuvem deve verificar se o provedor suporta ao menos um dos padrões proeminentes. O SAML é um padrão de federação amplamente suportado e utilizado pelos principais provedores de SaaS e PaaS. O suporte a múltiplos padrões permite um alto grau de flexibilidade.
3. O provedor de nuvem deve ser flexível para aceitar os formatos padrões de federação de diferentes provedores de identidade.

4.11.4 PARA CONTROLE DE ACESSO

1. O cliente de nuvem deve adequar o modelo de controle de acesso para o tipo de serviço ou dados.
2. O cliente de nuvem deve avaliar o suporte às políticas de privacidade necessárias para os dados.
3. O cliente de nuvem deve escolher o formato no qual especificará a política e a informação do usuário.
4. O cliente de nuvem deve registrar as informações necessárias para auditorias.

4.12 VIRTUALIZAÇÃO

As recomendações são:

1. O cliente de nuvem deve identificar quais os tipos de virtualização o provedor de nuvem usa.
2. Os 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.
3. O clientes deve saber quais controles de segurança estão implementados em suas máquinas virtuais, além de como é incorporado o isolamento do *hypervisor*, como detecção de intrusões, antivírus, escaneamento de vulnerabilidades, etc.
4. As configurações seguras de máquinas virtuais, que seguem as melhores práticas, devem ser implementadas nas máquinas virtuais para evitar *instant-on gaps*.
5. O cliente de nuvem deve saber quais controles de segurança estão implementados externamente às máquinas virtuais para proteger as interfaces administrativas expostas para eles.
6. O cliente de nuvem deve validar a procedência e integridade de qualquer máquina

virtual ou modelo originado do provedor de nuvem antes de utilizá-la.

7. Os mecanismos de segurança específicos de máquinas virtuais embarcados dentro das APIs do *hypervisor* devem ser utilizados para prover monitoração granular do tráfego entre o plano de fundo das máquinas virtuais, que não é visível aos controles tradicionais de segurança de rede.
8. O acesso administrativo e o 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.
9. O cliente de nuvem deve considerar a eficácia e a viabilidade de separar máquinas virtuais criando zonas de segurança por tipo de uso (estação ou servidor), etapas de produção (desenvolvimento, produção ou teste) e sensibilidade dos dados em componentes físicos de *hardware* (servidores, armazenamento, etc.).
10. O cliente de nuvem deve ter acesso a um mecanismo de relatórios que forneça evidências de isolação e emita alertas em caso de violação.
11. O cliente de nuvem deve estar ciente de situações de multilocação envolvendo suas máquinas virtuais onde preocupações regulatórias podem requerer sua separação.

5 PROPOSTA DE AUTENTICAÇÃO E ARMAZENAMENTO SEGUROS PARA SAAS

Neste capítulo são propostas, então, duas recomendações específicas de segurança em SaaS para dar mais segurança aos usuários contra o número crescente de invasões, sequestros de contas e de acesso não autorizado a dados sigilosos, como o caso da NSA que veio a público recentemente.

5.1 AUTENTICAÇÃO DE DOIS FATORES (2FA)

O usuário final é o elo mais vulnerável na computação em nuvem. Ele só pode proteger seus dados de acessos não autorizados através de uma senha, que pode ser facilmente descoberta por meio de técnicas de engenharia social, por observação, por vazamentos, ataque de *phishing* ou em computadores infectados/invadidos ou, ainda, se trafegarem na rede sem criptografia. Por isso, é importante que a verificação da identidade do usuário baseie-se em informações adicionais, além do uso único da senha.

Autenticação de dois fatores é um método que acrescenta uma camada extra de segurança no acesso aos serviços de nuvem contra potenciais invasores. Seu conceito não é novo. É utilizado há anos em caixas eletrônicos, mas muito pouco em serviços Web ou SaaS. Ele requer duas formas diferentes de provar a sua identidade, exigindo sua senha (algo que o usuário sabe) e seu cartão (algo que o usuário tem) (MOORE A, 2014).

Para acessar o serviço que utiliza 2FA, o usuário deve passar pelas duas etapas a seguir:

1. O primeiro passo é fazer o login usando o nome de usuário e senha. Esta é uma utilização do fator de conhecimento do usuário.
2. A segunda etapa requer um aplicativo autenticador, como o Google Authenticator, num celular, por exemplo. Esta é a aplicações do fator que o usuário tem.

Em seguida, abre-se o aplicativo, que gera um novo código de uso único com 8 dígitos a cada 20 segundos. Este código deve ser inserido na página seguinte para completar o registo no processo de login (Fig. 5.1). Caso a senha seja correta, mas o código de uso único seja errado, o usuário deve ser notificado, pois sua senha pode ter sido comprometida, voltando à autenticação em apenas um fator, o código de uso único.

Ainda que tenham outras camadas de segurança, os serviços de *internet banking* também utilizam apenas a 1FA e são suscetíveis a ataques de *phishing*, dentre outros já citados. O BB Code, solução de segurança do Banco do Brasil baseada em QR Code para

autorização de transações financeiras pela internet, da mais segurança às transferências bancárias substituindo a senha de 6 dígitos por um QR Code a ser capturar através do aplicativo do Banco do Brasil no celular, impossibilitando que uma transferência bancária fraudulenta seja feita por algum atacante (BANCO DO BRASIL, 2012). Apesar disso, o atacante ainda terá acesso à conta, sigilo bancário do usuário e informações pessoais, como o endereço residencial. Com posse desses dados, sabendo que o salário do correntista foi depositado no dia, o atacante poderia sequestra-lo na porta de casa e força-lo a sacar todo o dinheiro, por exemplo. Com a 2FA isso não seria possível. Neste caso, a combinação entre os dois, BB Code e 2FA, aumentaria a segurança dos bancos, evitando fraudes que chegam a milhões de reais aos seus cofres (DA COSTA, 2014).

Com a 1FA cada vez menos confiável como medida de segurança, a autenticação de dois fatores deve rapidamente ganhar importância para acesso a serviços online e deve virar padrão pra qualquer conta criada em qualquer serviço SaaS ou Web de qualquer empresa. Entretanto, estima se que cerca de 95% dos usuários não têm conhecimento da 2FA ou optam por não usá-la (MOORE B, 2014).

Figura 5.1. Ilustração do funcionamento da 2FA, adaptado de (CERT.BR, 2014).

Em 7 de outubro de 2014, o Yahoo! confirmou que alguns de seus servidores foram comprometidos dias antes por hackers que teriam explorado uma brecha em um código usado pela seção de esportes do portal, mas negou o acesso a dados (ROHR B, 2013). Entretanto, no dia seguinte recebi um e-mail do próprio Yahoo! avisando da tentativa de entrar em minha própria conta a partir dos EUA (Fig. 5.2). Este tipo de e-mail é enviado quando há uma tentativa de acesso a partir de uma região ou país diferente do habitual. Neste caso, login e senha estavam corretos, mas como o sistema de 2FA estava ativado não foi possível acessar a conta. Isto não só prova que o Yahoo! mentiu, mas também que o sistema de 2FA é eficaz contra invasões e sequestros de contas.

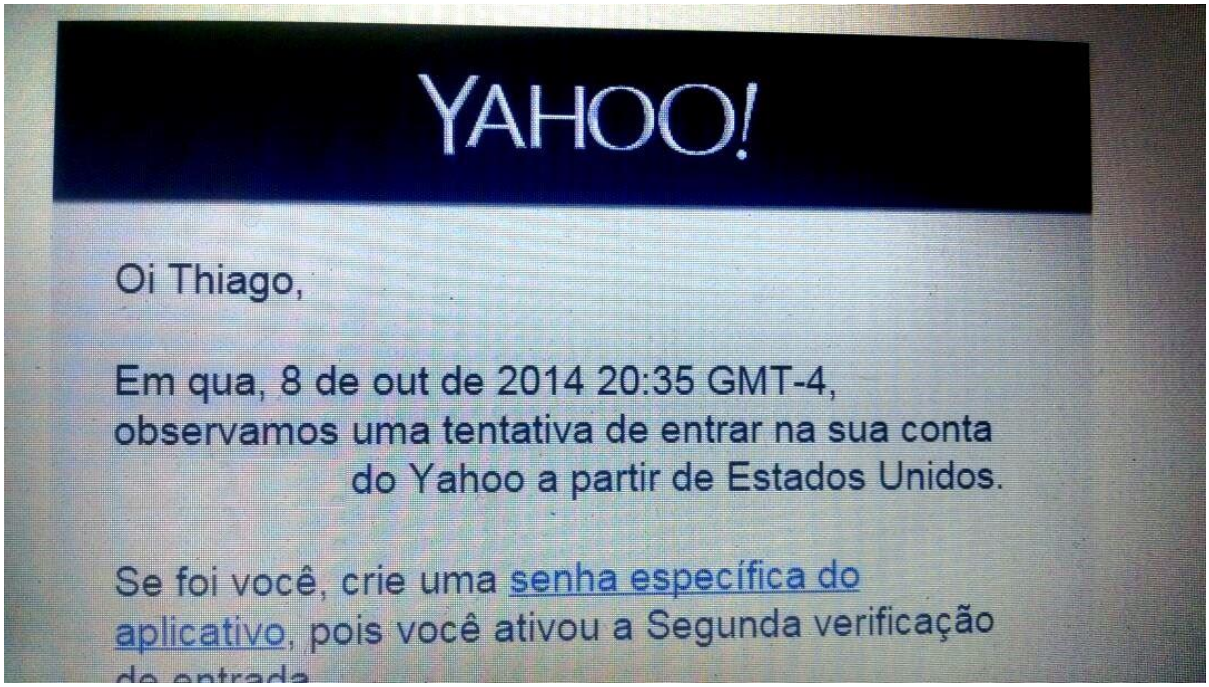

Figura 5.2. E-mail recebido do Yahoo! avisando da tentativa de entrar em minha conta a partir dos EUA.

5.1.1 VERIFICAÇÃO EM DUAS ETAPAS (2SV)

A verificação em duas etapas é erradamente usada como sinônimo para a autenticação de dois fatores. Ela funciona de maneira igual, mas introduz outros meios de se receber o código de uso único, como através de um e-mail de recuperação ou mensagem de texto. Esses meios são suscetíveis a ataques de *man-in-the-middle* ou redirecionamento de chamadas, como o que ocorreu com Grant Blakeman. Criminosos conseguiram redirecionar as chamadas do celular, para outro aparelho de posse deles, enviando mensagens e ligações. Assim, puderam receber o código de acesso à conta (BLAKEMAN, 2014). Pedidos de redirecionamento de chamadas e mensagens são feitos por telefone, bastando informar dados pessoais para que o atendente realize a operação.

A Figura (5.3) exemplifica visualmente o funcionamento dos três tipos de autenticação:

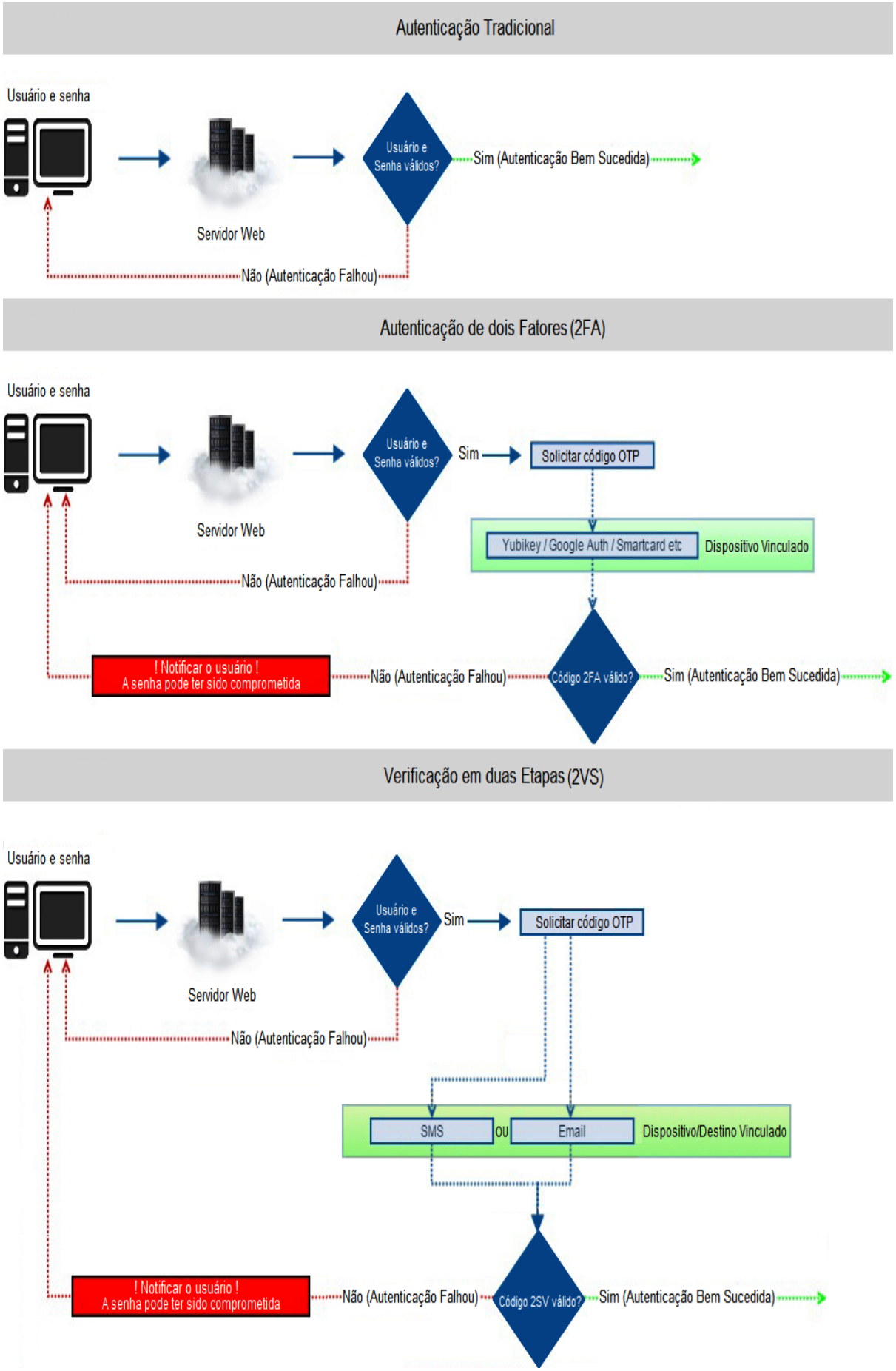

Figura 5.3. Comparação entre autenticação tradicional, 2FA e 2SV, adaptado de (MOORE B, 2014).

5.2 MODELO DE CRIPTOGRAFIA FIM-A-FIM (E2EE)

A 2FA pode impedir o acesso não autorizado de fora da nuvem aos dados armazenados nela, mas qualquer pessoa de dentro da nuvem pode ter acesso aos dados. Além disso, um funcionário descontente pode alterar ou destruir os dados utilizando de suas próprias credenciais de acesso, ou até mesmo o provedor pode ser obrigado a entregar os dados armazenados caso seja solicitado, por exemplo, pela NSA (JUNQUEIRA, 2013).

Em outubro de 2013 a imprensa publicou, com base nos documentos revelados por Edward Snowden, que através do MUSCULAR (Fig. 5.4), um dos programas do sistema de vigilância global, o GCHQ e a NSA secretamente invadiram os principais enlaces de comunicação dos centros de processamento de dados do Yahoo! e do Google ao redor do mundo, tendo acesso aos dados da nuvem de ambos (JB, 2013).

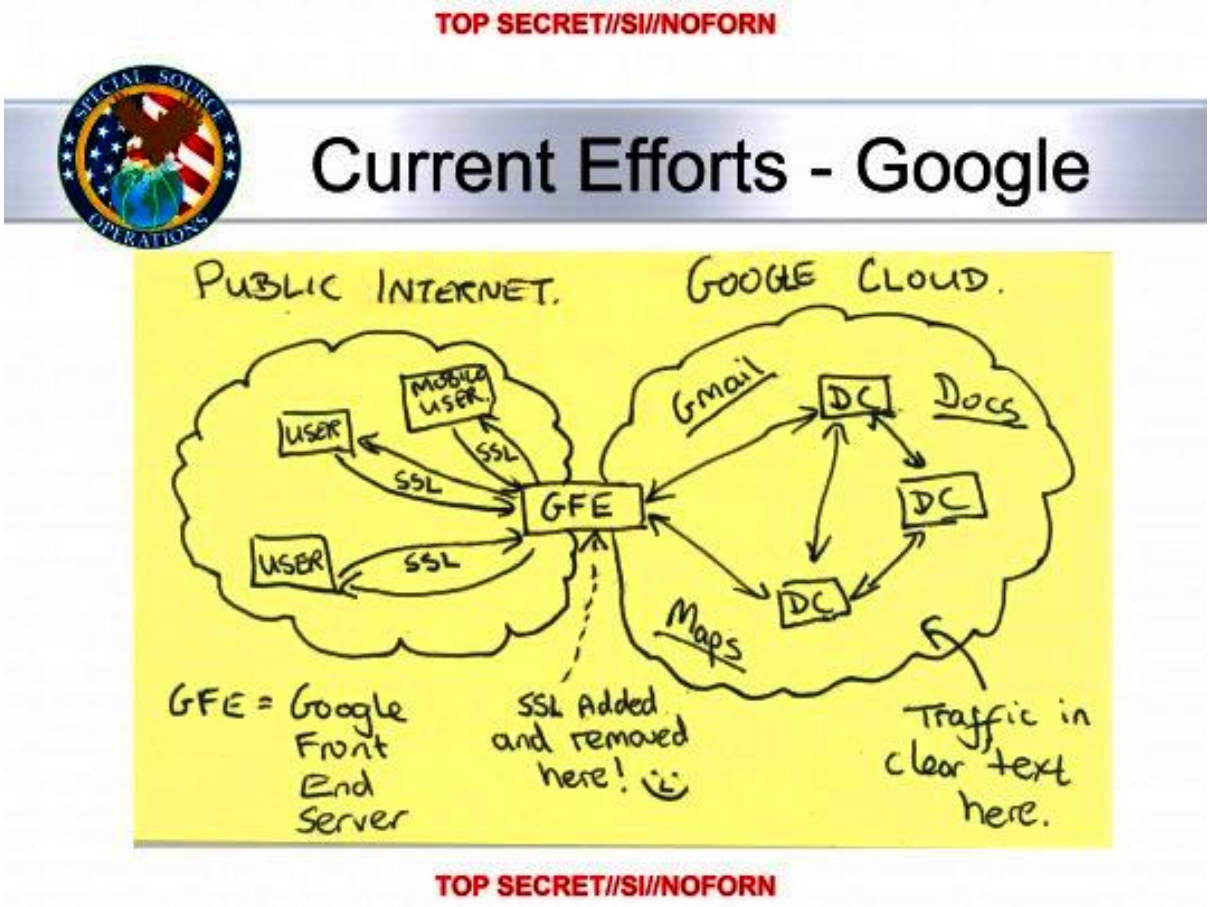

Figura 5.4. Slide da apresentação da NSA sobre o MUSCULAR indicando o sucesso na invasão à nuvem do Google (EFF, 2013).

Como em um sistema em nuvem é imprescindível utilizar o armazenamento criptografado dos dados, a maioria dos serviços de nuvem modernos faz uso de criptografia, mas não o modelo fim-a-fim, como mostra o slide da apresentação da NSA. Serviços Web populares, como Gmail e Hotmail utilizam criptografia SSL, mas enquanto esse tipo de

criptografia protege os usuários contra acessos não autorizados, é inútil contra os governos, como ocorreu no caso do Google (LEE, 2013).

Isso porque o SSL apenas protege os dados transferidos entre o dispositivo e os servidores do provedor de nuvem, como Google, Apple ou Microsoft. Eles têm acesso aos dados criptografados, mas como também têm as chaves criptográficas privadas, é como se os dados não estivessem criptografados. Assim, se o governo suspeitar de comportamento criminoso, pode obrigar o provedor a entregar os dados privados dos clientes (LEE, 2013).

Esse problema pode ser evitado com o modelo de criptografia fim-a-fim. Neste modelo, os dados são criptografados no dispositivo do transmissor e descriptografadas apenas no do receptor, já que, ao contrário do modelo de criptografia padrão, a chave de decodificação é armazenada no dispositivo do transmissor e compartilhada apenas com o receptor, usando criptografia de chave púbica (Fig. 5.5). Intermediários, como Google ou Microsoft, só veem a versão criptografada dos dados, o que torna impossível a leitura dos dados para o governo ou qualquer outra pessoa não autorizada (LEE, 2013). Mesmo que autoridades consigam obter os dados por ordem judicial, decifrá-los pode ser impossível na prática, pois encontrar a chave levará muito tempo (ROHR C, 2015).

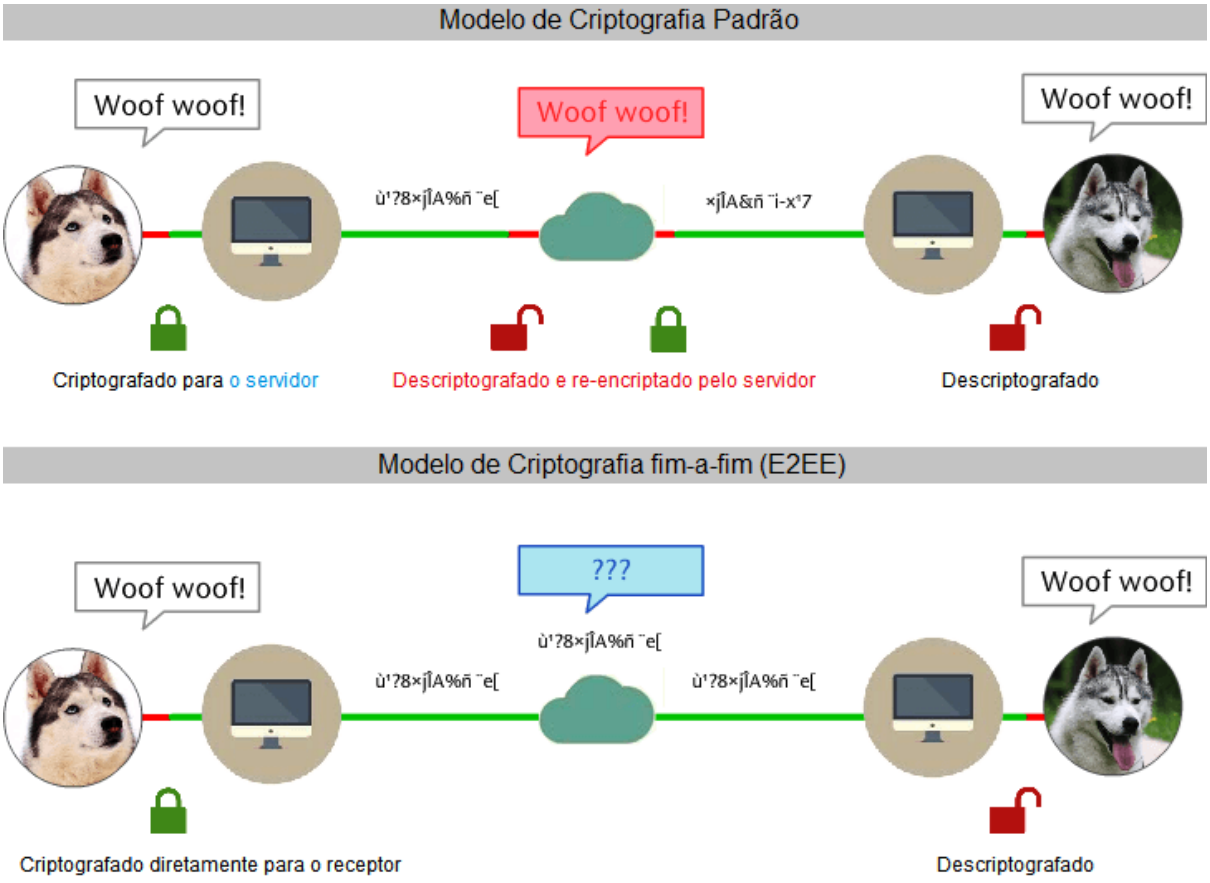

Figura 5.5. Comparação entre os modelos de criptografia padrão e E2EE, adaptado de (SUBROSA, 2014).

Em entrevista dada ao jornalista Glenn Greenwald, do jornal britânico *The Guardian*, em junho de 2013, Edward Snowden disse que "A criptografia funciona. Sistemas de criptografia forte implementados adequadamente são uma das poucas coisas em que você pode confiar. Infelizmente, a segurança da criptografia padrão é tão terrivelmente fraca que a NSA pode frequentemente encontrar maneiras de contorná-la." (GREENWALD, 2013). Diante desta declaração, prova se que o sistema de E2EE proposto é eficaz contra acessos não autorizados aos dados de clientes criptografados na nuvem.

6 CONCLUSÃO

O capitulo final apresentada as conclusões a respeito das recomendações propostas, a correspondência com os objetivos propostos e como os mesmos serão necessários para trabalhos futuros com o intuito de desenvolver as melhores praticas de segurança da informação na computação em nuvem.

Foi exposta uma visão geral da tecnologia da computação em nuvem e aprofundada nas falhas de segurança encontradas na literatura, fundamentadas por algumas análises em casos ocorridos recentemente. Pelo estudo realizado, nota-se que é um tema ainda não muito amadurecido, com amplo espaço para descobertas de novas vulnerabilidades, bem como, vertentes de pesquisas com a finalidade de encontrar e corrigir esses problemas.

Para o primeiro objetivo, foi feita uma pesquisa e um levantamento bibliográfico exploratório por meio de livros, artigos, estudos de caso, publicações, periódicos, e normas técnicas da ISO, ABNT e IEEE que continham os principais conceitos, características, motivações e principais áreas de preocupação quanto às ameaças à segurança da computação em nuvem hoje, principalmente os guias da CSA, que foram usados como base.

Em seguida para o segundo objetivo, uma análise meticulosa foi feita na bibliografia encontrada, desta vez analisando as recomendações de segurança da informação para as áreas de preocupação críticas quanto às ameaças à segurança encontradas na primeira parte. As recomendações que mais se relacionavam com os problemas encontrados na etapa anterior foram organizadas numa lista que cobre as principais ameaças e preocupações com segurança na nuvem hoje.

Finalmente para o terceiro objetivo, uma análise foi feita em dois casos recentes de vulnerabilidades na nuvem. Foram identificadas as ameaças e vulnerabilidades por meio de uma análise de riscos da segurança da informação, em seguida foram propostas duas recomendações para essas vulnerabilidades na segurança na nuvem.

Com as recomendações propostas, o trabalho aumentou a segurança na nuvem, a principal preocupação de quem quer ou já aderiu à nuvem. Estudou duas falhas de segurança específicas muito exploradas por hackers e agentes da Web, já citados em casos ocorridos recentemente, propondo duas soluções que melhoram a segurança dessas falhas.

Esclareceu os principais problemas de segurança dos mecanismos de autenticação de usuário, já que a ocorrência de invasões a contas de usuários em vários ambientes que hoje

não estão seguros é algo muito comum, e trouxe uma luz quanto à solução desses problemas.

A autenticação de dois fatores mostrou-se uma medida de segurança indispensável para contas de serviços Web, tais como e-mail, serviços bancários, ou rede social, tendo sua eficácia comprovada através do caso ocorrido com o Yahoo!. Embora a 2FA não signifique que elas estejam imunes à ataques, pois não há segurança infalível, ela aumenta muito segurança, fazendo o acesso não autorizado aos dados privados do usuário mais resistente, já que um atacante precisaria quebrar mais do que uma simples senha.

Já o sistema de criptografia fim-a-fim, mostra-se uma ferramenta muito poderosa contra o acesso não autorizado aos dados armazenados na nuvem, seja por usuários de dentro da nuvem, como funcionários do provedor, ou até mesmo de programas de vigilância global, como os da NSA, sendo descrito por Edward Snowden como uma das poucas coisas em que se pode confiar no que se refere à segurança dos dados.

As soluções propostas devem ser adotadas de maneira institucional pelos serviços eletrônicos do governo, pois não há uma política sobre isso, como mostrados nos casos do CNPq, MatrículaWeb e Telebrás, o que abre brechas pra que os sistemas sejam invadidos. Arquitetos de software também devem adotar as recomendações para os ambientes de software, além dos engenheiros de redes exigirem que essas recomendações sejam utilizadas.

Apesar das falhas de segurança mostradas, a computação em nuvem já faz parte do dia a dia da maioria das pessoas devido aos seus vários benefícios. O futuro aponta para um ambiente cada vez mais seguro para ser possível aproveitar todas as vantagens dessa tecnologia com segurança sem correr riscos.

Em trabalhos futuros, pode ser feita uma análise crítica das recomendações propostas para encontrar novas brechas de segurança que possam vir a aparecer, que possam se tornar obsoletas ou que não foram cobertas pelas recomendações, com o intuito de desenvolver as melhores praticas de segurança da informação na computação em nuvem.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2013.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança informação. Rio de Janeiro: ABNT, 2013.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/DIS 31000**: Gestão de riscos - Princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

ARRUDA, FELIPE. **Os 9 maiores roubos de dados da internet**, julho 2012. Disponível em: < http://www.tecmundo.com.br/seguranca/26476-os-9-maiores-roubos-de-dados-da-internet.htm >. Acesso em: 24/06/2015.

BANCO DO BRASIL. **BB Code**, agosto 2012. Disponível em: < http://www.bbseguranca.com.br/solucao-de-seguranca/1-BB-Code >. Acesso em: 23/03/2015.

BLAKEMAN, GRANT. **The Value of a Name**, novembro 2014. Disponível em: < http://ello.co/gb/post/knOWk-qeTqfSpJ6f8-arCQ >. Acesso em: 03/04/2015.

CAPUTO, VICTOR. **eBay é invadido por hackers e pede que usuários mudem senhas**, maio 2014. Disponível em: < http://exame.abril.com.br/tecnologia/noticias/ebay-e-invadido-por-hackers-e-pede-que-usuarios-mudem-senhas >. Acesso em: 21/05/2015.

CASTRO, R. C. C.; SOUSA, V. L. P. **Segurança em Cloud Computing - Governança e Gerenciamento de Riscos de Segurança**. Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE, Universidade Estadual do Ceará. Ceará - Brasil: 2010

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet - Fascículo Verificação em Duas Etapas**, novembro 2014. Disponível em: < http://cartilha.cert.br/fasciculos/verificacao-duas-etapas/fasciculo-verificacao-duas-etapas.pdf >. Acesso em: 23/01/2015.

CISCO. **Cisco Global Cloud Index: Forecast and Methodology**, 2013-2018, 2014. Disponível em: < http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf >. Acesso em: 23/01/2015.

CSA, CLOUD SECURITY ALLIANCE. **Corporate Members**, 2009. Disponível em: < http://cloudsecurityalliance.org/membership/corporate >. Acesso em: 12/04/2015.

CSA, CLOUD SECURITY ALLIANCE. **Top Threats to Cloud Computing V1.0**, março 2010. Disponível em: < http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf >. Acesso em: 17/01/2015.

CSA, CLOUD SECURITY ALLIANCE. **Security Guidance for Critical Areas of Focus in Cloud Computing V3.0**, 2011. Disponível em: < http://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf >. Acesso em: 17/01/2015.

CSA, CLOUD SECURITY ALLIANCE. **The Notorious Nine Cloud Computing Top Threats in 2013**, fevereiro 2013. Disponível em: < http://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf >. Acesso em: 17/01/2015.

CSABR, CLOUD SECURITY ALLIANCE - BRAZILIAN CHAPTER. **Adoção de Computação em Nuvem e suas Motivações**, agosto 2012. Disponível em: < http://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: 12/12/2014.

DA COSTA, MACHADO. **Fraude bancária faz Caixa e quatro bancos terem perda de R$ 10 milhões, diz MP**, maio 2014. Disponível em: < http://www1.folha.uol.com.br/mercado/2014/05/1461640-fraude-bancaria-faz-caixa-ter-perda-de-r-10-milhoes.shtml >. Acesso em: 04/02/2015.

EFF, ELECTRONIC FRONTIER FOUNDATION. **20131030-Wapo-Muscular Smiley**, outubro 2013. Disponível em: < http://www.eff.org/files/2014/04/14/20131030-wapo-muscular_smiley.pdf >. Acesso em: 03/04/2015.

G1. **Twitch redefine senhas de usuários após 'acesso não autorizado' a dados**, março 2015. Disponível em: < http://g1.globo.com/tecnologia/noticia/2015/03/twitch-redefine-senhas-de-usuarios-apos-acesso-nao-autorizado-dados.html >. Acesso em: 11/06/2015.

GARTNER. **Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010**, junho 2010. Disponível em: < http://www.gartner.com/newsroom/id/1389313 >. Acesso em: 13/02/2015.

GREENBERG, ANDY. **Cloud Computing's Stormy Side**, fevereiro 2008. Disponível em: < http://www.forbes.com/2008/02/17/web-application-cloud-tech-intel-cx_ag_0219cloud.html >. Acesso em: 31/01/2015.

GREENWALD, GLENN. **Edward Snowden: NSA whistleblower answers reader questions**, junho 2013. Disponível em: < http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower >. Acesso em: 26/05/2015.

GUSMÃO, GUSTAVO. **Brecha no iCloud pode ser responsável por parte dos vazamentos de fotos de celebridades**, setembro 2014. Disponível em: < http://info.abril.com.br/noticias/seguranca/2014/09/falha-no-icloud-pode-ser-responsavel-por-parte-dos-vazamentos-de-fotos-de-celebridades.shtml >. Acesso em: 26/05/2015.

HONOROF, MARSHALL. **How Secure Is Dropbox?**, julho 2013. Disponível em: < http://www.tomsguide.com/us/how-secure-is-dropbox,review-1809.html >. Acesso em: 26/05/2015.

HOST, ALEX. **Perspektivy perekhoda na IaaS**, março 2014. Disponível em: < http://www.alexhost.ru/perspektivy-perekhoda-na-iaas >. Acesso em: 07/04/2015.

IBM (A). **An architectural blueprint for autonomic computing**, junho 2005. Disponível em: < http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf >. Acesso em: 24/04/2015.

IBM (B). **Introduction to Grid Computing**, dezembro 2005. Disponível em: < http://www.redbooks.ibm.com/redbooks/pdfs/sg246778.pdf >. Acesso em: 12/02/2015.

IDC, International Data Corporation. **Cloud Computing 2010. IDC Enterprise Panel**, setembro 2009. Disponível em: < http://pt.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update >. Acesso em: 21/03/2015.

INFO. **Sem roupa: Fotos de Jennifer Lawrence e outras celebridades dos EUA vazam na internet**, setembro 2014. Disponível em: < http://info.abril.com.br/noticias/internet/2014/09/sem-roupa-fotos-de-jennifer-lawrence-e-outras-celebridades-dos-eua-vazam-na-internet.shtml >. Acesso em: 10/09/2014.

INTEL. **Next Generation Center: Grid Computing**, 2011. Disponível em: < http://tcc-web20.googlecode.com/svn/trunk/Pesquisa/Intel%20-%20Grid%20Computing.pdf >. Acesso em: 10/01/2015.

ISACA, INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives**, 2009. Disponível em: < http://www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_&_Governance-ISACA.pdf >. Acesso em: 22/05/2015.

ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **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, 2014.

ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27017**: Cloud Computing Security and Privacy Management System-Security Controls, 2015.

JN, JORNAL DO BRASIL. **Espionagem da NSA inclui invasão a data centers de Google e Yahoo!, diz jornal**, outubro 2013. Disponível em: < http://www.jb.com.br/ciencia-e-tecnologia/noticias/2013/10/31/espionagem-da-nsa-inclui-invasao-a-data-centers-de-google-e-yahoo-diz-jornal >. Acesso em: 03/04/2015.

JUNQUEIRA, DANIEL. **Microsoft teria dado à NSA acesso a emails, chamadas de vídeo e mais, segundo jornal** , julho 2013. Disponível em: < http://gizmodo.uol.com.br/microsoft-acesso-nsa >. Acesso em: 12/12/2014.

LEE, TIMOTHY B. **NSA-proof encryption exists. Why doesn't anyone use it?**, junho 2013. Disponível em: < http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it >. Acesso em: 26/04/2015.

LODI, JOÃO BOSCO. **Governança Corporativa: o Governo da Empresa e o Conselho de Administração**. Campus, 2000.

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

MCMILLAN, ROBERT. **Salesforce.com customer list stolen**, novembro 2007. Disponível em: < http://www.computerworlduk.com/news/security/6058/salesforcecom-customer-list-stolen >. Acesso em: 03/04/2015.

MOORE, PAUL (A). **Does Two Factor Authentication Actually Weaken Security?**, setembro 2014. Disponível em: < http://ramblingrant.co.uk/does-two-factor-authentication-actually-weaken-security >. Acesso em: 24/03/2015.

MOORE, PAUL (B). **The difference between two-factor and two-step authentication**, setembro 2014. Disponível em: < http://ramblingrant.co.uk/the-difference-between-two-factor-and-two-step-authentication >. Acesso em: 24/03/2015.

NICOLAU PAULO M., **Recomendações de Segurança da Informação para Soluções de Tecnologia da Informação e Comunicação Baseadas em Computação em Nuvem**. 2013. Faculdade de Tecnologia - FT, Universidade de Brasília. Brasília - Brasil: 2013

NIST, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication 800-144**: Guidelines on Security and Privacy in Public Cloud Computing. Gaithersburg : NIST, 2011.

NIST, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication 800-145**: The NIST Definition of Cloud Computing. Gaithersburg: NIST, 2011.

ROHR, ALTIERES (A). **Dados pessoais de usuários da PSN foram roubados, admite Sony**, abril 2011. Disponível em: < http://g1.globo.com/tecnologia/noticia/2011/04/dados-pessoais-de-usuarios-da-psn-foram-roubados-admite-sony.html >. Acesso em: 22/05/2015.

ROHR, ALTIERES (B). **Yahoo admite que sofreu invasão, mas nega acesso a dados**, outubro 2013. Disponível em: < http://g1.globo.com/tecnologia/noticia/2014/10/yahoo-admite-que-sofreu-invasao-mas-nega-acesso-dados.html >. Acesso em: 08/10/2014.

ROHR, ALTIERES (C). **Yahoo anuncia e-mail 'antigrampo' e 'senha única' enviada por SMS**, março 2015. Disponível em: < http://g1.globo.com/tecnologia/noticia/2015/03/yahoo-anuncia-e-mail-antigrampo-e-senha-unica-enviada-por-sms.html >. Acesso em: 28/03/2015.

ROUSE, MARGARET. **An introduction to SharePoint 2013**, setembro 2010. Disponível em: < http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery >. Acesso em: 11/01/2015.

SUBROSA. **Everything you ever say is recorded,** 2014. Disponível em: < http://subrosa.io/splash >. Acesso em: 16/03/2015.

MOGULL, RICH. **Data Security Lifecycle 2.0**, setembro 2011. Disponível em: < http://www.securosis.com/blog/data-security-lifecycle-2.0 >. Acesso em: 13/04/2015.

SILVA, ANTONIO LUÍZ. **Cloud Computing - Segurança e Privacidade da Informação na Nuvem**. IESF - Instituto Superior de Estudos Financeiros e Fiscais, julho 2012. Disponível em: < http://ssrn.com/abstract=2118225 >. Acesso em: 23/01/2015.

TORRES, IZABELLE. **Dilma contra o grande irmão,** fevereiro 2014. Disponível em: < http://www.istoe.com.br/reportagens/350108_DILMA+CONTRA+O+GRANDE+IRMAO >. Acesso em: 26/05/2015.

VELTE, TOBY J.; VELTE, ANTHONY T.; ELSENPETER, ROBERT. **Cloud Computing - A Practical Approach**. McGraw-Hill, 2009.

VMWARE. **Securing the Cloud: A Review of Cloud Computing, Security Implications and Best Pratices**, 2009. Disponível em: < http://www.vmware.com/files/pdf/cloud/VMware-Savvis-Cloud-WP-en.pdf >. Acesso em: 10/01/2015.

WARD, MARK. **How the modern world depends on encryption**, outubro 2013. Disponível em: < http://www.bbc.com/news/technology-24667834 >. Acesso em: 26/4/2014.

WINKLER, V. J. R. **Securing the Cloud: Cloud Computer Security Techniques and Tactics**. Syngress, 2011.

WONG, ANDREW. **Cloud Computing: Infrastructure as a Service (IaaS)**, abril 2014. Disponível em: < http://4ndrew.my/cloud-computing-infrastructure-as-a-service-iaas >. Acesso em: 06/12/2014.